Question #1 *Topic 1*

What is a result of enabling Cisco FTD clustering?

A. For the dynamic routing feature, if the master unit fails, the newly elected master unit maintains all existing connections.

B. Integrated Routing and Bridging is supported on the master unit.

C. Site-to-site VPN functionality is limited to the master unit, and all VPN connections are dropped if the master unit fails.

D. All Firepower appliances support Cisco FTD clustering.

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

Community vote distribution

C (100%)

jaciro11 11 months, 1 week ago

Selected Answer: C

c is correct

upvoted 2 times

aalnman 12 months ago

Answer given is correct - "Remote access VPN is not supported with clustering. VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities.

If the control unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control unit is elected, you must re-establish the VPN connections.

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

upvoted 4 times

rirani 1 year, 5 months ago

correct Answer based on https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/clustering_for_the_firepower_threat_defense.html

upvoted 4 times

Question #2 *Topic 1*

Which two conditions are necessary for high availability to function between two Cisco FTD devices? (Choose two.)

A. The units must be the same version

B. Both devices can be part of a different group that must be in the same domain when configured within the FMC.

C. The units must be different models if they are part of the same series.

D. The units must be configured only for firewall routed mode.

E. The units must be the same model.

Suggested Answer: *AE*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

Community vote distribution

AE (100%)

jaciro11 11 months, 1 week ago

Selected Answer: AE

A & E are correct

upvoted 2 times

Question #3 *Topic 1*

On the advanced tab under inline set properties, which allows interfaces to emulate a passive interface?

A. transparent inline mode

B. TAP mode

C. strict TCP enforcement

D. propagate link state

Suggested Answer: *B*

Community vote distribution

B (100%)

scanossa Highly Voted 4 years, 3 months ago

Tap Mode is the right anwer

Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/interface_overview_for_firepower_threat_defense.html#concept_DB45E8BBB07946728427FF98DB2DC56D

upvoted 16 times

Grandslam Most Recent 9 months ago

Selected Answer: B

Click Advanced to set the following optional parameters:

CORRECT ANSWER (B) Tap Mode — Set to inline tap mode.

INCORRECT ANSWER Propagate Link State:
Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up, also. In other words, if the link state of one interface changes, the device senses the change and updates the link state of the other interface to match it. Note that devices require up to 4 seconds to propagate link state changes. Link state propagation is especially useful in resilient network environments where routers are configured to reroute traffic automatically around network devices that are in a failure state.

upvoted 2 times

keen1 10 months, 2 weeks ago

what is the answer Cisco wants on test ?

upvoted 1 times

gwb 1 year, 3 months ago

what is benefit of TAP mode of inline set?

There are benefits to using tap mode with FTDs that are deployed inline. For example, you can set up the cabling between the FTD and the network as if the FTD were inline and analyze the kinds of intrusion events the FTD generates. Based on the results, you can modify your intrusion policy and add the drop rules that best protect your network without impacting its efficiency. When you are ready to deploy the FTD inline, you can disable tap mode and begin dropping suspicious traffic without having to reconfigure the cabling between the FTD and the network.

upvoted 1 times

Lautaros 2 years, 1 month ago

Its highlighted D as correct answer when should be B.

upvoted 3 times

Joe_Blue 2 years, 3 months ago

Selected Answer: B

The "TAP mode" option under the "Inline Set" properties on the Advanced tab of a Cisco FTD interface configuration also allows the interface to emulate a passive interface. In TAP mode, the interface is configured to passively monitor traffic by copying it to another interface, without actually forwarding or blocking any packets. This is useful for network monitoring or troubleshooting purposes, and can be combined with features like packet capture or intrusion detection.

upvoted 2 times

sis_net_sec 2 years, 5 months ago

Selected Answer: B

D is not correct

upvoted 1 times

Weyland 2 years, 7 months ago

Selected Answer: B

Dear Examtopics editor, when you don't change the answer on these obvious questions it makes us doubt all your answers. Do change it to Tap mode.

upvoted 2 times

johnny1001 2 years, 2 months ago

I guess, but it's the questions that are key, we can work out the answers if need be, and learn something in the process....if all the answers were guaranteed spot on it really would just be a question of memory recall.

upvoted 2 times

jaciro11 2 years, 11 months ago

Selected Answer: B

Answer is B

upvoted 2 times

xziomal9 3 years ago

Selected Answer: B

Correct answer is: B. TAP mode

upvoted 2 times

xziomal9 3 years ago

Correct answer is: B. TAP mode

upvoted 2 times

orotta 3 years, 4 months ago

The key phrase here is" interfaces to emulate a passive interface"

so Tap mode the correct answer

upvoted 3 times

ERGEGA 3 years, 5 months ago

D is the correct Answer.

upvoted 1 times

Sarbi 3 years, 9 months ago

Tap mode is the correct answer

upvoted 2 times

Bobster02 4 years ago

TAP mode indeed.

upvoted 3 times

ASherbiny_1604 4 years, 3 months ago

I agree with scanossa, TAP mode should be the correct answer.

Propagate link state has nothing to do with passive or active.

Link state propagation automatically brings down the second interface in the inline interface pair when one of the interfaces in an inline set goes down. When the downed interface comes back up, the second interface automatically comes back up.

upvoted 4 times

aken0527 4 years, 3 months ago

yes you are right ,thw answer should be tap mode.

upvoted 4 times

Question #4 *Topic 1*

What are the minimum requirements to deploy a managed device inline?

A. inline interfaces, security zones, MTU, and mode

B. passive interface, MTU, and mode

C. inline interfaces, MTU, and mode

D. passive interface, security zone, MTU, and mode

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/ips_device_deployments_and_configuration.html

Community vote distribution

C (100%)

darthrater Highly Voted 👍 3 years, 8 months ago

C, as a security zone ON the interface is not required to add to an inline pair. The GUI will tell you when you add the interfaces as a pair that it will remove any existing zone.

upvoted 7 times

tinyJoe Most Recent 🕓 5 months, 3 weeks ago

Selected Answer: A

I choose A.

As long as the documentation says the security zone setting is a “must”, I don't want to choose C.

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/interfaces-se ips.html#:~:text=Do%20not%20set%20the%20security%20zone%20yet;%20you%20must%20set%20it%20after%20you%20create%20the%20inline%20set%20la

upvoted 1 times

gwb 10 months, 3 weeks ago

(optional for security zone)

If you want to associate the inline interface with a security zone, do one of the following:

Choose an existing security zone from the Security Zone drop-down list.

Choose New to add a new security zone; see Creating Security Zone and Interface Group Objects.

upvoted 1 times

jaciro11 2 years, 5 months ago

Selected Answer: C

Correct is C

upvoted 2 times

orotta 2 years, 11 months ago

"minimum requirements"

The answer is C: Inline interface, MTU and Mode

Security zone is optional

upvoted 2 times

cryptofetti 3 years, 4 months ago

A is correct

The minimum set of requirements to deploy a device inline is to set the interfaces to inline, set the security zone, verify the MTU and set the mode (to none, which makes it inline).

upvoted 3 times

freemen810 11 months ago

Agree, to complete the inline set we need to assign security zone

upvoted 1 times

cryptofetti 3 years, 4 months ago

C, makes more sense here

upvoted 2 times

⊟ **kakakayayaya** 3 years, 7 months ago

You explicitly must fill up MTU and Inline pairs.

Mode is changing then you switch to Inline pair automatically. It is not configuration but is changes when you config Inline.

upvoted 2 times

⊟ **Deepub** 3 years, 8 months ago

The security zone also must configuration when deploying the devices inline.

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/ips_device_deployments_and_configuration.html#ID-2238-0000008b

"Create inline sets before you add security zones for the interfaces in the inline set; otherwise security zones are removed and you must add them again."

upvoted 2 times

Question #5 Topic 1

What is the difference between inline and inline tap on Cisco Firepower?

A. Inline tap mode can send a copy of the traffic to another device.

B. Inline tap mode does full packet capture.

C. Inline mode cannot do SSL decryption.

D. Inline mode can drop malicious traffic.

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **14a1949** 5 months, 3 weeks ago

Selected Answer: D

D. Inline mode can drop malicious traffic.

In inline mode, the device is placed directly in the path of network traffic and can actively block or drop malicious traffic. In contrast, inline tap mode sends a copy of the traffic to another device for analysis without affecting the actual traffic flow.

upvoted 1 times

⊟ **gwb** 10 months, 3 weeks ago

D This is a good reference site for different deployment mode

https://networkinterview.com/cisco-ftd-deployment-modes/

upvoted 2 times

⊟ **Cokamaniako** 1 year, 8 months ago

Selected Answer: D

Answer D

Inline mode can drop traffic

Inline Tap only can monitoring traffic

upvoted 1 times

⊟ **jaciro11** 2 years, 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

⊟ **aalnman** 2 years, 5 months ago

Selected Answer: D

The correct answer is D

Directly from the Official Cisco Press Cert Guide: "A threat defense in inline interface mode can block unintended traffic while it remains invisible to the network hosts. Inline mode allows a threat defense to block traffic based on the access control and intrusion rules you enable."

upvoted 1 times

⊟ **xziomal9** 2 years, 6 months ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

⊟ **Grandslam** 2 years, 9 months ago

Selected Answer: D

INLINE TAP

Copies the data to the SNORT Engine to be checked but then dropped while the actual data flow continues uninterrupted. Therefore, INLINE TAP does not send traffic to another device.

The Data is copied but not captured. You still would need to enable packet capture to capture packets (AKA Save PCAP).

INLINE:
Both inline and Inline Tap mode do not support SSL Decryption-resign... Although im a bit conflicted by this....

Truth is that Inline Mode can DROP malicious traffic but remember that Inline TAP mode CANNOT. Agan this is because tap mode sends a copy of the data to be inspected but not the actual data.

Best Answer is D.

upvoted 2 times

aadach 3 years, 2 months ago

oh sorry,
ONLY D !

upvoted 3 times

aadach 3 years, 2 months ago

A
1. With inline tap mode, the NGFW is only working with a copy of your data path traffic, as opposed to being inline with the actual data path.
2. It still sees all your traffic and can detect suspect traffic, but it cannot block your actual data path.
3. This lets you learn about how the NGFW responds in your particular environment, perhaps building your knowledge and confidence in preparation for Inline mode.
4. False positives and hardware failures will not affect your network connectivity.
5. However, there is a risk of some malicious traffic making inside your protected network.

upvoted 2 times

Sarbi 3 years, 2 months ago

sorry the correct answer is D only

upvoted 1 times

Sarbi 3 years, 2 months ago

The correct answer is B

upvoted 1 times

Grandslam 2 years, 9 months ago

TAP does not packet capture. It simply duplicates traffic to a provided destination.

upvoted 1 times

Question #6 *Topic 1*

With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. inline set

B. passive

C. routed

D. inline tap

Suggested Answer: *D*

Community vote distribution

D (67%) B (33%)

d0980cc 2 months, 2 weeks ago

Selected Answer: D

I believe it's D.
When I first read this statement, it did not make sense to me, but after careful reading, it states, "WITH Cisco FTD software". B, is correct but it requires an external device to mirror the traffic.

upvoted 1 times

14a1949 5 months, 2 weeks ago

Selected Answer: D

Passive Mode: This mode is used to monitor traffic without actively participating in the traffic flow. It receives a copy of the traffic for analysis but does not alter or forward the traffic itself.

Inline Tap Mode: This mode allows the device to monitor traffic inline, meaning it can see the traffic as it passes through the device, but it does not modify the traffic. It is similar to passive mode but is used in an inline deployment.

Given the requirement to passively receive traffic that passes through the appliance, Inline Tap Mode (Option D) could indeed be a suitable choice as it allows the device to monitor traffic inline without altering it.

upvoted 1 times

Grandslam 9 months ago

Selected Answer: D

With Cisco FTD software, which interface mode must be configured to
>>>>passively receive traffic
that
>>>>passes through the appliance?

INLINE TAP sends a COPY of the data to the SNORT Engineer where THAT COPY then is dropped... Meanwhile in parallel the actual traffic continues THROUGH the appliance uninterrupted.

This to me fits the definition of passive receiving traffic that PASSES THROUGH the appliance.

Answer D.

upvoted 3 times

mlu 10 months, 2 weeks ago

since the Traffic goes "THROUGH" the Firewall, Passive doesn't make sense.
So "Inline tap" is correct

upvoted 2 times

MB2222 1 year, 3 months ago

It is definitely B: (passive), since the question refers to the interface mode, and not the Inline-Set "Advanced Settings".

upvoted 1 times

bassfunk 1 year, 10 months ago

Selected Answer: B

The answer is B. Tested it in my lab. The only interface modes are ERSPAN, Passive and None. Tap is a mode for inline pairs. Not an interface.

upvoted 2 times

Stevens0103 1 year, 5 months ago

Inline Pair with Tap is an interface modehttps://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html#:~:text=Inline%20Pair%20with%20Tap

upvoted 2 times

gc999 1 year, 11 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html#:~:text=Inline%20Pair%20with%20Tap

upvoted 1 times

Shortbusruss 2 years ago

You have to really doubt the talent of anyone who answered "B" here, as Cisco is EXTREMELY clear about interface modes, which ones pass traffic THROUGH the appliance, and which ones just make copies of packets "passing by" the appliance. So much so, I have noted a couple of names in here that if my answers agree with theirs, I go back and take a HARD look at the documentation to make sure I am right. Some folks are so consistently wrong, and on such simple, basic questions, you almost gotta think they may be Cisco employees trying to muddy the waters.

upvoted 3 times

SegaMasterSystemAdmin 2 years ago

Selected Answer: D

It appears to be D as the traffic does still "passes through the appliance", if it is B, then it would only receive a copy of the traffic via SPAN or ERSpan

upvoted 2 times

YmerG 2 years ago

Selected Answer: D

Inline-tap for sure, because the key word here is "passing" and the interface in passive mode receives copies of the traffic

upvoted 2 times

Bbb78 2 years, 1 month ago

the main thing here is "passing"...with passive traffic is not "passing"

upvoted 2 times

saad_SEIU 2 years, 2 months ago

The answer is B, Passive Interface.

The Passive interface is passively receiving traffic thought the SPAN.

upvoted 2 times

Joe_Blue 2 years, 3 months ago

Selected Answer: D

The correct answer is D. inline tap. In inline tap mode, the Cisco FTD appliance is configured to passively receive a copy of the traffic that is passing through it, without actively processing or inspecting the traffic. This allows for non-disruptive monitoring and analysis of network traffic.

upvoted 1 times

Aarow 2 years, 9 months ago

Selected Answer: D

With passive interface configuration, traffic does not "pass through" the device, the FTD is configured in an out of band mode. Inline TAP seems a better answer.

upvoted 1 times

dique 2 years, 10 months ago

Selected Answer: D

Answer D

upvoted 1 times

jaciro11 2 years, 11 months ago

Selected Answer: B

Answer here is B

However most the question is formulated weirdly. Inline Set with TAP could be a better answer

upvoted 1 times

xziomal9 3 years ago

Correct answer is: D

upvoted 1 times

Question #7 *Topic 1*

Which two deployment types support high availability? (Choose two.)

A. transparent

B. routed

C. clustered

D. intra-chassis multi-instance

E. virtual appliance in public cloud

Suggested Answer: *AB*

Community vote distribution

AB (100%)

m70855712 7 months, 1 week ago

forgot to add to additonal

Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interfaces.
Different hostname [Fully Qualified Domain Name (FQDN)] for both chassis. In order to check the chassis hostname, navigate to FTD CLI and run this command:

upvoted 1 times

m70855712 7 months, 1 week ago

Conditions
In order to create an HA between 2 FTD devices, these conditions must be met:

Same model
Same version- this applies to FXOS and to FTD - major (first number), minor (second number), and maintenance (third number) must be equal.
Same number of interfaces
Same type of interfaces
Both devices as part of the same group/domain in FMC.
Have identical Network Time Protocol (NTP) configuration.
Be fully deployed on the FMC without uncommitted changes.
Be in the same firewall mode: routed or transparent.

upvoted 2 times

jaciro11 1 year, 11 months ago

Selected Answer: AB

A & B are good

upvoted 3 times

4study 2 years, 7 months ago

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html#anc2

upvoted 2 times

Question #8 *Topic 1*

Which protocol establishes network redundancy in a switched Firepower device deployment?

A. STP

B. HSRP

C. GLBP

D. VRRP

Suggested Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_threat_defense_high_availability.html

Community vote distribution

A (100%)

⊟ **thefiresays** **Highly Voted** 2 years, 2 months ago

Look in this doc for: Switched Deployment Redundancy

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01101000.html

upvoted 6 times

⊟ **jaciro11** **Most Recent** 11 months, 1 week ago

Selected Answer: A

Go for A

upvoted 1 times

Question #9 *Topic 1*

Which interface type allows packets to be dropped?

A. passive

B. inline

C. ERSPAN

D. TAP

Suggested Answer: *B*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200908-configuring-firepower-threat-defense-int.html

Community vote distribution

B (100%)

14a1949 5 months, 3 weeks ago

Selected Answer: B

he correct answer is:

B. inline

In inline mode, the device is placed directly in the path of network traffic and can actively block or drop malicious traffic.

upvoted 1 times

jaciro11 11 months, 1 week ago

Selected Answer: B

B is clear

upvoted 2 times

Question #10 *Topic 1*

Which Cisco Firepower Threat Defense, which two interface settings are required when configuring a routed interface? (Choose two.)

A. Redundant Interface

B. EtherChannel

C. Speed

D. Media Type

E. Duplex

Suggested Answer: *CE*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/fdm/fptd-fdm-config-guide-610/fptd-fdm-interfaces.html

Community vote distribution

CE (100%)

jaciro11 11 months, 1 week ago

Selected Answer: CE

C & E are good

upvoted 2 times

Question #11 *Topic 1*

Which two dynamic routing protocols are supported in Cisco FTD without using FlexConfig? (Choose two.)

A. EIGRP

B. OSPF

C. static routing

D. IS-IS

E. BGP

Suggested Answer: *BE*

Community vote distribution

BE (94%) 6%

kakakayayaya Highly Voted 👍 3 years ago

Wrong answer.

OSPF & BGP

upvoted 9 times

cryptofetti Highly Voted 👍 2 years, 10 months ago

B and E are correct

upvoted 5 times

cryptofetti 2 years, 10 months ago

FTD supports the following dynamic routing protocols:

OSPF

RIP

BGP

upvoted 3 times

abul8223 Most Recent 🕒 5 months, 1 week ago

Selected Answer: BE

ans: BE

upvoted 1 times

Aransi90 7 months, 4 weeks ago

Selected Answer: BE

Dynamic*

upvoted 2 times

bassfunk 11 months ago

In the new FMC7, i can now see EIGRP listed under routing. It was not here in previous versions. Does this mean its now natively supported?

upvoted 2 times

tinyJoe 5 months, 3 weeks ago

Very important point.

In fact, EIGRP can be configured in FMC ver 7.2 without going through FlexConfig.

If this question were asked now, there would be three correct answers.

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/routing-eigrp.html#Cisco_Reference.dita_036398ef-b5c1-4dc5-b280-5a330dbca578

upvoted 1 times

jewell2j 1 year ago

Selected Answer: BE

When the question says which two "DYNAMIC" routing protocols, I can't understand how the person running this place could choose static...

upvoted 2 times

hephep 1 year ago

Selected Answer: BE

static is the opposite of dynamic.

upvoted 2 times

SegaMasterSystemAdmin 1 year ago

Selected Answer: BE

Static routing is not a dynamic routing protocol

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: BE

In Cisco FTD, the two dynamic routing protocols that are supported natively (without requiring the use of FlexConfig) are OSPF and BGP.

upvoted 2 times

TCN 1 year, 8 months ago

Selected Answer: BE

According to cisco config guide answer is BE

upvoted 1 times

dique 1 year, 10 months ago

Selected Answer: BE

Correct answer: OSPF and BGP

upvoted 2 times

jaciro11 1 year, 11 months ago

Selected Answer: BE

Static Routing is not dynamic routing protocol

upvoted 1 times

hz033 2 years, 1 month ago

Selected Answer: BE

static routing is not dynamic routing

So, ospf and bgp

upvoted 1 times

Networkdumb 2 years, 2 months ago

Guys please read this " EIGRP, ISIS, and PBR are supported through Flex Config in FMC (see Predefined FlexConfig Objects). Configure only global virtual router interfaces for these features."

from: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/virtual-routing-for-firepower-threat-defense.html

upvoted 1 times

Grandslam 2 years, 3 months ago

Selected Answer: BE

OSPF and BGP are the two dynamic routing protocols that can be used withOUT FlexConfig.

upvoted 3 times

powerchiken 2 years, 6 months ago

Selected Answer: CE

Guys... Look this link.

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-routing.html

In the Supported Routing Protocols table appears OSPFv2, v3 and static route.

I believe Cisco shows C/E as right because option B is OSPF only.

upvoted 1 times

cewe 2 years, 4 months ago

the question is about dynamic routeing, static is not dynamic. also v3 is not available. so bgp and ospf are the right one

upvoted 2 times

azeol 2 years, 8 months ago

Dynamic Routing Protocols without FlexConfig are OSPF and BGP

upvoted 4 times

Question #12 *Topic 1*

Which policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI?

A. a default DMZ policy for which only a user can change the IP addresses.

B. deny ip any

C. no policy rule is included

D. permit ip any

Suggested Answer: *C*

Community vote distribution

C (86%) 14%

□ **abul8223** 5 months, 1 week ago

Selected Answer: C

ans: C

upvoted 1 times

□ **Grandslam** 9 months ago

Selected Answer: C

There is no DMZ setup during initial deployment of a CISCO NGFW using the FMC GUI... You would have to specify an interface designated to receive DMZ traffic, associate it to a security zone designated to DMZ traffic and lastly configure a policy to act on the DMZ traffic....

However, when creating a NEW access control policy you have to choose from one of the 3 default actions:
Block all traffic
Intrusion Prevention
Network Discovery

So Technical C would be correct because there is no DMZ deployment during initial setup but if you were to setup a DMZ after initial setup you would most likely block all traffic by default and change it after to allow all traffic... Because it's a DMZ...

I would say C.

upvoted 2 times

□ **eazy99** 9 months ago

Selected Answer: C

This is a tricky questions, both answers can be correct. The DMZ is here to throw us off, the default action for the FMC in the policy rules is Block ALL Traffic. Would they count this as a policy? Only the person who wrote the question knows. However, there are no Policies configured at all, that's why after you create your interface, you need to go and add your policy rules or it will be blocked by default. That's why I say it depends on what they are looking for with this question. Is there a "deny ip any" yes sure, but that's the default for everything and not only the DMZ, does it count as a policy? I don't think so, because when you go to the ACP it will tell you that you don't have any rules and you have to create a rule.
With that being said, I will go with the provided answer and pray for the best.

upvoted 1 times

□ **Joe_Blue** 2 years, 3 months ago

Selected Answer: C

No policy rule is included in the deployment of a local DMZ during the initial deployment of a Cisco NGFW through the Cisco FMC GUI. The administrator must create the necessary policy rules to allow traffic to and from the DMZ.

upvoted 2 times

□ **Baumb** 2 years, 4 months ago

Selected Answer: B

If we ask ourselves "Would traffic flow through a vanilla deployed FTD?" Then the answer would be no, which is why I would go with B

upvoted 1 times

□ **jaciro11** 2 years, 11 months ago

Selected Answer: C

I will go for C .. strange question though

upvoted 2 times

⊟ **Panjarakuttan** 3 years, 4 months ago

Answer is B

upvoted 1 times

⊟ **SLVan** 3 years, 5 months ago

Wrong "deny ip any"

upvoted 2 times

Question #13 *Topic 1*

What are two application layer preprocessors? (Choose two.)

A. CIFS

B. IMAP

C. SSL

D. DNP3

E. ICMP

Suggested Answer: *BC*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html

Community vote distribution

BC (100%)

gwb 9 months, 3 weeks ago

The DCE/RPC Preprocessor
The DNS Preprocessor
The FTP/Telnet Decoder
The HTTP Inspect Preprocessor
The Sun RPC Preprocessor
The SIP Preprocessor
The GTP Preprocessor
The IMAP Preprocessor
The POP Preprocessor
The SMTP Preprocessor
The SSH Preprocessor
The SSL Preprocessor

upvoted 4 times

jaciro11 2 years, 5 months ago

Selected Answer: BC

B & C are good

upvoted 2 times

Bobster02 3 years, 6 months ago

Original answers are correct: B and C

upvoted 2 times

scanossa 3 years, 9 months ago

it is the right question

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Application_Layer_Preprocessors.html#concept_75FF473E6A694C619489AD5C03E0B907

upvoted 4 times

Question #14 *Topic 1*

An engineer is implementing Cisco FTD in the network and is determining which Firepower mode to use. The organization needs to have multiple virtual
Firepower devices working separately inside of the FTD appliance to provide traffic segmentation. Which deployment mode should be configured in the Cisco
Firepower Management Console to support these requirements?

A. multi-instance

B. multiple deployment

C. single deployment

D. single-context

Suggested Answer: *A*

Community vote distribution

A (100%)

jaciro11 11 months, 1 week ago

Selected Answer: A

Answer is A

upvoted 3 times

4study 1 year, 7 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/multi-instance/multi-instance_solution.html#concept_vc4_2lh_3hb

upvoted 3 times

Question #15 *Topic 1*

A network engineer is extending a user segment through an FTD device for traffic inspection without creating another IP subnet. How is this accomplished on an
FTD device in routed mode?

A. by assigning an inline set interface

B. by using a BVI and creating a BVI IP address in the same subnet as the user segment

C. by leveraging the ARP to direct traffic through the firewall

D. by bypassing protocol inspection by leveraging pre-filter rules

Suggested Answer: *B*

Community vote distribution

B (58%) A (42%)

14a1949 5 months, 2 weeks ago

Selected Answer: B

Using an inline set interface is a valid approach in some cases, but for extending a user segment through an FTD (Firepower Threat Defense) device in routed mode without creating another IP subnet, the recommended method is using a BVI (Bridge Virtual Interface).

An inline set typically involves pairs of interfaces used for transparent or bridged mode, where traffic passes through the FTD device without routing, mainly used for intrusion prevention.

In routed mode, using a BVI allows the device to bridge two or more interfaces at Layer 2 while still inspecting traffic at Layer 3 and 4. This allows you to maintain the same IP subnet across these interfaces.

upvoted 1 times

Mohammad_h_tarawneh 10 months, 1 week ago

I think the key word is inspection , since you can extend subnet in inline and Bridg group ,
but the answer is "'A" since the inline set interface is used for inspection .

upvoted 2 times

squirrelzzz 11 months, 1 week ago

Selected Answer: A

BVI is for transparent mode

upvoted 2 times

gc999 2 years ago

Selected Answer: A

Extending a user segment without creating another segment. I believe only inline set can do it. Because it does not need to setup another IP address. Since the segment is already here, if we use BVI, it still needs to configure IP address and it would not be allowed as there is the same IP segment on one existing interface.

upvoted 2 times

Bbb78 2 years, 1 month ago

I have done this in a LAB. Option B looks to be correct.

upvoted 2 times

Initial14 2 years, 3 months ago

Selected Answer: B

The key here is Extend, so B. You can Have here BVI with no name and in that way the BVI acts as transparent firewall. So with that you have extended LAN network, the Gateway stays the same (ex. GW is 192.168.1.1 and BVI is 192.168.1.2) so nothing changes for users. If you go with Inline, you do not extend network, Inline only has inline par interfaces and that does not extend the LAN

upvoted 1 times

gwb 1 year, 4 months ago

I think B is correct. but your explanation is little not clear. Gateway should be 192.168.1.1 for BVI in your case because BVI is the gateway IP address.

upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: B

B. by using a BVI and creating a BVI IP address in the same subnet as the user segment.

A Bridged Virtual Interface (BVI) can be configured on an FTD device in routed mode to extend a user segment without the need to create another IP subnet. The BVI is configured with an IP address in the same subnet as the user segment, and the user segment is then connected to one of the switch ports on the FTD device. The BVI is then configured to bridge the traffic between the user segment and the FTD device's inside network, allowing the FTD device to inspect the traffic passing through it.

upvoted 2 times

Baumb 2 years, 4 months ago

Selected Answer: B

In: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

Its stated that "The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes. See Inline Sets and Passive Interfaces for Firepower Threat Defense for more information about IPS-only interfaces. Inline sets might be familiar to you as "transparent inline sets," but the inline interface type is unrelated to the transparent firewall mode described in this chapter or the firewall-type interfaces."

So Inline Interfaces have nothing to do with this deployment

upvoted 2 times

Weyland 2 years, 7 months ago

Selected Answer: A

"without creating another IP subnet". A BVI requires a subnet interface. Inline set acts like layer 2 but can be set up in a FTD in routed mode. No need for creating additionel IP-addresses or l3-interfaces. See "Inline IPS Interfaces" on CBT nuggets, Skill:
Cisco Firepower IPS/IDS.

upvoted 2 times

> **Weyland** 2 years, 7 months ago
>
> However B can also work if you use an existing network as BVI. But then you need to create extensive ACPs between the bridge groups. This one is super tricky but I'd still go with A.
>
> upvoted 1 times
>
> **gwb** 1 year, 4 months ago
>
> BVI uses the same ip subnet. For example, if connected devices are 192.168.0.2 and 3 /24 and want to add one more user segment, the subnet can be stayed same 192.168.0.0/24 and make BVI interface on FTD (192.168.0.1/24) so segment can be added without adding additional subnet.
> check this link especially diagram for ROUTE MODE BVI
> https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html
>
> upvoted 1 times

BorZol 2 years, 9 months ago

Correct answer is A. "Inline Set, with optional Tap mode—An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the FTD to be installed in any network environment without the configuration of adjacent network devices."
https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

upvoted 1 times

abdulmalik_mail 2 years, 10 months ago

Answer is A. On question say "FTD Device in Routed Mode". BVI is switched interface mode and only support transparent deployment mode

upvoted 2 times

> **gwb** 1 year, 4 months ago
>
> yeah.. BVI supports both transparent and routed. check this link
> https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html
>
> upvoted 1 times
>
> **Weyland** 2 years, 7 months ago

Bridge group interfaces can be deployed in Routed and Transparent firewall mode. However in transparent mode, each bridge group is separate and cannot communicate
with each other.
upvoted 2 times

jaciro11 2 years, 11 months ago

Selected Answer: B

For me both options A and B are correct. Wording could do the trick here. We do not assign inline sets, we add them an assign interfaces to it.
upvoted 1 times

xziomal9 3 years ago

Correct answer is: B
upvoted 1 times

kj2022 3 years, 1 month ago

Selected Answer: B

the question in not clear well
upvoted 1 times

jaruch8412 3 years, 7 months ago

The key is here the "routed mode" statement. Inline set interface can be created only in IPS-only mode, not routed mode. So B is correct.
upvoted 1 times

BorZol 2 years, 9 months ago

The firewall mode only affects regular firewall interfaces, and not IPS-only interfaces such as inline sets or passive interfaces. IPS-only interfaces can be used in both firewall modes.
upvoted 1 times

4study 3 years, 7 months ago

I think the key here might be the INSPECT keyword as inline-sets are meant to be used in a pure IPS setup that might be what they are hinting at
upvoted 1 times

Sarbi 3 years, 8 months ago

Answer A is
correct
upvoted 1 times

Question #16 *Topic 1*

An engineer is configuring a Cisco FTD appliance in IPS-only mode and needs to utilize fail-to-wire interfaces. Which interface mode should be used to meet these requirements?

A. passive

B. routed

C. transparent

D. inline set

Suggested Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

Community vote distribution

D (100%)

abul8223 5 months, 1 week ago

Selected Answer: D

Yes, D is correct

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: D

The correct answer is:

D. inline set

In IPS-only mode, using an inline set allows the Cisco FTD appliance to act as a bump on the wire, binding two interfaces together to transparently pass traffic while providing intrusion prevention capabilities. This setup supports fail-to-wire interfaces, ensuring traffic continues to flow even if the appliance fails

upvoted 1 times

m70855712 7 months, 1 week ago

Never mind, routed is an interface type.

upvoted 1 times

m70855712 7 months, 1 week ago

Straight out the gate you can eliminate Routed & Transparent since those are FTD Deployment modes Not interfaces modes.

upvoted 1 times

tanri04 1 year, 3 months ago

D. inline set.

When configuring a Cisco FTD appliance in IPS-only mode and utilizing fail-to-wire interfaces, the inline set interface mode should be used. This mode allows the device to inspect traffic and take action on it inline without disrupting traffic flow. The transparent mode allows the FTD to operate as a Layer 2 bridge, while the routed mode operates at Layer 3. The passive mode allows the FTD to monitor traffic without taking any action on it.

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: D

Fail-to-wire interfaces are used for bypassing traffic around an FTD appliance during a failure, and can only be used with the inline set interface mode. Therefore, the correct answer is D, inline set.

upvoted 1 times

jaciro11 1 year, 11 months ago

Selected Answer: D

Transparent is not an interface mode, inline set is

upvoted 1 times

Question #17 Topic 1

An organization has noticed that malware was downloaded from a website that does not currently have a known bad reputation. How will this issue be addressed globally in the quickest way possible and with the least amount of impact?

A. by creating a URL object in the policy to block the website.

B. Cisco Talos will automatically update the policies.

C. by denying outbound web access

D. by isolating the endpoint

Suggested Answer: *A*

Community vote distribution

A (80%) B (20%)

⊟ **ASIFIMRAN** Highly Voted 3 years, 11 months ago

Correct Ans A

upvoted 6 times

⊟ **squirrelzzz** Most Recent 11 months, 1 week ago

Selected Answer: B

Talos submission

upvoted 1 times

⊟ **Cokamaniako** 2 years, 1 month ago

Selected Answer: A

quickest way possible

The anser is A

upvoted 1 times

⊟ **Joe_Blue** 2 years, 3 months ago

Selected Answer: A

A. by creating a URL object in the policy to block the website.

Creating a URL object in the policy to block the website is the quickest way to address the issue globally with the least amount of impact. This approach is more targeted and less disruptive than denying all outbound web access or isolating the endpoint. Cisco Talos may eventually update the policies, but it could take some time before the new threat is identified and added to the blacklist.

upvoted 1 times

⊟ **Mevijil** 2 years, 6 months ago

Selected Answer: A

I believe it is A - I think they mean 'global' here in the sense that it needs to be addressed across the FMC deployment

upvoted 2 times

⊟ **BorZol** 2 years, 9 months ago

Does not currently bad reputation... Threat Grid could be a good solution - it can chack it in sandbox and set a bad reputation but it is time consuming.

Correct is A

upvoted 1 times

⊟ **aalnman** 3 years, 1 month ago

A = real-world scenario, as someone who manages these devices I do answer A on a regular basis. It takes about 3-minutes to implement, is global to the org, and only impacts the malicious site.

When I can do this myself why in the world would I submit it to Talos and keep my fingers crossed while there is potential for malware to spread throughout my network.

upvoted 2 times

⊟ **hz033** 3 years, 1 month ago

tricky is the following, "How will this issue be addressed globally" and "in the quickest way possible" and "with the least amount of impact"

How will this issue be addressed globally - The answer can be B, but

"in the quickest way possible" - The answer will be A

We can not wait for Talos to do an update because this is not the quickest way.

so I vote for A

upvoted 4 times

Reece_S 3 years, 1 month ago

Answer is B. You can do a manual submission to Talos and the disposition returned will be updated. Also it says "least amount of impact". Answer A will need to be deployed after you change the policy.

upvoted 2 times

Cokamaniako 2 years, 1 month ago

quickest way possible

The anser is A

upvoted 1 times

Shortbusruss 2 years ago

You have a lotta confidence in your answer, given that you are presupposing the exam question writer is expecting the exam taker to make a jump of logic that 1. option B requires manual intervention on the engineer's part, 2. That Talos will update disposition on a timely matter, instead of an hour or two, and meanwhile, connections from your network can still reach the malicious site and spew malware into your environment. Answer is A.

upvoted 1 times

orotta 3 years, 5 months ago

There are four keywords in the question:

Organization, globally, quickest and least amount of impact

Globally means worldwide, if it is referring to internal, it should say organizational

Talos feeds are updated by default every hour. You can change the update frequency.

I would go for B.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-sec-intel.html

upvoted 2 times

IPsecchio 3 years, 7 months ago

the correct answer is?

upvoted 1 times

ccnp_archer_dk 3 years, 8 months ago

Globally doesnt mean world wide, but instead globally within your company (as apposed to locally - device specific).

Therefore A must be the correct answer.

upvoted 2 times

essie007 3 years, 11 months ago

I would expect the correct answer to be about blacklisting

upvoted 2 times

Bobster02 4 years ago

50/50 chance

upvoted 1 times

kakakayayaya 4 years ago

Cisco Talos will not rely on your malware detection verdict automatically. It might happen what site will never be added to Talos.

upvoted 1 times

Bobster02 4 years ago

I agree that it may take some time to get Cisco Talos updates, however, the key words are ADDRESSED GLOBALLY, therefore answer B will have my vote.

upvoted 1 times

kakakayayaya 4 years ago

We can wait a lot until Talos adds URL to DB.

A - better decision.

upvoted 2 times

Question #18 *Topic 1*

The event dashboard within the Cisco FMC has been inundated with low priority intrusion drop events, which are overshadowing high priority events. An engineer has been tasked with reviewing the policies and reducing the low priority events. Which action should be configured to accomplish this task?

A. drop packet

B. generate events

C. drop connection

D. drop and generate

Suggested Answer: *A*

Community vote distribution

A (100%)

Joe_Blue Highly Voted 1 year, 9 months ago

Selected Answer: A

To reduce low priority intrusion drop events and keep the high priority events visible, the "drop packet" action can be configured in the intrusion policy. This will silently drop the packets that trigger low priority intrusion events without generating any event or alert, thereby reducing the noise in the event dashboard.

upvoted 5 times

14a1949 Most Recent 5 months, 3 weeks ago

Selected Answer: A

To reduce the low priority intrusion drop events and focus on high priority events, the engineer should configure the action to:

A. drop packet

By setting the action to "drop packet," the system will drop the packets without generating events for low priority intrusions. This helps in reducing the clutter of low priority events in the event dashboard, allowing high priority events to stand out

upvoted 1 times

Lautaros 1 year, 7 months ago

it highlighted as B the correct answer. should be A

upvoted 2 times

jaciro11 2 years, 5 months ago

Selected Answer: A

go with A

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

SanchezEldorado 2 years, 8 months ago

This had me really confused for a bit, because I didn't see an option to just drop packet anywhere. I appears there is a difference between the versions of when this question was originally posted and now. The only Drop option in newer versions is Drop and generate events. I think the correct answer now would be to add a threshold to limit the number of events.

Here's a link for version 6.2 that doesn't show a drop and generate events option:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/working_with_intrusion_events.html

Here's a link for 7.0 that doesn't show a drop option:
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/working_with_intrusion_events.html

upvoted 2 times

⊟ **gwb** 10 months, 3 weeks ago

Drop packets — Click Set this rule to drop the triggering packet... to set the rule to drop packets that trigger it.

If your managed device is deployed inline on your network, you can set the rule that triggered the event to drop packets that trigger the rule in all policies that you can edit locally. Alternately, you can set the rule only in the current policy (that is, the policy that generated the event) if you can edit the current policy locally.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/working_with_intrusion_events.html

- This is a link for "drop packet" in event

upvoted 1 times

⊟ **orotta** 2 years, 11 months ago

A seems to be correct:

IPS has three rule state:

Generate Event, Drop and Generate Events and Disable

currently, the rule is set to Drop and Generate Events and the event on the dashboard is inundated with low priority intrusion drop events, and they are asking to reduce it, so the best option is to set the low priority events to "Generate Event" so option A is correct, I believe.

upvoted 3 times

⊟ **powerchiken** 3 years ago

Selected Answer: A

I agree with kakakayayaya.

upvoted 1 times

⊟ **jnk12** 3 years, 4 months ago

Intrusion policy only has generate events, disabled, and drop and generate events. So the answer is correct.

upvoted 4 times

⊟ **anwar1** 2 years, 7 months ago

Thank you for mentioning that, though our logic is correct but still we need to follow Cisco guidelines to be able to correct score a mark for correct answer.

upvoted 1 times

⊟ **ASIFIMRAN** 3 years, 5 months ago

Drop packet is correct

upvoted 2 times

⊟ **Bobster02** 3 years, 6 months ago

A would make the most seance to me.

upvoted 1 times

⊟ **kakakayayaya** 3 years, 6 months ago

PS Event filtering with threshold should be the most appropriate solution for reducing events but there is no such answer......

upvoted 3 times

⊟ **kakakayayaya** 3 years, 6 months ago

generate events - it is exactly what was asked to avoid. To reduce amount of events we need to drop packets.

Block with reset even better.

So A and C make scene for me but would I vote for A.

upvoted 2 times

Question #19 *Topic 1*

With Cisco FTD integrated routing and bridging, which interface does the bridge group use to communicate with a routed interface?

A. subinterface

B. switch virtual

C. bridge virtual

D. bridge group member

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

greeklover84 10 months ago

it is C.... see the reference below

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

upvoted 3 times

Question #20 *Topic 1*

An engineer is setting up a new Firepower deployment and is looking at the default FMC policies to start the implementation. During the initial trial phase, the organization wants to test some common Snort rules while still allowing the majority of network traffic to pass. Which default policy should be used?

A. Balanced Security and Connectivity

B. Security Over Connectivity

C. Maximum Detection

D. Connectivity Over Security

Suggested Answer: *D*

Community vote distribution

D (54%) A (46%)

d0980cc 2 months, 2 weeks ago

Selected Answer: D

I'm thinking D, because of "common rule" reference.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/fdm/fptd-fdm-config-guide-700/fptd-fdm-intrusion.html#:~:text=Only%20the%20most%20critical%20rules%20that%20block%20traffic%20are%20enabled.

upvoted 1 times

whysohardwhy 4 months, 2 weeks ago

Selected Answer: A

The question is poorly worded. I think everyone here knows the differences. Just the question was written in a way to confuse people.
Default should be Balanced.
Only if you want minimum disruptions - go with Connectivity.
As a start, you should do it in Balanced + IDS mode.
Bad wording for a questio.

upvoted 2 times

14a1949 5 months, 3 weeks ago

Selected Answer: A

In this context, A. Balanced Security and Connectivity is indeed the best choice, as it provides a balance between security and allowing network traffic, which is ideal for an initial trial phase.

D. Connectivity Over Security is more focused on ensuring maximum network connectivity, possibly at the expense of security, and might not be suitable if you want to test Snort rules effectively.

So, Balanced Security and Connectivity remains the recommended default policy for your scenario. If you have any further questions or need additional clarification, feel free to ask!

upvoted 1 times

xBojmir215x 6 months ago

Selected Answer: A

I think its A, balanced security over connectivity. While D does allow the majority of traffic to pass, the question ends with "by default". Answer A, Balanced Security and Connectivity, is the default and still allows most traffic to pass.

upvoted 1 times

loser4fun 7 months, 2 weeks ago

Answer A

As the Connectivity Over Security policy does prioritize allowing network traffic to pass with minimal restrictions. However, for testing common Snort rules while still maintaining a reasonable level of security, the Balanced Security and Connectivity policy is generally more appropriate. It strikes a good balance between security and performance, ensuring that you can test the rules effectively without compromising too much on security.

If the primary goal is to ensure maximum network traffic flow with minimal interference, then Connectivity Over Security could be considered. However, this might not provide enough security controls to effectively test the Snort rules.

upvoted 1 times

Joe_Blue 9 months ago

Selected Answer: A

The default policy that should be used in this scenario is "Balanced Security and Connectivity". This policy provides a balanced approach to security and network connectivity, allowing common traffic to pass while still detecting threats using a set of predefined rules, including common Snort rules. The "Security Over Connectivity" and "Maximum Detection" policies are more restrictive and may block legitimate traffic, while "Connectivity Over Security" is less secure and may allow malicious traffic to pass.

upvoted 1 times

squirrelzzz 11 months, 1 week ago

Selected Answer: D

For testing

upvoted 2 times

wordisbondkid 1 year, 3 months ago

This should be a "No-Brainer" but I am really surprised so many think A is the answer. The answer is 100% Text Book - D. connectivity over security. It's the text book use case.

upvoted 3 times

devildog 10 months ago

It's such a "no brainer" that you could not include a source to justify your answer. Don't be condescending, we are all here trying to learn.

upvoted 2 times

SegaMasterSystemAdmin 2 years ago

Selected Answer: A

I'd go with A because based on the article "Balanced Security and Connectivity" is a good starting point:

"These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types. The system uses the Balanced Security and Connectivity network analysis policy as the default."

The question states that the engineer is setting up a new deployment so there you go.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-intrusion.html

upvoted 2 times

tanri04 2 years, 3 months ago

The Connectivity Over Security policy prioritizes network connectivity over security and allows traffic to pass through with a minimal number of intrusion detection rules applied. This would be appropriate for testing common Snort rules while still allowing most network traffic to pass through.

However, it is important to note that this policy may not provide the highest level of security and should only be used for testing purposes. It is recommended to use a policy that provides a balance between security and connectivity or prioritizes security once the testing phase is complete

upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: A

Key word here is default settings. By using the "Balanced Security and Connectivity" policy as a starting point, the organization can test common Snort rules while still allowing most traffic to pass, and then adjust the policy as needed based on the results of the testing and the specific needs of the organization.

upvoted 1 times

Joe_Blue 2 years, 4 months ago

Selected Answer: A

These policies are built for both speed and detection. Used together, they serve as a good starting point for most networks and deployment types. The system uses the Balanced Security and Connectivity network analysis policy as the default.

upvoted 1 times

Baumb 2 years, 4 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-intrusion.html

upvoted 1 times

minon_bob 2 years, 6 months ago

The answer should be 'A', Balanced is a good starting point, this is noted in the question.

upvoted 1 times

xziomal9 3 years ago

Selected Answer: D

Correct answer is: D

upvoted 3 times

orotta 3 years, 4 months ago

The key phrase is "allowing the majority of network traffic to pass"

so I will go with Connectivity over Security

upvoted 3 times

Alee86 3 years, 5 months ago

Balanced Security and Connectivity – A compromise of speed and detection

Connectivity over Security – Used when connectivity is more important. Only the most critical rules are enabled

Security over Connectivity – When connectivity is the secondary concern. Enables most rules. May result in higher false positives

Maximum detection – Every rule is turned on, and will likely result in false positives. Best to only use this for labs and testing

No Rules Active – All rules are disabled. Would generally only be used as a template

upvoted 1 times

Question #21 *Topic 1*

An engineer is configuring a second Cisco FMC as a standby device but is unable to register with the active unit. What is causing this issue?

A. The code versions running on the Cisco FMC devices are different.

B. The licensing purchased does not include high availability.

C. The primary FMC currently has devices connected to it.

D. There is only 10 Mbps of bandwidth between the two devices.

Suggested Answer: *A*

aadach 7 months ago

FMC High Availability. High Availability is available on physical Firepower Management Center appliances (and FMCv since 6.7. 0).

Before configuring FMC HA make sure that…

• Hardware is identical (no mix and match between virtual and/or physical form factors)

• Software release is identical on both FMCs

• There are no sensors registered to the secondary FMC

upvoted 3 times

Question #22 *Topic 1*

While configuring FTD, a network engineer wants to ensure that traffic passing though the appliance does not require routing or VLAN rewriting. Which interface mode should the engineer implement to accomplish this task?

A. inline set

B. passive

C. transparent

D. inline tap

Suggested Answer: *A*

Community vote distribution

A (67%) C (17%) B (17%)

kakakayayaya Highly Voted 👍 3 years ago

"traffic passing though the appliance" - Passive interface doesn't allow this.
Transparent - is not an interface mode.
"inline tap" can be appropriate but it should be named as "inline set with tap".
As for me "inline set" - is the best choice.

upvoted 12 times

14a1949 Most Recent 5 months, 3 weeks ago

Selected Answer: A

You're right, "transparent" is a deployment mode, not an interface mode. For Cisco FTD, if you want to ensure that traffic passing through the appliance does not require routing or VLAN rewriting, you should use:

A. inline set

In inline set mode, the device binds two interfaces together to transparently pass traffic without requiring routing or VLAN rewriting

upvoted 2 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

While **A. inline set** is a mode where the device is placed inline to inspect and potentially alter traffic, it might involve routing and VLAN rewriting, which doesn't align with your requirement of not needing routing or VLAN rewriting.

The correct choice is:

C. transparent

In transparent mode, the Cisco FTD appliance acts as a bridge (bump-in-the-wire), allowing traffic to pass through without any routing or VLAN tagging changes. This ensures that the traffic remains unaltered while passing through the device.

If you have any more questions or need further clarification, feel free to ask!

upvoted 2 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

should it be A
While A. inline set is a mode where the device is placed inline to inspect and potentially alter traffic, it involves routing and VLAN rewriting, which doesn't align with your requirement of not needing routing or VLAN rewriting.

The correct choice is indeed:

C. transparent

In transparent mode, the Cisco FTD appliance acts as a bridge, allowing traffic to pass through without any routing or VLAN tagging changes. This ensures that the traffic remains unaltered while passing through the device.

upvoted 1 times

bassfunk 10 months, 2 weeks ago

Selected Answer: A

This is one of the worst questions Ive seen for this exam. Inline set is the only answer that can be correct but it is not an interface mode, its a type of deployment for interfaces. Passive is the only interface mode listed here. Still, i would go with A.

upvoted 3 times

achille5 12 months ago

Selected Answer: A

Inline set

upvoted 1 times

Bbb78 1 year, 2 months ago

A - inline set is the only option that passes traffic.

D and C are not real options - D is sub option of A and C is another name for A

B - do not pass traffic - only receives packets from switch SPAN port

upvoted 1 times

eric0430 1 year, 3 months ago

Selected Answer: A

interface mode = C is not an interface mode.

pass through the appliance = B is not does not pass through traffic.

Did not say not allowed to drop malicious traffic = A (as security engineer, best to always chose the most secured design).

upvoted 1 times

tanri04 1 year, 3 months ago

Transparent is not an interface mode in Cisco FTD. The correct answer is D. Inline set. This mode allows traffic to be forwarded through the FTD device as if it were a simple Layer 2 switch, without requiring any routing or VLAN rewriting.

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: C

The interface mode that should be implemented to ensure that traffic passing through the FTD does not require routing or VLAN rewriting is transparent mode. In transparent mode, the FTD is placed in-line with the network traffic, and it can inspect traffic without making changes to IP addresses or VLAN tags. The transparent mode is also known as bridge mode and is often used for passive intrusion detection and prevention.

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: C

No, the passive interface mode does not allow traffic to pass through the appliance, it only allows the appliance to receive a copy of the traffic for inspection.

To ensure that traffic passing through the FTD appliance does not require routing or VLAN rewriting, the network engineer should implement the transparent interface mode.

upvoted 1 times

Baumb 1 year, 4 months ago

Selected Answer: A

It should be A, since https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

upvoted 1 times

minon_bob 1 year, 6 months ago

Selected Answer: A

An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the FTD to be installed in any network environment without the configuration of adjacent network devices.

upvoted 1 times

BorZol 1 year, 9 months ago

Inline tap is not good.

With tap mode, the device is deployed inline, but instead of the packet flow passing through the device, a copy of each packet > do not flow through the device

upvoted 2 times

⊟ **BorZol** 1 year, 9 months ago

Passive interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted. Inline is correct.

An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the system to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

upvoted 1 times

⊟ **jaciro11** 1 year, 11 months ago

Selected Answer: B

Inline Set requires VLAN rewriting

upvoted 2 times

⊟ **z6st2a1jv** 8 months, 2 weeks ago

No, inline-set does not require VLAN rewriting. An inline set in Firepower Threat Defense (FTD) is a pair of interfaces1. One interface is for incoming (IN) traffic and the other is for outgoing (OUT) traffic1. You cannot create a VLAN for IN/OUT traffic for the inline set1. This means that VLAN rewriting is not a requirement when configuring an inline set on FTD devices

upvoted 1 times

⊟ **xziomal9** 2 years ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

Question #23 *Topic 1*

A mid-sized company is experiencing higher network bandwidth utilization due to a recent acquisition. The network operations team is asked to scale up their one
Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth. Which design option should be used to accomplish this goal?

A. Deploy multiple Cisco FTD HA pairs in clustering mode to increase performance.

B. Deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.

C. Deploy multiple Cisco FTD appliances using VPN load-balancing to scale performance.

D. Deploy multiple Cisco FTD HA pairs to increase performance.

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-cluster-solution.html#concept_C8502505F840451C9E600F1EED9BC18E

tanri04 9 months, 2 weeks ago
Option:B)To scale up a one Cisco FTD appliance deployment to higher capacities due to the increased network bandwidth, the design option that should be used to accomplish this goal is B, deploy multiple Cisco FTD appliances in firewall clustering mode to increase performance.

Firewall clustering allows multiple FTD appliances to be joined together to form a single logical entity, which can increase performance by distributing traffic processing across multiple devices. This design option provides a scalable solution that can handle increased network bandwidth while maintaining network security and performance.
upvoted 3 times

Question #24 *Topic 1*

In a multi-tenant deployment where multiple domains are in use, which update should be applied outside of the Global Domain?

A. minor upgrade

B. local import of intrusion rules

C. Cisco Geolocation Database

D. local import of major upgrade

Suggested Answer: *B*

Community vote distribution

B (100%)

achille5 11 months ago

"In a multidomain deployment, you can import local intrusion rules in any domain, but you can import intrusion rule updates from Talos in the Global domain only"

upvoted 2 times

RayHK 1 year, 2 months ago

this link have a clear table about the update for scope of domain

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html

upvoted 1 times

tanri04 1 year, 3 months ago

The correct answer is B. Local import of intrusion rules should be applied outside of the Global Domain.

In a multi-tenant deployment, the Global Domain applies to all tenants, while each tenant has its own domain with its own policies, objects, and configurations. If a minor upgrade or a major upgrade is applied, it should be done globally and affects all tenants. Similarly, the Cisco Geolocation Database should be updated globally as it applies to all tenants.

However, intrusion rules can be specific to a tenant's needs and should be imported locally in the tenant's domain to ensure that only the desired rules are applied to that tenant's traffic.

upvoted 2 times

minon_bob 1 year, 6 months ago

Selected Answer: B

In a multidomain deployment, you can import local intrusion rules in any domain. You can view local intrusion rules imported in the current domain and ancestor domains.

upvoted 1 times

xziomal9 2 years ago

Selected Answer: B

Correct answer is: B

upvoted 1 times

anwar1 2 years, 1 month ago

Selected Answer: B

Answer C has no reference as well, B looks more accurate as per below Cisco guide.

upvoted 1 times

anwar1 2 years, 1 month ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/system_software_updates.html

upvoted 1 times

kj2022 2 years, 1 month ago

Selected Answer: B

the answer is B

upvoted 1 times

⊟ **hz033** 2 years, 1 month ago

Selected Answer: B

B sounds OK

upvoted 1 times

⊟ **trickbot** 2 years, 4 months ago

Selected Answer: B

geo IP data and software updates are global only

upvoted 1 times

⊟ **joister** 3 years ago

B is correct answer.

upvoted 1 times

⊟ **Bobster02** 3 years ago

100% agree. B is the only correct answer.

upvoted 1 times

⊟ **kakakayayaya** 3 years ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/system_software_updates.html

B fits better

In a multidomain deployment, you can import local intrusion rules in any domain. You can view local intrusion rules imported in the current domain and ancestor domains.

upvoted 4 times

Question #25 *Topic 1*

An organization has a compliancy requirement to protect servers from clients, however, the clients and servers all reside on the same Layer 3 network. Without readdressing IP subnets for clients or servers, how is segmentation achieved?

A. Change the IP addresses of the servers, while remaining on the same subnet.

B. Deploy a firewall in routed mode between the clients and servers.

C. Change the IP addresses of the clients, while remaining on the same subnet.

D. Deploy a firewall in transparent mode between the clients and servers.

Suggested Answer: *D*

Community vote distribution

D (57%) B (43%)

jmosilva Highly Voted 4 years ago

Agree 100%. D should be the answer

upvoted 9 times

kakakayayaya Highly Voted 4 years ago

B is a silly. We can't route same subnet.

D is better.

upvoted 7 times

hz033 3 years, 1 month ago

But it did not say the same subnet !!! , subnets on same layer 3 network, this is tricky

upvoted 4 times

Weyland 2 years, 7 months ago

"clients and servers all reside on the same Layer 3 network". That's the same subnet.

upvoted 1 times

houhou12322 Most Recent 9 months, 3 weeks ago

Is it possible that we need VRF to segment the networks?

In this case may be B is correct, we need routed interfaces.

upvoted 1 times

Luke4 1 year, 5 months ago

Selected Answer: D

A,C:"change the IP addresses...." but we can't change IP addresses

B:"Deploy a firewall in routed mode between servers and clients" but them are in the same subnet.

We need to protect servers FROM clients in same subnet (layer2).

We can inspect traffic in L2 in transparent mode with a bridge group: servers after an interface and clients after the otherone with firewall inspection between

IMHO the answer is D

upvoted 3 times

bofu 1 year, 6 months ago

Selected Answer: D

B will need readdressing of subnets

upvoted 1 times

achille5 1 year, 10 months ago

Selected Answer: B

Correct is B, transparent operates in L2.

upvoted 2 times

achille5 1 year, 5 months ago

changed to D.https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

upvoted 1 times

gc999 2 years ago

Selected Answer: B

What is the difference between "clients and servers all reside on the same Layer 3 network" and "clients and servers all reside on the same Layer 2 network"? If question is "on the same Layer 2 network", then I may choose D.
Here I will choose B.

upvoted 2 times

ureis 2 years, 2 months ago

Why configure transparent if the network using Layer 3 already ?

upvoted 1 times

Cokamaniako 2 years, 1 month ago

All devices are in the same network

upvoted 1 times

ureis 2 years, 2 months ago

The correct answer is B.

By deploying a firewall in routed mode between the clients and servers, traffic can be filtered based on specific criteria, such as source and destination IP addresses, port numbers, and protocol types. This creates a barrier between the clients and servers, preventing unauthorized access and ensuring compliancy requirements are met.

Option A, changing the IP addresses of the servers, would require reconfiguration of all servers and applications that rely on the original IP addresses, which can be a time-consuming and error-prone process.

Option C, changing the IP addresses of the clients, would also require reconfiguration of all clients and devices that rely on the original IP addresses, which can also be a time-consuming and error-prone process.

Option D, deploying a firewall in transparent mode, would not provide the necessary segmentation between the clients and servers as it would only monitor traffic without being able to filter it based on specific criteria.

upvoted 1 times

tanri04 2 years, 3 months ago

A firewall in transparent mode can be used to segment clients and servers while still using the same IP subnet. This is because a transparent firewall does not modify the IP addresses of the packets, it just inspects them and makes forwarding decisions based on the layer 2 information. Therefore, the clients and servers can remain on the same subnet, but the firewall can be used to filter and control the traffic between them.

So, the correct answer is A. Deploy a firewall in transparent mode between the clients and servers.

upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: D

D. Deploy a firewall in transparent mode between the clients and servers.

Transparent mode firewall deployment can provide layer 2 segmentation between clients and servers without requiring any IP address reconfiguration. The firewall operates as a bridge, filtering traffic between the two segments based on the configured policies. This allows the clients and servers to remain on the same Layer 3 network while still providing a level of segmentation to meet the compliancy requirement.

upvoted 1 times

Aarow 2 years, 9 months ago

Selected Answer: D

Same subnet, we need a layer two solution, no Routing. Correct answer is D

upvoted 2 times

xziomal9 3 years ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

rolmok 3 years, 1 month ago

Selected Answer: D

same layer 3 network mean same subnet

upvoted 1 times

anwar1 3 years, 1 month ago

Selected Answer: D

Agree D is correct based on below explanation:

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place. Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the Firepower Threat Defense device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other

upvoted 1 times

hz033 3 years, 1 month ago

Selected Answer: B

It’s pretty much a trick question

The clients and servers all reside on the same Layer 3 network - Same layer 3 network but it's not say "same subnet" so

Without readdressing IP subnets for clients or servers - so it says subnetS no subnet!

So we can conclude there are minimum two subnets (same and one layer 3 network) so the routed mode is OK and B is correct

upvoted 4 times

Reece_S 3 years, 1 month ago

B. It says they are on the same layer 3 network but not the same subnet. "readdressing IP subnets for clients or servers" Subnets is plural.

upvoted 2 times

outlawww 2 years, 5 months ago

"readdressing IP subnets for clients or servers" can also mean segmenting existing subnet, which effectively means decreasing the IP subnet size by changing the subnet mask on clients and servers, assuming that clients and servers IP's are grouped enough that this is achievable. since they don't want to do that, the only option is transparent mode (answer D), since clients and servers communicate directly.

upvoted 1 times

Question #26 *Topic 1*

Network traffic coming from an organization's CEO must never be denied. Which access control policy configuration option should be used if the deployment engineer is not permitted to create a rule to allow all traffic?

A. Change the intrusion policy from security to balance.

B. Configure a trust policy for the CEO.

C. Configure firewall bypass.

D. Create a NAT policy just for the CEO.

Suggested Answer: *B*

Community vote distribution

B (100%)

Joe_Blue 9 months, 3 weeks ago

Selected Answer: B

The correct answer is B. Configure a trust policy for the CEO.

A trust policy is a special type of access control policy that identifies trusted hosts and networks that are exempt from certain intrusion policies. By creating a trust policy for the CEO, the engineer can ensure that traffic coming from the CEO is always allowed, regardless of any other rules or policies that may be in place. This is a more targeted and specific solution than simply changing the intrusion policy or creating a general firewall bypass. NAT policies, while useful for translating IP addresses, do not provide the same level of control over traffic as access control policies.

upvoted 2 times

Bobster02 2 years, 6 months ago

Answer B is still the most appropriate. Sometimes examiners may use the wrong definition, like probably in this case. It happened before.

upvoted 4 times

kakakayayaya 2 years, 7 months ago

A is not appropriate choice too. Connectivity over Security and personal CEO's rule would be perfect solution but we do not have such answer......

upvoted 2 times

kakakayayaya 2 years, 7 months ago

Vague question and answer.
Trust is an ACTION and is NOT a POLICY.

upvoted 3 times

Question #27 *Topic 1*

What is a characteristic of bridge groups on a Cisco FTD?

A. In routed firewall mode, routing between bridge groups is supported.

B. Routing between bridge groups is achieved only with a router-on-a-stick configuration on a connected router.

C. In routed firewall mode, routing between bridge groups must pass through a routed interface.

D. In transparent firewall mode, routing between bridge groups is supported.

Suggested Answer: *A*

Community vote distribution

A (100%)

14a1949 5 months, 2 weeks ago

Selected Answer: A

According to the Cisco documentation, in routed firewall mode, bridge group traffic can indeed be routed to other bridge groups or routed interfaces. Therefore, the correct answer is:

A. In routed firewall mode, routing between bridge groups is supported.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

Actually, the correct answer is:

C. In routed firewall mode, routing between bridge groups must pass through a routed interface.

This characteristic ensures that even in routed firewall mode, bridge groups function in a way that traffic must pass through a routed interface for inter-group communication.

If you have more questions or need further clarification, feel free to ask!

upvoted 3 times

Weyland 9 months ago

Answer is A. "Bridge group traffic can be routed to other bridge groups or routed interfaces."
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#ID-2106-000000ae

upvoted 1 times

BorZol 9 months, 2 weeks ago

Reference is about ASA. But the question is about FTD.

upvoted 1 times

hz033 1 year, 1 month ago

Selected Answer: A

In routed mode, you can have one or more isolated bridge groups like in transparent mode, but also have normal routed interfaces as well for a mixed deployment.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/configuration/general/asa-99-general-config/intro-fw.html#ID-2106-0000000a

upvoted 1 times

liqucika 1 year, 5 months ago

Selected Answer: A

In routed mode: The BVI acts as the gateway between the bridge group and other routed interfaces. To route between bridge groups/routed interfaces, you must name the BVI. For some interface-based features, you can use the BVI itself.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.pdf

upvoted 4 times

⊟ **SLVan** 1 year, 5 months ago

The correct rep. is B

upvoted 1 times

⊟ **ion123** 1 year, 5 months ago

why given answer " A. In routed firewall mode, routing between bridge groups is supported." is not correct?

upvoted 2 times

Question #28 *Topic 1*

A Cisco FTD device is running in transparent firewall mode with a VTEP bridge group member ingress interface. What must be considered by an engineer tasked with specifying a destination MAC address for a packet trace?

A. The output format option for the packet logs is unavailable.

B. Only the UDP packet type is supported.

C. The destination MAC address is optional if a VLAN ID value is entered.

D. The VLAN ID and destination MAC address are optional.

Suggested Answer: *C*

Community vote distribution

C (100%)

Cokamaniako Highly Voted 1 year, 1 month ago

Selected Answer: C

If the Firepower Threat Defense device is running in transparent firewall mode, and the ingress interface is VTEP, Destination MAC Address is required if you enter a value in VLAN ID. Whereas if the interface is a bridge group member, Destination MAC Address is optional if you enter a VLAN ID value, but required if you do not enter a VLAN ID value.

If the Firepower Threat Defense is running in routed firewall mode, VLAN ID and Destination MAC Address are optional if the input interface is a bridge group member

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

upvoted 7 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: C

When specifying a destination MAC address for a packet trace on a Cisco FTD device running in transparent firewall mode with a VTEP bridge group member ingress interface, the engineer must consider that:

C. The destination MAC address is optional if a VLAN ID value is entered1.

This allows for flexibility in specifying the necessary details for the packet trace.

upvoted 1 times

z6st2a1jv 8 months, 2 weeks ago

Selected Answer: D

The following tables provide full information pertaining to the interface-dependent behavior of VLAN identity and Destination MAC address in transparent and routed firewall modes respectively.

Transparent firewall mode :
Interface: Management
VLAN: Enabled (Optional)
Destination MAC address: Disabled

Interface: VTEP
VLAN: Enabled (Optional)
Destination MAC address: Disabled. When the user enters a value in VLAN, the Destination MAC address is enabled but is optional.

Interface: Bridge Virtual Interface (BVI)
VLAN: Enabled (Optional)

Destination MAC address: Enabled (Mandatory). When the user enters a value in VLAN, the Destination MAC address is optional.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/pa-pn-commands.html

upvoted 4 times

tanri04 1 year, 3 months ago

When an interface is in a bridge group, specifying a destination MAC address is optional as long as a VLAN ID value is provided. So the correct answer is indeed A: "The destination MAC address is optional if a VLAN ID value is entered."

upvoted 1 times

tanri04 1 year, 3 months ago

answer:C

upvoted 1 times

Mevijil 1 year, 6 months ago

Selected Answer: C

Given answer is correct - as long as an interface is in a bridge group, Destination MAC is optional if you provide a VLAN ID value.

upvoted 1 times

Question #29 *Topic 1*

With Cisco FTD software, which interface mode must be configured to passively receive traffic that passes through the appliance?

A. ERSPAN

B. firewall

C. tap

D. IPS-only

Suggested Answer: *C*

Community vote distribution

C (47%) | D (28%) | A (25%)

⊟ **SegaMasterSystemAdmin** Highly Voted 👍 2 years ago

Selected Answer: C

IDS is passive but IPS is not, with IPS the inline traffic can be dropped. I go with tap

upvoted 7 times

⊟ **trickbot** Highly Voted 👍 3 years, 4 months ago

Selected Answer: D

We're screwed with this question. The correct answer depends on whether the question is based on the FMC configuration Guide, or the FMC GUI user interface.

If this question comes from the FMC configuration Guide, the answer could very well be D - IPS-only mode. According to the first sentence of the "INTERFACE MODES AND TYPES" section of The FMC configuration manual:
"You can deploy FTD interfaces in two modes: Regular firewall mode and IPS-only mode." TAP mode would be an Advanced setting on an interface in IPS-only mode.

If this question is based on the FMC GUI, then there are three modes available. Two mode choices on Firewall mode interfaces. Default is mode:none, but mode can be set to passive mode, or ERSPAN mode. There is one mode on an inline pair interface, "Tap mode" found in the advanced options.

And to muddy the waters even more, ERSPAN could also be the correct answer because ERSPAN traffic is passive copies of traffic that doesnt go through the device, but the original traffic still has to go out somewhere, and that somewhere is probably through that ftd's firewall mode interfaces.

I'm undecided between IPS-only mode, and TAP mode.

upvoted 6 times

⊟ **14a1949** Most Recent ⏲ 5 months, 3 weeks ago

Selected Answer: D

For Cisco FTD software, the correct interface mode to passively receive traffic is IPS-only mode (option D). This mode allows the appliance to monitor and analyze traffic without actively participating in the traffic flow.

Tap mode (option C) is another passive monitoring option, but it is typically used in inline deployments where the device is physically inserted into the network path. In contrast, IPS-only mode is specifically designed for passive monitoring without affecting the traffic flow.

upvoted 1 times

⊟ **Silexis** 4 months, 3 weeks ago

IPS is a deployment type and NOT an interface mode

upvoted 1 times

⊟ **xBojmir215x** 6 months ago

Selected Answer: D

It's gotta be D, IPS-only. Of the interface modes, there's Routed, Passive and ERSPAN. Tap is a mode that's used with inline tap or inline set. IPS-only is NOT an interface mode, however it can be configured to allow traffic to flow through an interface passively, as counterintuitive as that might seem.

upvoted 1 times

⊟ **Silexis** 4 months, 3 weeks ago

IPS is a deployment type and NOT an interface mode

TAP is an interface deployment mode, of IPS

upvoted 1 times

Doris8000 11 months ago

Agree it should be D as the TAP woulnd't let the traffic pass

upvoted 1 times

gwb 1 year, 4 months ago

I don't understand why Cisco exam is doing this tricky question. Although I don't like this kind of question, I think I am going to choose IPS-Only mode. like trickbot explained very well below. I am more focusing higher interface mode (firewall vs IPS-mode) although TAP and ERSPAN are also possible answers.

upvoted 1 times

achille5 1 year, 11 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/fpmc-config-guide-v622_chapter_01111001.html

upvoted 2 times

achille5 1 year, 1 month ago

https://rayka-co.com/lesson/cisco-firepower-deployment-modes/

upvoted 1 times

bassfunk 1 year, 11 months ago

Selected Answer: A

I wish there was a way to upload pics to these boards. I'm looking at the FMC right now and the only interface modes are passive, ERSPAN or none. I'm going with ERSPAN. Some of you might be going off of old guides based on older versions of the software. I'm using FMC7.2.

upvoted 4 times

killian64 1 year, 11 months ago

A - ERSPAN. If we're talking interface type, ERSPAN is the only option here. tap is a setting on on inline set (which isn't an interface type).

upvoted 2 times

Silexis 4 months, 3 weeks ago

ERSPAN is not of traffic passing through the appliance but a traffic received in IDS mode from different distant devices separated by Layer 3

upvoted 1 times

Marco_Vela03 2 years, 1 month ago

D is correct, IPS-Only is an interface mode. Tap mode is a type of interface mode can be deployed:

IPS-only interfaces can be deployed as the following types

upvoted 1 times

saad_SEIU 2 years, 2 months ago

Selected Answer: A

I would go with ERSPAN, this is a Passive interface with encapsulating mode.

TAP is a copy of the traffic.

upvoted 3 times

Joe_Blue 2 years, 3 months ago

Selected Answer: C

The correct answer is C, tap. The tap mode is used for passive monitoring of traffic without affecting the traffic flow. The traffic is simply copied to the tap interface for analysis, while the original traffic continues to its destination.

upvoted 3 times

Weyland 2 years, 9 months ago

Selected Answer: D

From the start, only two answers are possible. B and D. There are only two interface modes on FTD, "You can deploy FTD interfaces in two modes: Regular firewall mode and IPS-only mode. You can include both firewall and IPS-only interfaces on the same device. IPS-only interfaces can be deployed as the following types: Inline Set, with optional Tap mode". So you could have IPS-only as inline with tap that would make it into IDS and therefore passive. Firewall interface mode can be deployed as Routed or Bridge Groups with BVI. Do your own reading here: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/interface_overview_for_firepower_threat_defense.html

upvoted 3 times

Weyland 2 years, 9 months ago

And you could also set an IPS-only interface to passive to boot.

upvoted 1 times

Joninjimbo 1 year, 8 months ago

Agree with D according to the Cisco docs. IPS-only mode selected means you can use inline tap which satisfies the question criteria.

Updated link for version 7.0 here which still holds true:
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/interface_overview_for_firepower_threat_defense.html

upvoted 1 times

BorZol 2 years, 9 months ago

TAP interface is not copy any traffic to other interface. Just received it. (Passive)
IPS-only the correct. —An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the system to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

upvoted 1 times

ureis 2 years, 2 months ago

A TAP is a network device that copies and transfers traffic to
another system. Unlike a SPAN port on a switch, which is configured
at the software level, a network TAP is dedicated hardware that is
designed to replicate and transfer traffic.

upvoted 1 times

dique 2 years, 10 months ago

Selected Answer: C

Correct answer: C

upvoted 3 times

johanhc20 2 years, 11 months ago

Selected Answer: C

Correct C
With tap mode, the FTD is deployed inline, but the network traffic flow is undisturbed. Instead, the FTD makes a copy of each packet so that it can analyze the packets. Note that rules of these types do generate intrusion events when they are triggered, and the table view of intrusion events indicates that the triggering packets would have dropped in an inline deployment. There are benefits to using tap mode with FTDs that are deployed inline

upvoted 3 times

Soter 2 years, 11 months ago

of the "Interface modes" the only valid answers is "TAP" or "ERSPAN" Tap is passive and traffic is not going through the FTD, but with ERSPAN it does. Further there is no "IPS-only" mode on interface. if any discussion about "xxx-only" mode is shout be "IDS-only" mode and that would be a passive interface mode

upvoted 1 times

Grandslam 2 years, 11 months ago

With Cisco FTD software, ****which interface mode**** must be configured to passively receive traffic that passes through the appliance?

You can deploy FTD interfaces in two modes: Regular firewall mode and IPS-only mode.

D

upvoted 2 times

Question #30 *Topic 1*

An engineer is monitoring network traffic from their sales and product development departments, which are on two separate networks. What must be configured in order to maintain data privacy for both departments?

A. Use passive IDS ports for both departments.

B. Use a dedicated IPS inline set for each department to maintain traffic separation.

C. Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation.

D. Use one pair of inline set in TAP mode for both departments.

Suggested Answer: *A*

Community vote distribution

C (47%) A (41%) 12%

⊟ **Bobster02** Highly Voted 4 years ago

Agree 100%: B is the only logical choice.

upvoted 9 times

⊟ **Cokamaniako** 2 years, 1 month ago

Why?
Use a dedicated IPS for each departament is most expesive.
The better is configure one pair interfaces inline set for echa departament

I go for D

upvoted 2 times

⊟ **netwguy** Highly Voted 3 years, 10 months ago

The phrasing of answer D is terrible. "Use one pair of inline set in TAP mode for both departments". If what is meant is a dedicated pair for each department (two pairs, 4 interfaces), then Answer D is a correct answer (tap for monitoring). If what is meant is only one pair for both networks, then answer D is incorrect, and Answer B more appropriate. Also, note that by "dedicated IPS inline set", what is meant is likely IPS-only, which makes sense for monitoring as well. I will be answering B if this one pops up.

upvoted 5 times

⊟ **Andy0724** Most Recent 4 months ago

Selected Answer: D

as the wording of monitoring.

upvoted 1 times

⊟ **14a1949** 5 months, 2 weeks ago

Selected Answer: C

I understand why you might think that, but using passive IDS ports (option A) would only allow for monitoring traffic without actively managing or separating it. This wouldn't ensure data privacy between the two departments.

Using 802.1Q inline set Trunk interfaces with VLANs (option C) is the best choice because it allows for logical separation of traffic, ensuring that data from the sales and product development departments remain private and secure.

upvoted 1 times

⊟ **14a1949** 5 months, 3 weeks ago

Selected Answer: B

Using passive IDS ports (option A) can monitor traffic without actively interfering, but it doesn't inherently ensure data privacy between departments.

To maintain data privacy for both departments, option B (using a dedicated IPS inline set for each department) is the best choice. This setup ensures that traffic from each department is monitored separately, maintaining privacy and security for both networks.

Option C (using 802.1Q inline set Trunk interfaces with VLANs) is also a valid approach for logical separation, but it may not offer the same level of dedicated security and privacy as using separate IPS inline sets.

So, while option A can monitor traffic passively, option B is generally preferred for maintaining strict data privacy and security.

upvoted 2 times

Doris8000 11 months ago

not sure how the traffic is gonna be monitored with the 802.1Q inline set Trunk

upvoted 1 times

zbeugene7 1 year, 8 months ago

It' D which is correct, A, B and C is incorrect. Check this out : https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/200924-configuring-firepower-threat-defense-int.html

upvoted 1 times

achille5 1 year, 11 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/fpmc-config-guide-v622_chapter_01111001.html

upvoted 1 times

> **achille5** 1 year, 6 months ago
>
> changed answer to C.
>
> upvoted 1 times
>
> > **achille5** 1 year, 5 months ago
> >
> > Final ans D
> >
> > upvoted 1 times

gc999 2 years ago

Selected Answer: A

Using Passive Mode for these two department which just only consume two interfaces. While all the other options would consume four interfaces. Besides, Passive Mode is configured on interface level, it can highly prevent policy misconfiguration on applying Access Control Policy with drop action, traffic redirection, SSL Encryption, etc., which can provide confidence to users.

upvoted 1 times

greeklover84 2 years ago

Selected Answer: C

for me C makes sense.

upvoted 2 times

bobie 2 years ago

Selected Answer: C

Non-complicated answer is C.

upvoted 3 times

tanri04 2 years, 3 months ago

Answer A, which suggests using a dedicated IDS inline set for each department to maintain traffic separation, is a better choice for passively monitoring and separating the two departments. Using an IDS instead of an IPS avoids the risk of accidentally blocking legitimate traffic, while still allowing for monitoring and detection of potential threats. Additionally, using dedicated inline sets for each department ensures that their traffic is kept separate and prevents any accidental leakage of sensitive information between the two departments.

upvoted 2 times

> **bassfunk** 1 year, 10 months ago
>
> It doesn't say inline set though. It says IDS ports. Which i'm imagining is just a standard port configuration with snort enabled for IDS. The two departments would still be able to route to each other. The vlan approach sounds best.
>
> upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: C

C. Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation.

By using 802.1Q inline set trunk interfaces with VLANs, each department can be isolated on separate VLANs while still passing through the same FTD device. This allows for logical separation of network traffic while maintaining data privacy for each department. Using a dedicated IPS inline set for each department would require multiple FTD devices, and using one pair of inline set in TAP mode for both departments would not provide sufficient network isolation. Using passive IDS ports would not allow for any traffic to be blocked, which could lead to security vulnerabilities.

upvoted 2 times

tanri04 2 years, 4 months ago

C. Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation.

To maintain data privacy for both departments, the engineer should use logical traffic separation using VLANs. By configuring 802.1Q trunk interfaces with VLANs, the engineer can separate the traffic from the two departments into different VLANs, which will keep the traffic from each department separate and secure.

Option A is not a viable solution for maintaining data privacy as passive IDS ports only monitor network traffic and do not provide any separation or protection.

Option B is also not the best solution as dedicated IPS inline sets can be expensive and difficult to manage for multiple departments, and can potentially introduce additional latency or points of failure.

Option D is not recommended as it will allow both departments to receive the same traffic and potentially expose sensitive information to both parties.

upvoted 1 times

dique 2 years, 10 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

xziomal9 3 years ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

hz033 3 years, 1 month ago

Selected Answer: C

Use 802.1Q inline set Trunk interfaces with VLANs to maintain logical traffic separation

upvoted 1 times

Question #31 *Topic 1*

A hospital network needs to upgrade their Cisco FMC managed devices and needs to ensure that a disaster recovery process is in place. What must be done in order to minimize downtime on the network?

A. Configure a second circuit to an ISP for added redundancy.

B. Keep a copy of the current configuration to use as backup.

C. Configure the Cisco FMCs for failover.

D. Configure the Cisco FMC managed devices for clustering.

Suggested Answer: *D*

Community vote distribution

D (47%) B (33%) C (20%)

d0980cc 2 months, 2 weeks ago

Selected Answer: C

I'm going with C. I think Cisco is purposely throwing a curve ball with "failover", which is an element of HA.
https://www.cisco.com/c/en/us/solutions/hybrid-work/what-is-high-availability.html#~infrastructure-elements

upvoted 1 times

14a1949 5 months, 2 weeks ago

Selected Answer: D

Both options C and D are valid for minimizing downtime and ensuring disaster recovery, but they serve slightly different purposes:

Option C: Configure the Cisco FMCs for failover - This ensures that if one FMC fails, another can take over, providing redundancy and minimizing downtime.
Option D: Configure the Cisco FMC managed devices for clustering - This allows multiple devices to work together, sharing the load and providing redundancy, which can be more effective in maintaining continuous network operation.
If you need to choose one, option D (clustering) generally offers a more robust solution by providing load balancing and redundancy. However, if your primary concern is simply having a backup device ready to take over, option C (failover) is also a strong choice.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

While **D. Configure the Cisco FMC managed devices for clustering** can enhance performance and provide redundancy, the most effective solution for minimizing downtime during a disaster recovery process is:

C. Configure the Cisco FMCs for failover.

Failover configuration ensures that if one FMC fails, the other can take over seamlessly, thereby minimizing network downtime and ensuring continuous management and operation of the network.

If you have any more questions or need further clarification, feel free to ask!

upvoted 2 times

Thusi26 7 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/backup_and_restore.html

upvoted 1 times

Aransi90 1 year, 7 months ago

Selected Answer: D

Managed device* and to ensure no downtime, it is the managed devices passing users traffic not the FMC

upvoted 4 times

brightfox99 1 year, 11 months ago

Selected Answer: B

Outlines to backup for a disaster:

https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide/upgrade_firepower_threat_defense.html

upvoted 1 times

gc999 2 years ago

Selected Answer: B

Seems "B" is the best answer. Not sure the question is on FMC or its managed devices, but I assume it is the managed devices.

C - FMC Failover cannot help for the downtime.

D - Managed Devices Clustering, as far as I know, not all the devices can support clustering. Clustering is not the same has HA.

upvoted 2 times

Gabranch 2 years, 1 month ago

Selected Answer: D

The upgrade is happening on FMC managed devices - Firewalls/IPSs

Having the FMCs in HA does nothing for network uptime. You can shud down a stand-alone FMC managing 30 FTDs and network traffic still flows.

Using clustering on the FTDs allows for upgrading the managed devices with minimal downtime.

upvoted 3 times

Initial14 2 years, 3 months ago

In Cisco's documentation disaster recovery means backup

upvoted 2 times

Joe_Blue 2 years, 3 months ago

Selected Answer: C

To minimize downtime on the network during an upgrade and to ensure a disaster recovery process is in place, the hospital network should configure the Cisco FMC managed devices for failover. herefore, configuring the Cisco FMCs for failover is the best option as it provides a mechanism for automatic failover in the event of a failure during the upgrade of the Cisco FMC managed devices. This ensures that the network remains operational even in the event of an unexpected failure, minimizing downtime and ensuring business continuity.

upvoted 3 times

tanri04 2 years, 4 months ago

D. Configure the Cisco FMC managed devices for clustering.

To minimize downtime on the network during an upgrade, the hospital network should configure the Cisco FMC managed devices for clustering. Clustering allows multiple FMC devices to be managed as a single entity, providing redundancy and load sharing. If one device in the cluster fails or needs to be taken offline for maintenance, the other devices can continue to operate, minimizing downtime.

upvoted 3 times

xziomal9 3 years ago

Selected Answer: B

Correct answer is: B

upvoted 2 times

> **tanri04** 2 years, 4 months ago
>
> Option B (keep a copy of the current configuration to use as backup) is important, but it is not sufficient for disaster recovery. A disaster recovery process should include not only backup configuration files, but also a plan for how to quickly restore the FMC devices to operational status in the event of a failure.
>
> upvoted 1 times

trickbot 3 years, 4 months ago

This question is about recovering from a disastrous software upgrade on an FTD or other firepower device, and NOT the FMC appliance. C -configure FMC for failover, is the trick answer (examtopics folks fell for it. haha). We're upgrading the managed devices, not the FMC, so the FMC isnt going to fail the upgrade. If your upgrade turns into a disaster and the devices dont comeback up, you got downtime, and its all about those backups.

upvoted 3 times

orotta 3 years, 4 months ago

I have noticed in the question "in order to minimize downtime on the network?" there is no downtime when you have FMC failover.

To minimize downtime, in case the upgrade fails, you should have FMC backup so I strongly believe the correct answer is B

upvoted 3 times

orotta 3 years, 5 months ago

Simply by looking at the choices, the answer looks C but when you read carefully, the keywords are Disaster Recovery, so the answer should be B. I excerpted from Cisco Site "As part of your disaster recovery plan, we recommend that you perform periodic backups to a secure remote location."

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/backup_and_restore.html

upvoted 1 times

⊟ **netwguy** 3 years, 10 months ago

Correct answer is likely B.

D: No, we cant cluster the devices, as they might have different functions - cant just cluster (with the (lack of) info we are given).

C: No, FMC failover wont minimize downtime.

B: Yes, if a device fails its update/upgrade, or crashes for some reason during the update, then we have a means to restore the device, or another device if replacement is needed.

A: Just silly

upvoted 1 times

⊟ **anonymous1334232** 3 years, 11 months ago

Option is for D

upvoted 3 times

Question #32 *Topic 1*

An organization has implemented Cisco Firepower without IPS capabilities and now wants to enable inspection for their traffic. They need to be able to detect protocol anomalies and utilize the Snort rule sets to detect malicious behavior. How is this accomplished?

A. Modify the network discovery policy to detect new hosts to inspect.

B. Modify the access control policy to redirect interesting traffic to the engine.

C. Modify the intrusion policy to determine the minimum severity of an event to inspect.

D. Modify the network analysis policy to process the packets for inspection.

Suggested Answer: *B*

Community vote distribution

B (80%) D (20%)

14a1949 5 months, 2 weeks ago

Selected Answer: B

I understand why you might think option D is correct. However, B. Modify the access control policy to redirect interesting traffic to the engine is actually the most appropriate choice in this scenario.

The access control policy is where you specify which traffic should be inspected by the Firepower Threat Defense (FTD) engine. By redirecting interesting traffic to the inspection engine, you ensure that protocol anomalies are detected and Snort rule sets are applied to identify malicious behavior.

Modifying the network analysis policy (D) does involve processing packets for inspection, but it primarily focuses on pre-processing and detection of protocol anomalies at a more basic level, rather than leveraging the full capabilities of Snort rules for detecting malicious behavior.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: D

I understand your perspective. Modifying the access control policy to redirect interesting traffic to the engine (option B) is indeed important for defining which traffic should be inspected.

However, to specifically enable inspection for protocol anomalies and utilize Snort rule sets to detect malicious behavior, modifying the network analysis policy (option D) is the correct approach. The network analysis policy processes packets for inspection, allowing the detection of protocol anomalies and the application of Snort rule sets1.

Modifying the access control policy (option B) is crucial for directing traffic to be inspected, but the actual inspection for anomalies and malicious behavior is handled by the network analysis policy.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: B

To enable inspection for traffic on a Cisco Firepower device without IPS capabilities and utilize Snort rule sets to detect malicious behavior, the correct action would be:

B. Modify the access control policy to redirect interesting traffic to the engine.

By modifying the access control policy, you can specify which traffic should be inspected by the Firepower device, allowing it to detect protocol anomalies and utilize Snort rule sets for identifying malicious behavior.

upvoted 1 times

Aransi90 1 year, 1 month ago

Selected Answer: B

B is the way to achieve this

upvoted 1 times

Joninjimbo 1 year, 2 months ago

Selected Answer: B

The traffic flow diagram in the guide below proves its B. The last thing it hits in the firewall which determines whether the traffic is sent to the IPS/IDS is the L3/L4 ACP. So its definitively B.

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

upvoted 1 times

achille5 1 year, 4 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/fdm/fptd-fdm-config-guide-670/fptd-fdm-intrusion.html

upvoted 1 times

achille5 12 months ago

Changed B

upvoted 1 times

Initial14 1 year, 8 months ago

Selected Answer: B

B. If you do not have preprocessor enabled, lets say SCADA but you have snort rules enabled for SCADA protocols SNORT will enable preprocessor for SCDA, so the only option is B

upvoted 3 times

tanri04 1 year, 9 months ago

To enable inspection for traffic and detect protocol anomalies and utilize the Snort rule sets to detect malicious behavior, the intrusion policy must be modified.

The intrusion policy determines which traffic is inspected and which Snort rules are used to detect malicious behavior. By default, when Firepower is installed, it uses a basic intrusion policy that does not have IPS capabilities. Therefore, modifying the intrusion policy is the correct solution to enable inspection for traffic and utilize the Snort rule sets.

So, the correct answer is C. Modify the intrusion policy to determine the minimum severity of an event to inspect.

upvoted 1 times

tanri04 1 year, 9 months ago

To enable inspection for traffic and detect protocol anomalies using Snort rule sets to detect malicious behavior in Cisco Firepower without IPS capabilities, both the access control policy and intrusion policy must be modified.

The access control policy should be modified to redirect interesting traffic to the engine for inspection. The intrusion policy should be modified to enable intrusion and file policy, select the Snort rule sets to use for inspection, and configure the protocol inspection settings to detect anomalies.

The minimum severity of an event to inspect is determined by the intrusion policy, but it is not the only modification required to enable inspection for traffic and utilize the Snort rule sets. Therefore, option C is not the correct answer.

The correct answer is: A. Modify the access control policy to redirect interesting traffic to the engine, and C. Modify the intrusion policy to utilize Snort rule sets and detect malicious behavior.

upvoted 2 times

Joe_Blue 1 year, 9 months ago

Selected Answer: B

To enable inspection for traffic and detect protocol anomalies using Snort rule sets in Cisco Firepower without IPS capabilities, the organization needs to modify the access control policy to redirect interesting traffic to the engine. Therefore, the correct answer is option B.

upvoted 2 times

johanhc20 2 years, 5 months ago

Selected Answer: B

B is correct

upvoted 2 times

xziomal9 2 years, 6 months ago

Selected Answer: B

Correct answer is: B

upvoted 1 times

Grandslam 2 years, 9 months ago

Selected Answer: D

I get why people are picking B but I have to go with D. NAP is specific for identifying Anomalies...

upvoted 2 times

liqucika 2 years, 11 months ago

Selected Answer: B

Each rule in the ACP has control over whether the traffic is sent to snort to be inspected or not. If the traffic is allowed and an intrusion policy is selected, then the traffic will go on to be inspected by snort.

upvoted 2 times

Sarbi 3 years, 3 months ago

B is the correct answer.

upvoted 2 times

orotta 2 years, 11 months ago

Can you please explain why B is correct answer

upvoted 1 times

Bobster02 3 years, 6 months ago

B indeed makes more sense:

A network analysis policy (NAP) governs how traffic is decoded and preprocessed so that it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.
To apply intrusion policies to network traffic, you select the policy within an access control rule that allows traffic. You do not directly assign intrusion policies.

upvoted 4 times

kakakayayaya 3 years, 6 months ago

PS We do not need additionally to enable NAP. By default it uses Balances Security and Connectivity config.
So for me answer B is more reasonable.

upvoted 1 times

kakakayayaya 3 years, 6 months ago

Network analysis policy will not work without the access control policy. I see that we need to make B AND D steps.
For me "redirect interesting traffic" most be the most important step....

upvoted 3 times

Question #33 *Topic 1*

An engineer is tasked with deploying an internal perimeter firewall that will support multiple DMZs. Each DMZ has a unique private IP subnet range. How is this requirement satisfied?

A. Deploy the firewall in transparent mode with access control policies

B. Deploy the firewall in routed mode with access control policies

C. Deploy the firewall in routed mode with NAT configured

D. Deploy the firewall in transparent mode with NAT configured

Suggested Answer: *B*

Community vote distribution

B (88%) 13%

houhou12322 9 months, 3 weeks ago

I think the key here is "access policies" plural. an FTD can support only one access controle policy.

The correct answer is C

upvoted 1 times

gwb 1 year, 4 months ago

another tricky question that I don't like. DMZ does NOT mean that we need NAT because internal DMZ without internet access (not NAT) is possible based on question. Thus I will go C

upvoted 2 times

achille5 1 year, 10 months ago

Selected Answer: C

a DMZ concept is partly internal, own by organization. Some set up of organization's web servers that are facing internet reside in DMZ, with NAT configured.

upvoted 1 times

> **achille5** 1 year, 4 months ago
>
> We need to know the meaning of DMZ first by Cisco. Go through this link below.
>
> https://www.cisco.com/c/dam/assets/sol/sb/isa500_emulator/help/guide/ad1681599.html
>
> upvoted 2 times

THEODORABLE 2 years, 1 month ago

what do they mean by "internal perimeter" firewall? my guess is that it is entirely within the private address space so why would it need NAT? but the word perimeter makes me wonder if the person who wrote this meant it to be a site level Internet edge device and they are just bad at describing things.

upvoted 2 times

ureis 2 years, 2 months ago

With Routed Mode you can have each DMZ with different routing table and unique private IP subnet range, ACP can be used to control traffic between the different DMZs, NAT could be used but is not required in this case.

upvoted 2 times

Joe_Blue 2 years, 3 months ago

Selected Answer: B

To support multiple DMZs with unique private IP subnet ranges, the engineer should deploy the firewall in routed mode with access control policies. Therefore, the correct answer is option B. By deploying the firewall in routed mode with access control policies, the engineer can configure the firewall to route traffic between the DMZs and the internal network based on their unique private IP subnet ranges. The access control policies can be used to enforce security policies to control which traffic is allowed between the DMZs and the internal network. This provides a secure and efficient way to manage traffic between the DMZs and the internal network.

upvoted 3 times

felagund 2 years, 4 months ago

Although ACPs seem obvious, the concept of perimeter firewall is generalized as well as the private IP addressing, implying the need for NAT..., as their are no more specific variables.

upvoted 1 times

Weyland 2 years, 9 months ago

A perimeter firewall could mean internet but it does not explicit say internet, so does not explicit say a need for NAT. However it does excplicit ask for support of DMZ:s, and you can't have working DMZs without ACPs. You can have working DMZ:s without NAT. I'd go with B.

upvoted 1 times

Soter 2 years, 11 months ago

I think what we need to look at there is how the question is formed, and it says "Firewall" not FTD, og IPS or firepower. So in pure firewall mode, there is no IDS, so we need to assume that a "Perimiter" firewall is connected to the internet, regardles of the "internal" statement. And so we need NAT configured.

C is the answer

upvoted 2 times

xziomal9 3 years ago

Selected Answer: B

Correct answer is: B

upvoted 2 times

Grandslam 3 years, 3 months ago

This is a horrible question... But you cant have NAT without ACP... Since we can't pick two we will have to go with B.... But I dont like it.

upvoted 2 times

trickbot 3 years, 4 months ago

Selected Answer: B

Answers with NAT are wrong because it's an INTERNAL firewall, so no public routers are in play, the DMZs are all private ranges, and obscurity of IPs isnt beneficial against insiders. You'll definitely need routed interfaces, and access control policies to prevent unsolicited traffic from DMZ to inside.

upvoted 2 times

> **netwguy** 3 years, 3 months ago
>
> Its not possible to assign multiple ACPs to a firewall in a non-multidomain setup. If this was a multidomain setup, the question would/should have stated that. If the question reads "policy" during your test, choose B. If it reads "policies", go with C, as B will be incorrect. Using NAT is not incorrect. Like kaka says, there might be scenarios where u want to use NAT.
>
> upvoted 2 times

kplost 3 years, 9 months ago

I ll go with B , you can have an internal perimeter Firewall with DMZ without NAT but surely ACPs are needed for the low security DMZ zones.

upvoted 1 times

Sarbi 3 years, 9 months ago

The correct answer is B. With ACP we can control the traffic.

C why we need Nat ? Does not make any sense.

upvoted 1 times

netwguy 3 years, 10 months ago

I would have gone for B if the answer had said "access control policy". It does however state "access control policies", and having multiple ACPs for one firewall makes no sense. The question is very bad, as we dont know details on the setup, and scenarios without NAT are possible, but I think the answer is C

upvoted 1 times

> **netwguy** 3 years, 10 months ago
>
> Also, the fact that they point out that the DMZ interfaces do not have public ranges configured tells me that they want the NAT answer "Each DMZ has a unique private IP subnet range".
>
> upvoted 2 times

Javimc 3 years, 10 months ago

Why do you need nat in a internal firewall?

upvoted 1 times

> **kakakayayaya** 3 years, 10 months ago
>
> It just possible solution that satisfy requirements.
>
> upvoted 1 times

Bobster02 3 years, 11 months ago

C has my final vote of confidence.

upvoted 2 times

Question #34 *Topic 1*

An engineer must configure high availability for the Cisco Firepower devices. The current network topology does not allow for two devices to pass traffic concurrently. How must the devices be implemented in this environment?

A. in active/active mode

B. in a cluster span EtherChannel

C. in active/passive mode

D. in cluster interface mode

Correct Answer: *C*

d0980cc 3 months, 1 week ago

Selected Answer: B

Etherchannel would be concurrent

upvoted 1 times

Question #35 *Topic 1*

When deploying a Cisco ASA Firepower module, an organization wants to evaluate the contents of the traffic without affecting the network. It is currently configured to have more than one instance of the same device on the physical appliance. Which deployment mode meets the needs of the organization?

A. inline tap monitor-only mode

B. passive monitor-only mode

C. passive tap monitor-only mode

D. inline mode

Suggested Answer: *A*

Community vote distribution

A (86%) 14%

14a1949 5 months, 2 weeks ago

Selected Answer: A

Option B, passive monitor-only mode, is also a valid approach for evaluating traffic without affecting the network. In this mode, the device monitors traffic passively, meaning it doesn't interfere with the traffic flow, which meets the requirement of not affecting the network.

However, the key difference is that inline tap monitor-only mode (option A) provides visibility into what the ASA FirePOWER module would have done to the traffic if it were actively managing it, without actually impacting the network. This can be particularly useful for evaluating the potential impact of security policies and actions.

upvoted 2 times

tinyJoe 5 months, 3 weeks ago

Selected Answer: B

I agree that the answer is B.
"However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth."

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.html#:~:text=the%20ASA%20does%20apply%20its%20policies%20to%20the%20traffic

upvoted 2 times

tinyJoe 5 months, 3 weeks ago

However, it depends on what is meant by the description “You must operate the ASA in single context transparent mode.

If “single context” means the same thing as “not multi instance”, then the answer would be A.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: B

I can understand why you might think that, but let's clarify the best option. To evaluate the contents of the traffic without affecting the network, the correct deployment mode would be:

B. passive monitor-only mode

In passive monitor-only mode, the Cisco ASA Firepower module can analyze traffic without actively interfering with it, making it ideal for evaluating traffic without impacting the network.

A. inline tap monitor-only mode would still involve placing the device inline, which can affect network traffic flow to some extent.

upvoted 1 times

spambox730 11 months, 2 weeks ago

Selected Answer: A

Passive monitor only (B) could be the answer if there was only 1 instance but the question says there are more tan one.
Thus the second option which does not affect traffic is inline tap monitor only (A)

upvoted 1 times

⊟ **bobie** 1 year ago

Selected Answer: A

Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

upvoted 1 times

⊟ **ureis** 1 year, 2 months ago

A. inline tap monitor-only mode - Affect CPU and hardware intensive

B. passive monitor-only mode - Only monitor the traffic - Correct option

C. passive tap monitor-only mode - Not exist

D. inline mode - Question not asking to copy all the traffic, so not a option here

upvoted 3 times

⊟ **Joe_Blue** 1 year, 3 months ago

Selected Answer: C

The Firepower module can be deployed in either inline mode, passive monitor-only mode, or passive tap monitor-only mode. In this mode, the Cisco ASA Firepower module is configured to passively monitor traffic without introducing any delay or disruption to the network. This is achieved by configuring the module to operate in tap mode, where a copy of the traffic is sent to the module for inspection and analysis, but the original traffic continues to flow uninterrupted.

upvoted 1 times

⊟ **bassfunk** 1 year, 7 months ago

Selected Answer: A

A is correct as inline would drop packets and therefor, affect the network.

upvoted 1 times

⊟ **dique** 1 year, 10 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

⊟ **xziomal9** 2 years ago

Selected Answer: A

Correct answer is: a

upvoted 1 times

⊟ **harshal0408** 2 years, 1 month ago

A is correct

upvoted 1 times

⊟ **Grandslam** 2 years, 3 months ago

Selected Answer: A

A @Orotta is correct

upvoted 1 times

⊟ **trickbot** 2 years, 4 months ago

Thank you @orotta for the reference, and reminder that we are talking about an ASA with firepower module. The answer is A inline TAP

upvoted 1 times

⊟ **orotta** 2 years, 5 months ago

" Let you evaluate the content of the traffic, without impacting the network. "

The question is taken exact sentence from the Cisco site for the Inline tap monitor-only Mode. Please see link below. So A is the correct answer.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.html

upvoted 4 times

⊟ **TLOVE** 2 years, 2 months ago

Orotta, thanks for the link, it confirms the answer is (A) Inline Tap mode

upvoted 1 times

⊟ **jamesque23** 2 years, 7 months ago

A

The problem with B is that in passive monitor-only you cannot have more than one instance.

Passive monitor-only (traffic forwarding) mode—If you want to prevent any possibility of the ASA with FirePOWER Services device impacting traffic, you can configure a traffic-forwarding interface and connect it to a SPAN port on a switch. In this mode, traffic is sent directly to the ASA FirePOWER module without ASA processing. The traffic is dropped, and nothing is returned from the module, nor does the ASA send the traffic out any interface. You must operate the ASA in single context transparent mode to configure traffic forwarding.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/firewall/asa-910-firewall-config/access-sfr.html

upvoted 2 times

⊟ **kj2022** 2 years, 1 month ago

A is right answer

upvoted 1 times

⊟ **elliot67** 2 years, 8 months ago

The tap mode "IS affecting the traffic", so B is correct

upvoted 2 times

⊟ **Bobster02** 3 years ago

Indeed, A fits better.

Inline tap monitor-only mode (ASA inline)—In an inline tap monitor-only deployment, a copy of the traffic is sent to the ASA FirePOWER module, but it is not returned to the ASA. Inline tap mode lets you see what the ASA FirePOWER module would have done to traffic, and lets you evaluate the content of the traffic, without impacting the network. However, in this mode, the ASA does apply its policies to the traffic, so traffic can be dropped due to access rules, TCP normalization, and so forth.

upvoted 2 times

Question #36 *Topic 1*

An organization has a Cisco FTD that uses bridge groups to pass traffic from the inside interfaces to the outside interfaces. They are unable to gather information about neighboring Cisco devices or use multicast in their environment. What must be done to resolve this issue?

A. Create a firewall rule to allow CDP traffic

B. Create a bridge group with the firewall interfaces

C. Change the firewall mode to transparent

D. Change the firewall mode to routed

Suggested Answer: *A*

Community vote distribution

A (44%) C (41%) D (16%)

gc999 Highly Voted 2 years ago

Selected Answer: A

The case already has the bridge group configured, any change of the firewall mode would cause the routing impact. Only option A is acceptable. From the link below, I believe no matter then bridge group is on routed mode or transparent mode, it needs access rule to pass the multicast traffic when using bridge group.

upvoted 8 times

gc999 2 years ago

The link is here

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#ID-2106-0000001e:~:text=Broadcast%20and%20multicast%20traffic%20can%20be%20passed%20using%20access%20rules

upvoted 2 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: C

Creating a firewall rule to allow CDP traffic (option A) might seem like a straightforward solution, but it's important to consider how Cisco Firepower Threat Defense (FTD) operates in different firewall modes.

When the FTD is in routed mode, it functions at Layer 3 and doesn't support CDP (Cisco Discovery Protocol) or multicast traffic by default. Switching the FTD to transparent mode (option C) would enable Layer 2 features, such as CDP and multicast, because in transparent mode, the device acts more like a bridge, allowing Layer 2 traffic to pass through.

So, for full functionality including gathering information about neighboring Cisco devices and supporting multicast traffic, changing the firewall mode to transparent is the most appropriate solution.

upvoted 1 times

TECH3K3 3 weeks, 5 days ago

This is a reply from ChatGPT not that you know anything

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

Changing the firewall mode to routed (option D) would allow the FTD device to participate in Layer 3 routing, which can help with gathering information about neighboring devices and supporting multicast traffic. However, this mode requires each interface to be on a different subnet, which might not align with your current network setup using bridge groups.

On the other hand, changing the firewall mode to transparent (option C) allows the firewall to operate at Layer 2, passing traffic between interfaces without being seen as a router hop. This mode supports protocols like CDP (Cisco Discovery Protocol) and multicast traffic, which are essential for gathering information about neighboring devices and using multicast in the environment.

So, while routed mode (option D) could work, transparent mode (option C) is generally more suitable for environments using bridge groups and needing Layer 2 connectivity.

upvoted 1 times

⊟ **14a1949** 5 months, 3 weeks ago

Selected Answer: C

You are correct! Changing the firewall mode to transparent (option C) would resolve the issue. In transparent mode, the firewall operates at Layer 2, allowing it to pass traffic between interfaces without being seen as a router hop. This mode supports protocols like CDP (Cisco Discovery Protocol) and multicast traffic, which are essential for gathering information about neighboring devices and using multicast in the environmen

upvoted 1 times

⊟ **14a1949** 5 months, 3 weeks ago

Selected Answer: D

I understand your perspective. However, creating a firewall rule to allow CDP traffic (**A**) would only address the discovery of neighboring Cisco devices through CDP. It would not solve the multicast issue in the environment.

To enable both CDP and multicast functionalities, the firewall needs to operate at Layer 3, which is achieved by:

D. Change the firewall mode to routed

Switching to routed mode will allow the Cisco FTD to handle Layer 3 tasks, including CDP and multicast routing, thereby resolving the issues faced by the organization.

If you have any further questions or need more clarification, I'm here to help!

upvoted 1 times

⊟ **devildog** 10 months ago

Selected Answer: D

Guidelines for Multicast Routing
Firewall Mode
Supported only in routed firewall mode. Transparent firewall mode is not supported.

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/multicast_routing_for_firepower_threat_defense.html

upvoted 2 times

⊟ **devildog** 8 months, 1 week ago

Changing my answer to C. Transparent firewall mode

A. seems to be popular, but CDP uses multicast. The question states that both CDP and multicast are not working. This would mean that allowing CDP through the firewall would not fix the underlying issue of multicast not functioning. Transparent mode supports multicast which in turn means CDP should work.

upvoted 1 times

⊟ **squirrelzzz** 11 months, 1 week ago

Selected Answer: C

Allows CDP and multicast by default in transparent mode

upvoted 2 times

⊟ **MB2222** 1 year, 2 months ago

Correct answer is: A

https://community.cisco.com/t5/security-knowledge-base/what-do-you-need-to-know-about-transparent-firewall-asa-or-ftd/ta-p/3773884

NON-IP traffic will be blocked by default in transparent firewall mode.

upvoted 1 times

⊟ **touchy** 1 year, 4 months ago

Selected Answer: A

"In routed mode, some types of traffic cannot pass through the ASA even if you allow it in an access rule. The bridge group, however, can allow almost any traffic through using either an access rule (for IP traffic) or an EtherType rule (for non-IP traffic):

IP traffic—In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL).

Non-IP traffic—AppleTalk, IPX, BPDUs, and MPLS, for example, can be configured to go through using an EtherType rule."

Based on the above, changing the mode to routed will not solve the issue. Furthermore, in transparent mode non-IP traffic is blocked by default. Answer B is the least possible since we already have bridge groups. So we are left with A

upvoted 1 times

achille5 1 year, 10 months ago

Selected Answer: A

Broadcast and multicast traffic can be passed using access rules.

upvoted 1 times

achille5 1 year, 10 months ago

CDP packets are sent to a multicast

upvoted 2 times

bassfunk 1 year, 10 months ago

Selected Answer: A

IP traffic—In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL)

upvoted 3 times

spambox730 1 year, 11 months ago

Selected Answer: A

see gc999 link

upvoted 1 times

ureis 2 years, 2 months ago

This organization use bridge groups already -> Answer B is not correct.
Answer A seems to be not correct as the firewall rule only allows CDP traffic, not multicast.
So only answer C is left.
Note: Bridge groups are supported in both transparent and routed firewall mode.

upvoted 2 times

saad_SEIU 2 years, 2 months ago

Selected Answer: D

Bridge groups can't pass traffic between each others in Transparent mode.

upvoted 2 times

Initial14 2 years, 3 months ago

Selected Answer: A

The firewall is in Transparent mode, but CDP with BVI in transparent mode has no limitation, so there must be rule implemented to allow CDP. For me the answer is A

upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: C

The inability to gather information about neighboring Cisco devices or use multicast in a Cisco FTD environment that uses bridge groups is likely due to the fact that the firewall is operating in routed mode. In order to resolve this issue and enable the necessary features, the firewall mode needs to be changed to transparent mode.

In transparent mode, the firewall operates as a bridge between the two interfaces, allowing multicast traffic to pass through and enabling the organization to gather information about neighboring Cisco devices. In addition, it is not necessary to create a bridge group when operating in transparent mode, as the firewall acts as a transparent bridge between the two interfaces.

upvoted 3 times

Weyland 2 years, 9 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/general/asa-96-general-config/intro-fw.html Search for CDP and do your own reading.

upvoted 2 times

Weyland 2 years, 9 months ago

I mean routed, transparent or bridge groups does not pass CDP. This negates -A, -B and -C.

upvoted 1 times

bassfunk 1 year, 10 months ago

Your own link refutes this. Read the last sentence. The answer is A.

IP traffic—In routed firewall mode, broadcast and multicast traffic is blocked even if you allow it in an access rule, including unsupported dynamic routing protocols and DHCP (unless you configure DHCP relay). Within a bridge group, you can allow this traffic with an access rule (using an extended ACL)

upvoted 2 times

Question #37

Topic 1

A network engineer implements a new Cisco Firepower device on the network to take advantage of its intrusion detection functionality. There is a requirement to analyze the traffic going across the device, alert on any malicious traffic, and appear as a bump in the wire. How should this be implemented?

A. Specify the BVI IP address as the default gateway for connected devices

B. Enable routing on the Cisco Firepower

C. Add an IP address to the physical Cisco Firepower interfaces

D. Configure a bridge group in transparent mode

Suggested Answer: *D*

jamesque23 Highly Voted 7 months ago

D is correct

Traditionally, a firewall is a routed hop and acts as a default gateway for hosts that connect to one of its screened subnets. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices. However, like any other firewall, access control between interfaces is controlled, and all of the usual firewall checks are in place.

Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the ASA uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa97/configuration/general/asa-97-general-config/intro-fw.html

upvoted 5 times

Question #38 *Topic 1*

Which two conditions must be met to enable high availability between two Cisco FTD devices? (Choose two.)

A. same flash memory size

B. same NTP configuration

C. same DHCP/PPoE configuration

D. same host name

E. same number of interfaces

Suggested Answer: *BE*

Bobster02 Highly Voted 3 years, 6 months ago

Disagree with you:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

Conditions

In order to create an HA between 2 FTD devices, these conditions must be met:

Same model
Same version (this applies to FXOS and to FTD - (major (first number), minor (second number), and maintenance (third number) must be equal))
Same number of interfaces
Same type of interfaces
Both devices as part of same group/domain in FMC
Have identical Network Time Protocol (NTP) configuration
Be fully deployed on the FMC without uncommitted changes
Be in the same firewall mode: routed or transparent.
Note that this must be checked on both FTD devices and FMC GUI since there have been cases where the FTDs had the same mode, but FMC does not reflect this.
Does not have DHCP/Point-to-Point Protocol over Ethernet (PPPoE) configured in any of the interface
Different hostname (Fully Qualified Domain Name (FQDN)) for both chassis. In order to check the chassis hostname navigate to FTD CLI and run this command
Therefore original answers are correct: B and E

upvoted 20 times

Gabranch 1 year, 7 months ago

A/E - how would one end up with different flash sizes if they must be the same model? Different flash sizes = different model = no HA.

upvoted 1 times

trudint 1 year, 6 months ago

you're actually confirming Bobster02's point... same model = same flash size, so if you're complying with HA requirements, you'll never start off with incongruent flash sizes.

upvoted 1 times

gwb Most Recent 10 months, 3 weeks ago

Another tricky quesiton. Yes. flash size should be same. But we are assuming here that the same model has a same flash size unless you open the hardware and add or remove RAM. NTP configuration is required for HA. So I will use NTP and same interface here

upvoted 1 times

kakakayayaya 3 years, 6 months ago

Bobster 02, thanks! Great explanation.

upvoted 1 times

kakakayayaya 3 years, 6 months ago

a and e

upvoted 2 times

Question #39 *Topic 1*

An engineer is building a new access control policy using Cisco FMC. The policy must inspect a unique IPS policy as well as log rule matching. Which action must be taken to meet these requirements?

A. Configure an IPS policy and enable per-rule logging

B. Disable the default IPS policy and enable global logging

C. Configure an IPS policy and enable global logging

D. Disable the default IPS policy and enable per-rule logging

Suggested Answer: *A*

Community vote distribution

A (75%) C (25%)

14a1949 5 months, 3 weeks ago

Selected Answer: A

To meet the requirements of inspecting a unique IPS policy and logging rule matching in a new access control policy using Cisco FMC, the correct action is:

A. Configure an IPS policy and enable per-rule logging.

This approach ensures that each rule within the access control policy can be inspected with the specified IPS policy and that logging is enabled for each rule to track and log matching traffic

Option C: Configure an IPS policy and enable global logging. This would apply the IPS policy and enable logging globally, but it might not provide the granularity needed for per-rule inspection and logging

upvoted 1 times

gc999 1 year, 6 months ago

The policy must inspect a unique IPS policy as well as log "rule" matching, so does it mean the rule is IPS rule or Access Control Policy rule? I can only see logging option at Access Control Policy level. so should the answer "global" is more safe?

upvoted 1 times

Cokamaniako 1 year, 8 months ago

Selected Answer: A

"The policy must inspect a unique IPS policy as well as log rule matching"
In each policy yo can enable logging for more traffic detail.
You also can enable the logging in default policy
Answer A

upvoted 2 times

Initial14 1 year, 8 months ago

Selected Answer: A

Only A

upvoted 1 times

Joe_Blue 1 year, 9 months ago

Selected Answer: A

To meet the requirements of inspecting a unique IPS policy as well as logging rule matching in a new access control policy using Cisco FMC, the engineer should configure an IPS policy and enable per-rule logging. Therefore, the correct answer is A: Configure an IPS policy and enable per-rule logging.

upvoted 2 times

matan24 1 year, 10 months ago

Selected Answer: A

as cewe said,
"you can set logging per rule for an access control policy, so A is the right one"

upvoted 1 times

⊟ **minon_bob** 2 years ago

Selected Answer: C

There is no per-rule logging on the system. Also there would be no need to log the ACL rule as an Intrusion event will cause the rule to generate an event.

upvoted 2 times

⊟ **cryptofetti** 3 years, 4 months ago

C, seems to make more sense here

I do not think there is a setting to enable per-rule logging

upvoted 3 times

⊟ **gwb** 10 months, 3 weeks ago

There is a per-rule logging. yeah C makes sense (global), but I will go with rule base (A)

upvoted 1 times

⊟ **cewe** 2 years, 10 months ago

you can set logging per rule for an access control policy, so A is the right one

upvoted 4 times

Question #40 *Topic 1*

Which two OSPF routing features are configured in Cisco FMC and propagated to Cisco FTD? (Choose two.)

A. OSPFv2 with IPv6 capabilities

B. virtual links

C. SHA authentication to OSPF packets

D. area boundary router type 1 LSA filtering

E. MD5 authentication to OSPF packets

Suggested Answer: *BE*

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/ospf_for_firepower_threat_defense.html

Community vote distribution

BE (100%)

ASherbiny_1604 Highly Voted 2 years, 9 months ago

B & E are the correct answers as per below :

The Firepower Threat Defense device supports the following OSPF features:

Intra-area, inter-area, and external (Type I and Type II) routes.

Virtual links.

LSA flooding.

Authentication to OSPF packets (both password and MD5 authentication).

Configuring the Firepower Threat Defense device as a designated router or a designated backup router. The Firepower Threat Defense device also can be set up as an ABR.

Stub areas and not-so-stubby areas.

Area boundary router Type 3 LSA filtering.

Reference : https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/ospf_for_firepower_threat_defense.html

upvoted 12 times

matan24 Most Recent 10 months, 1 week ago

Selected Answer: BE

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/ospf_for_firepower_threat_defense.html

upvoted 2 times

rcharger00 1 year, 7 months ago

B&E Correct

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/ospf_for_firepower_threat_defense.html?bookSearch=true

The Firepower Threat Defense device supports the following OSPF features:

- Intra-area, inter-area, and external (Type I and Type II) routes.
- Virtual links.
- LSA flooding.

- Authentication to OSPF packets (both password and MD5 authentication).
- Configuring the Firepower Threat Defense device as a designated router or a designated backup router. The Firepower Threat Defense device also can be set up as an ABR.
- Stub areas and not-so-stubby areas.
- Area boundary router Type 3 LSA filtering.

upvoted 1 times

Grandslam 1 year, 9 months ago

A. OSPFv2 with IPv6 capabilities

-You use OSPFv3 for IPv6

B. virtual links

-Correct

C. SHA authentication to OSPF packets

-This doesn't make sense

D. area boundary router type 1 LSA filtering

-Would have been correct if it stated Type 3 LSA Filtering

E. MD5 authentication to OSPF packets

-supports Password and MD5

upvoted 3 times

kakakayayaya 2 years, 7 months ago

Checked on working environment.

B and E correct.

upvoted 3 times

Question #41

Topic 1

When creating a report template, how are the results limited to show only the activity of a specific subnet?

A. Create a custom search in Cisco FMC and select it in each section of the report.

B. Add an Input Parameter in the Advanced Settings of the report, and set the type to Network/IP.

C. Add a Table View section to the report with the Search field defined as the network in CIDR format.

D. Select IP Address as the X-Axis in each section of the report.

Suggested Answer: *B*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/Reports.html#87267

Community vote distribution

B (100%)

rbrain 6 months, 3 weeks ago

Selected Answer: C

I think the correct answer is C.

Adding a input parameter in the advanced setting will only add the Network/ip definition to the report. It does not limit the view.

Adjusting the search field in the table view will

upvoted 2 times

d0980cc 3 months, 3 weeks ago

I first thought "C", but the question specifically ask for "creating a report template". There is an advanced option in the Report Template for Network/IP which provides for IP/CIDR notation.

Changed my answer to B

upvoted 1 times

d0980cc 2 months, 1 week ago

No, (wrong again). It does not provide for CIDR.

rbrain is correct. It's C

upvoted 1 times

cewe 1 year, 4 months ago

Selected Answer: B

B is the right Answer

upvoted 2 times

Question #42 *Topic 1*

What is the disadvantage of setting up a site-to-site VPN in a clustered-units environment?

A. VPN connections can be re-established only if the failed master unit recovers.

B. Smart License is required to maintain VPN connections simultaneously across all cluster units.

C. VPN connections must be re-established when a new master unit is elected.

D. Only established VPN connections are maintained when a new master unit is elected.

Suggested Answer: *C*

Community vote distribution

C (100%)

greeklover84 1 year ago

Selected Answer: C

yes I agree C.

upvoted 2 times

matan24 1 year, 4 months ago

Selected Answer: C

"VPN functionality is limited to the control unit and does not take advantage of the cluster high availability capabilities. If the control unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new control unit is elected, you must reestablish the VPN connections."

reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/ftd-4100-9300-cluster.html

upvoted 3 times

Question #43 *Topic 1*

What are two features of bridge-group interfaces in Cisco FTD? (Choose two.)

A. The BVI IP address must be in a separate subnet from the connected network.

B. Bridge groups are supported in both transparent and routed firewall modes.

C. Bridge groups are supported only in transparent firewall mode.

D. Bidirectional Forwarding Detection echo packets are allowed through the FTD when using bridge-group members.

E. Each directly connected network must be on the same subnet.

Suggested Answer: *BE*

Community vote distribution

BE (100%)

Bobster02 Highly Voted 2 years, 6 months ago

C and D are the wrong answers. Must be B and E.
Cisco FMC config guide v 6.2 states that:

Bridge Group Guidelines (Transparent and Routed Mode):
You can create up to 250 bridge groups, with 64 interfaces per bridge group.
Each directly-connected network must be on the same subnet.

upvoted 11 times

lollo1234 Highly Voted 2 years, 5 months ago

"Bridge groups are supported in both transparent and routed firewall mode"
"Each directly-connected network must be on the same subnet."

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

upvoted 8 times

Lautaros Most Recent 7 months ago

The anser Highlighted are C and D, and should be B and E.

upvoted 1 times

THEODORABLE 7 months, 2 weeks ago

B & E -- https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/fpmc-config-guide-v61_chapter_01110000.pdf

Bidirectional Forwarding Detection (BFD) echo packets are not allowed through the FTD when using
bridge group members. If there are two neighbors on either side of the FTD running BFD, then the FTD
will drop BFD echo packets because they have the same source and destination IP address and appear to be part of a LAND attack.

upvoted 1 times

xziomal9 1 year, 6 months ago

Selected Answer: BE

Correct answer is: B and E

upvoted 2 times

anwar1 1 year, 7 months ago

C is correct as per below Cisco config guide "About Bridge Groups". However, Bridge group traffic can be routed to other bridge groups or routed interfaces. You can choose to isolate bridge group traffic by not assigning a name to the BVI interface for the bridge group. If you name the BVI, then the BVI participates in routing like any other regular interface.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/fpmc-config-guide-v61_chapter_01110000.pdf

upvoted 1 times

anwar1 1 year, 7 months ago

D is definitely wrong as explicitly mentioned in same document. Check "Guidelines for Firewall Mode".

upvoted 1 times

anwar1 1 year, 7 months ago

My answer is C and E as explicitly mentioned in same document "Guidelines for Firewall Mode".

upvoted 1 times

Miksik 1 year, 10 months ago

Selected Answer: BE

Must be BE

upvoted 2 times

liqucika 1 year, 11 months ago

Selected Answer: BE

Supported in both modes and must be the same subnet.

upvoted 3 times

kakakayayaya 2 years, 6 months ago

Completely wrong answer

BVI supported in R and T mode and have to be same subnet as connected network.

upvoted 3 times

Question #44 *Topic 1*

Which command is run on an FTD unit to associate the unit to an FMC manager that is at IP address 10.0.0.10, and that has the registration key Cisco123?

A. configure manager local 10.0.0.10 Cisco123

B. configure manager add Cisco123 10.0.0.10

C. configure manager local Cisco123 10.0.0.10

D. configure manager add 10.0.0.10 Cisco123

Suggested Answer: *D*

Community vote distribution

D (100%)

ekandjoum Highly Voted 2 years, 12 months ago

D: is the Good answer

upvoted 5 times

SegaMasterSystemAdmin Most Recent 6 months, 3 weeks ago

They sure like to ask this question

upvoted 1 times

aalnman 1 year, 6 months ago

Selected Answer: D

D with 100% certainty. I've done this 4 times in production and the first time took me 4 hours to figure out. I will never forget this command, lol.

upvoted 3 times

cewe 1 year, 10 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/misc/fmc-ftd-mgmt-nw/fmc-ftd-mgmt-nw.html#id_106101

upvoted 1 times

Bobster02 2 years, 5 months ago

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

upvoted 2 times

Bobster02 2 years, 6 months ago

D is indeed the only correct.

upvoted 3 times

Question #45 *Topic 1*

Which two actions can be used in an access control policy rule? (Choose two.)

A. Block with Reset

B. Monitor

C. Analyze

D. Discover

E. Block ALL

Suggested Answer: *AB*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/AC-Rules-Tuning-

Overview.html#71854

Community vote distribution

AB (100%)

Nian 2 months, 2 weeks ago

Selected Answer: AB

Policy rule actions:

Allow, Trust, Block, Block with reset, Interactive block, Monitor

upvoted 1 times

CHERIFNDIAYE 12 months ago

Selected Answer: AB

MONITOR AND BLOCK AND RESET ARE THE CORRECT ANSWER;

upvoted 1 times

Bobster02 3 years, 6 months ago

A and B are confirmed to be correct.

upvoted 4 times

ekandjoum 3 years, 12 months ago

A,B is OK answer

upvoted 3 times

Question #46 *Topic 1*

Which two routing options are valid with Cisco FTD? (Choose two.)

A. BGPv6

B. ECMP with up to three equal cost paths across multiple interfaces

C. ECMP with up to three equal cost paths across a single interface

D. BGPv4 in transparent firewall mode

E. BGPv4 with nonstop forwarding

Suggested Answer: *AB*

Community vote distribution

AB (60%) BE (40%)

⊟ **netwguy** Highly Voted 3 years, 10 months ago

Cisco is trying to throw us off here - correct answers are A and C. As pfunky states, we can have up to 8 routes, meaning that C is a "valid" answer. The reason E is incorrect is that we cannot configure NSF for BGPv4 - we can only configure graceful restart, which relies on info from NSF capable/aware devices. For OSPF however, we can configure a device to be fully NSF capable/aware. Read through this if you are still in doubt: https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-ospf.html

upvoted 6 times

⊟ **Last00i** Most Recent 3 weeks, 1 day ago

Selected Answer: BE

BGPv6 isn't supported according to cisco documentation

upvoted 1 times

⊟ **d0980cc** 3 months ago

Selected Answer: BE

https://www.cisco.com/c/en/us/td/docs/security/firepower/710/fdm/fptd-fdm-config-guide-710/fptd-fdm-routing.html?bookSearch=true#ID-2101-0000004d:~:text=you%20can%20configure%20multiple%20default%20routes%20across%20three%20interfaces%20in%20the%20zone%3A

https://www.cisco.com/c/en/us/td/docs/security/firepower/710/fdm/fptd-fdm-config-guide-710/fptd-fdm-bgp.html?bookSearch=true#:~:text=The%20graceful%20restart%20capability%20is%20negotiated%20between%20nonstop%20forwarding%20(NSF)

B and E is correct

upvoted 1 times

⊟ **d0980cc** 2 months, 2 weeks ago

A&B correct
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/bgp_for_firepower_threat_defense.html#ID-2100-0000004a:~:text=IPv6%20Guidelines-,Supports%20IPv6,-.%20Graceful%20restart

upvoted 1 times

⊟ **rbrain** 6 months, 3 weeks ago

Selected Answer: AB

A :
https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-bgp.html
" BGP IPv4 is supported both on global and user-defined virtual routers. However, only BGP IPv6 configuration is supported on a global virtual router."
Its about Cisco FTD devices and not Cisco FTDv appliance
B : https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/routing-ecmp.html
" You can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within each zone." I read this as 1 equal cost route per interface. So 3 equal cost paths means 3 interfaces, not 1. So B must be valid and not C.

upvoted 2 times

⊟ **caalbert** 9 months, 1 week ago

Selected Answer: BE

Routing protocols

upvoted 1 times

⊟ gwb 1 year, 4 months ago

BGPv6 (A) is no doubt. So A is first answer. My confusion is this. B and C are saying up to 3. but all links that here mentioned up to 8 interfaces. "You can associate only 8 interfaces per ECMP zone." 3 is NOT same as 8? why B and C?

upvoted 1 times

⊟ achille5 1 year, 4 months ago

Selected Answer: AB

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01100011.html#ID-2101-0000000e

https://www.cisco.com/c/en/us/td/docs/security/firepower/710/fdm/fptd-fdm-config-guide-710/fptd-fdm-virtual-routers.html

upvoted 1 times

⊟ bofu 1 year, 5 months ago

Selected Answer: BE

Supported Routing Protocols:

BGPv4: Cisco FTD supports BGPv4 for IPv4 routing, enabling it to exchange routes with other BGP-speaking devices and participate in dynamic routing environments.
OSPFv2: FTD also supports OSPFv2, another interior gateway protocol (IGP) commonly used within a single autonomous system for IPv4 routing.
Static routes: You can manually configure static routes to define specific paths for traffic to reach certain destinations.
Key Routing Features:

ECMP (Equal Cost Multi-Path): Allows for load balancing across up to three equal cost paths for improved performance and redundancy. However, it's important to note that ECMP is limited to multiple interfaces, not a single interface.
NSR (Nonstop Forwarding) with BGPv4: Ensures continuous forwarding of traffic even during BGP process restarts or failovers, enhancing network resilience.

upvoted 1 times

⊟ Bubu3k 1 year, 5 months ago

Selected Answer: AB

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/routing-ecmp.html

"You can associate only 8 interfaces per ECMP zone."

upvoted 2 times

⊟ Abetong 1 year, 10 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/bgp_for_firepower_threat_defense.html#:~:text=BGP%20is%20supported%20only%20in%20routed%20mode.

Guidelines for BGP
Firewall Mode Guidelines
Does not support transparent firewall mode. BGP is supported only in routed mode.

FTD supports BGPv6

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/bgp_for_firepower_threat_defense.html

FTD ECMP
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/routing-ecmp.html

The FTD device supports Equal-Cost Multi-Path (ECMP) routing. You can configure traffic zones per virtual router to contain a group of interfaces.
You can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within each zone.
For example, you can configure multiple default routes across three interfaces in the zone

upvoted 1 times

⊟ aadach 3 years, 5 months ago

so it means that A E are correct answers

upvoted 2 times

⊟ **aadach** 3 years, 5 months ago

Equal-Cost Multi-Path (ECMP) Routing - You can have up to 8 equal cost static or dynamic routes per interface

upvoted 1 times

⊟ **pfunkylol** 3 years, 11 months ago

Why is not C an option to be considered ? I cannot find anything in the documentation related to BGP NSF , but I do about ECMP.

Equal-Cost Multi-Path (ECMP) Routing
The Firepower Threat Defense device supports Equal-Cost Multi-Path (ECMP) routing.
You can have up to 8 equal cost static or dynamic routes per interface.

upvoted 1 times

⊟ **Bobster02** 4 years ago

Agree: A and E.

upvoted 2 times

⊟ **kakakayayaya** 4 years ago

A and E

upvoted 2 times

Question #47 *Topic 1*

Which object type supports object overrides?

A. time range

B. security group tag

C. network object

D. DNS server group

Suggested Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

SanchezEldorado 8 months, 1 week ago

Reference link is broken. C is correct and here's the link:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

upvoted 2 times

cryptofetti 1 year, 4 months ago

C is correct
Object Overrides supported are:
Network
Port
VLAN tag
URL

upvoted 2 times

Question #48 *Topic 1*

Which Cisco Firepower rule action displays an HTTP warning page?

A. Monitor

B. Block

C. Interactive Block

D. Allow with Warning

Suggested Answer: *C*

Reference:
https://www.cisco.com/c/en/us/td/docs/security/firesight/541/user-guide/FireSIGHT-System-UserGuide-v5401/AC-Rules-Tuning-Overview.html#76698

gwb 10 months, 2 weeks ago

Interactive is a KEY. (web page)

upvoted 2 times

Question #49 *Topic 1*

What is the result a specifying of QoS rule that has a rate limit that is greater than the maximum throughput of an interface?

A. The rate-limiting rule is disabled.

B. Matching traffic is not rate limited.

C. The system rate-limits all traffic.

D. The system repeatedly generates warnings.

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/quality_of_service_qos.pdf

⊟ **ASherbiny_1604** 9 months, 1 week ago

Correct

If you specify a limit greater than the maximum throughput of an interface, the system does not rate limit matching traffic. Maximum throughput may be affected by an interface's hardware configuration, which you specify in each device's properties (Devices > Device Management).

Reference : https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/quality_of_service__qos__for_firepower_threat_defense.html

upvoted 3 times

Question #50 Topic 1

Which Firepower feature allows users to configure bridges in routed mode and enables devices to perform Layer 2 switching between interfaces?

A. FlexConfig

B. BDI

C. SGT

D. IRB

Suggested Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.html

Doris8000 Highly Voted 9 months, 3 weeks ago
Integrated Routing and Bridging (IRB) : Customers often want to have multiple physical interfaces configured to be part of the same VLAN. The IRB feature meets this demand by allowing users to configure bridges in routed mode, and enables the devices to perform L2 switching between interfaces (including subinterfaces).
upvoted 7 times

Doris8000 Most Recent 10 months ago
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/relnotes/Firepower_System_Release_Notes_Version_620/new_features_and_functionality.h
upvoted 1 times

Question #51 *Topic 1*

In which two places are thresholding settings configured? (Choose two.)

A. on each IPS rule

B. globally, within the network analysis policy

C. globally, per intrusion policy

D. on each access control rule

E. per preprocessor, within the network analysis policy

Suggested Answer: *AC*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-
Threshold.pdf

Community vote distribution

AC (100%)

tinyJoe 7 months, 1 week ago

Selected Answer: AC

I agree with the A&C.

I would like to add that in Snort2, Threshold can be applied both per policy and globally, but in Snort3, it can only be applied per policy.

https://community.cisco.com/t5/tkb-%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3-%E3%83%89%E3%82%AD%E3%83%A5%E3%83%A1%E3% 83%B3%E3%83%88/intrusion-event-%E7%94%9F%E6%88%90%E3%81%AE%E9%96%BE%E5%80%A4%E5%A4%89%E6%9B%B4%E3%81%AE%E3%81%94%E7%B4%B9%E4%BB%8B /ta-p/4703848

upvoted 2 times

Weyland 2 years, 8 months ago

Selected Answer: AC

According to real life environment, you can set it on per IPS rules and globally. A & C.

upvoted 2 times

Doris8000 3 years, 9 months ago

You can set a global threshold across all traffic to limit how often events from a specific source or
destination are logged and displayed per specified time period. For more information, see
Understanding Thresholding, page 22-1 and Configuring Global Thresholds, page 22-3.

• You can set thresholds per shared object rule, standard text rule, or preprocessor rule in your
intrusion policy configuration, as described in Configuring Event Thresholding, page 20-21.

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-Threshold.pdf

upvoted 2 times

Doris8000 3 years, 10 months ago

Integrated Routing and Bridging (IRB) : Customers often want to have multiple physical interfaces configured to be part of the same VLAN. The IRB feature meets this demand by allowing users to configure bridges in routed mode, and enables the devices to perform L2 switching between interfaces (including subinterfaces).

upvoted 1 times

Question #52 *Topic 1*

In which two ways do access control policies operate on a Cisco Firepower system? (Choose two.)

A. Traffic inspection is interrupted temporarily when configuration changes are deployed.

B. The system performs intrusion inspection followed by file inspection.

C. They block traffic based on Security Intelligence data.

D. File policies use an associated variable set to perform intrusion prevention.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

Suggested Answer: *CE*

Community vote distribution

CE (60%) AC (40%)

d0980cc 2 months ago

Selected Answer: CE

B is correct as well, If deep packet inspection is applied. Why does Cisco DO THIS?!!!

I'll choose C&E

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: CE

The correct answers are actually C and E:

C. They block traffic based on Security Intelligence data.

Access control policies on Cisco Firepower systems can block connections based on the latest IP address, URL, and domain name reputation intelligence.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

The system performs a preliminary inspection on trusted traffic to ensure it matches the trusted parameters before allowing it through.

Option A is not correct because traffic inspection is not typically interrupted temporarily when configuration changes are deployed.

upvoted 1 times

gwb 10 months, 2 weeks ago

I think the key is "Access Control Policies" here.

A - "Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection." This is how ACP works along with Intrusion Policy.

B - This is correct (ACL layer 3 -> SI -> ACL layer7 ->File policy -> Intrusion policy) Intrusion policy is after the file policy. However this is NOT relevant to ACP.

C - SI can block the traffic, but this is NOT also relevant to ACP.

D - File Policy and Intrusion Policy with variable set are for Inspection. So this should be like this "Intrusion policy use an associated variable set to perform inspection.

E - Technically this is right before a packet goes into Snort from Firewall. But I count this as ACP behavior. So A and E

upvoted 1 times

Vlad_Is_Love_ua 1 year, 4 months ago

Selected Answer: AC

"... Changing the total number of intrusion policies used by an access control policy restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. ..."

from this https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/getting_started_with_access_control_policies.html#ID-2176-00000027

upvoted 2 times

spambox730 1 year, 5 months ago

Selected Answer: AC

Not B because file policy is before inspection policy

Not D because variables belong to inspection policy

Not E because there is zero inspection on trusted traffic

That leaves it with A and C.

upvoted 1 times

Bbb78 1 year, 7 months ago

Selected Answer: CE

A is correct BUT the traffic is dropped - the way they worded this it looks like traffic is permitted - no, traffic is dropped.

Still C and E are the other options for me.

upvoted 2 times

Joe_Blue 1 year, 9 months ago

Selected Answer: CE

C. They block traffic based on Security Intelligence data.

E. The system performs a preliminary inspection on trusted traffic to validate that it matches the trusted parameters.

upvoted 2 times

ureis 1 year, 8 months ago

they do not perform a preliminary inspection on trusted traffic to validate parameters.

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: AC

Correct answer is: A and C

upvoted 1 times

Markl3ver 2 years, 8 months ago

My opinion is A and B, Security inteligence it is another engine which blocks trafic by it self, not ACP block it with corresponding with SE

upvoted 1 times

japm1801 2 years, 4 months ago

SI doesn't block by itself, in fact, SI has to be configured under ACP to take effect, so A and C fit in this question

upvoted 1 times

SanchezEldorado 2 years, 8 months ago

Selected Answer: CE

C and E make the most sense to me. We're all agreed on C, but SNORT doesn't always restart when policies are deployed and it isn't a "way" that ACPs operate. A trust rule within an ACP will use parameters to specify traffic such as IP, Port, etc... The firewall does need to inspect traffic that much to see that the traffic is trusted and then allow it without further SNORT inspection.

upvoted 2 times

cewe 2 years, 10 months ago

Selected Answer: AC

like 4study explained

upvoted 1 times

4study 3 years, 1 month ago

It seems to be A and C

When deploying changes SNORT can restart causing traffic interuptions -->

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html#reference_F11C552688424DEF85ED145FA97283B7

I disagree with D because File policies don't make use of Variable sets, those are used for Intrusion policies.

upvoted 3 times

Sarbi 3 years, 3 months ago

The correct answer is C and D.A does not make any sense to be correct.

upvoted 1 times

Question #53 *Topic 1*

Which two types of objects are reusable and supported by Cisco FMC? (Choose two.)

A. dynamic key mapping objects that help link HTTP and HTTPS GET requests to Layer 7 application protocols.

B. reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists

C. network-based objects that represent IP addresses and networks, port/protocol pairs, VLAN tags, security zones, and origin/destination country

D. network-based objects that represent FQDN mappings and networks, port/protocol pairs, VXLAN tags, security zones and origin/destination country

E. reputation-based objects, such as URL categories

Suggested Answer: *BC*

Community vote distribution

BC (100%)

gwb 10 months, 2 weeks ago

D is a common way to do at FMC. C inherited policy may work. But the question is asking "locally significant internal network subnets at each location" i.e, 10.0.1.0/24 10.0.2.0/24 10.0.3.0/24 there are three subnets (Inside_net). By using inherited policy, it can include those subnets with a rule such as https outbound allowed. So C seems ok, but because of "only the locally significant network subnet" - It makes sense D more to me

upvoted 1 times

ureis 1 year, 8 months ago

B. Reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists are reusable objects supported by Cisco FMC.

C. Network-based objects that represent IP addresses and networks, port/protocol pairs, VLAN tags, security zones, and origin/destination country are also reusable objects supported by Cisco FMC.

A is not a valid type of reusable object in Cisco FMC.

D contains VXLAN tags, which are not mentioned as a supported type of object.

E is similar to option B but specifically mentions URL categories, which is not an exhaustive list of all types of reputation-based objects supported by Cisco FMC.

upvoted 2 times

Joe_Blue 1 year, 9 months ago

Selected Answer: BC

The two types of objects that are reusable and supported by Cisco FMC are:

B. Reputation-based objects that represent Security Intelligence feeds and lists, application filters based on category and reputation, and file lists.

C. Network-based objects that represent IP addresses and networks, port/protocol pairs, VLAN tags, security zones, and origin/destination country.

upvoted 2 times

Mevijil 2 years ago

Selected Answer: BC

I believe B & C are correct - SI feeds/lists and basic network objects are two common use cases for objects. Answer "A" is dynamic so you probably wouldn't use a reusable object, same with answer "D". In E - you can store URLs in objects but not categories, I don't think.

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/730/management-center-device-config-73/objects-object-mgmt.html#ID-2243-0000045f

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: BC

Correct answer is: B and C

upvoted 1 times

Bobster02 3 years, 5 months ago

After all original answer is correct.

upvoted 1 times

⊟ **Bobster02** 3 years, 6 months ago

My answers are C and E.

upvoted 2 times

⊟ **Bobster02** 3 years, 6 months ago

However, exam stipulates two answers not one.......

upvoted 1 times

⊟ **kakakayayaya** 3 years, 6 months ago

Right answer was provided.

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/reusable_objects.html

upvoted 3 times

⊟ **kakakayayaya** 3 years, 6 months ago

Security zones and Security Intelligence are not reusable. Answer A looks odd.

I see just one right answer - E.

upvoted 1 times

⊟ **essie007** 3 years, 5 months ago

Incorrect, security zones can be reused in device config and ACP. Custom SI feeds and list can also be used in ACP SI. Provided answer is correct.

upvoted 1 times

Question #54 *Topic 1*

A security engineer is configuring an Access Control Policy for multiple branch locations. These locations share a common rule set and utilize a network object called INSIDE_NET which contains the locally significant internal network subnets at each location. What technique will retain the policy consistency at each location but allow only the locally significant network subnet within the application rules?

A. utilizing a dynamic ACP that updates from Cisco Talos

B. creating a unique ACP per device

C. utilizing policy inheritance

D. creating an ACP with an INSIDE_NET network object and object overrides

Suggested Answer: *D*

Community vote distribution

D (67%) C (33%)

14a1949 5 months, 2 weeks ago

Selected Answer: D

The best technique to retain policy consistency across multiple branch locations while allowing only the locally significant network subnet within the application rules is:

D. creating an ACP with an INSIDE_NET network object and object overrides

This approach allows you to maintain a consistent Access Control Policy (ACP) across all locations while using object overrides to specify the locally significant subnets for each branch (https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/access-rules.html) (https://www.cisco.com/c/en/us/td/docs/security/firepower/710/fdm/fptd-fdm-config-guide-710/fptd-fdm-access.html).

upvoted 1 times

Kris92 10 months, 1 week ago

Selected Answer: D

should be D, policy inheritance is doing part of the job, but the more important thing is to have the object values specific to the location, which can be done with object overrides
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reusable_Objects.html#concept_8BFE8B9A83D742D9B647A74F7AD50053

upvoted 2 times

bassfunk 1 year, 4 months ago

Selected Answer: D

D is the only answer that makes sense.

upvoted 2 times

gc999 1 year, 6 months ago

Selected Answer: C

If for D, finally each device would obtain the firewall policy with ALL the unrelated subnets at the inside, which is violated to the question "allow only the locally significant network subnet".

upvoted 3 times

Mevijil 2 years ago

Selected Answer: D

Definitely D - object override allows you to create a single object with multiple values, which is what they're doing for the two different networks sharing one rule set

upvoted 2 times

dique 2 years, 4 months ago

Selected Answer: D

Answer is D

upvoted 2 times

⊟ **hz033** 2 years, 7 months ago

Selected Answer: C

it sounds as the right answer is C

upvoted 1 times

⊟ **SegaMasterSystemAdmin** 1 year, 6 months ago

no that can't be it because policy inheritance will just ensure that child policies will inherit the policies from the parent policy

upvoted 2 times

⊟ **ureis** 1 year, 7 months ago

explain

upvoted 1 times

Question #55 *Topic 1*

An organization has seen a lot of traffic congestion on their links going out to the internet. There is a Cisco Firepower device that processes all of the traffic going to the internet prior to leaving the enterprise. How is the congestion alleviated so that legitimate business traffic reaches the destination?

A. Create a NAT policy so that the Cisco Firepower device does not have to translate as many addresses.

B. Create a flexconfig policy to use WCCP for application aware bandwidth limiting.

C. Create a QoS policy rate-limiting high bandwidth applications.

D. Create a VPN policy so that direct tunnels are established to the business applications.

Suggested Answer: *C*

Community vote distribution

C (100%)

japm1801 10 months, 2 weeks ago

Selected Answer: C

the way to resolve congestion is rate limiting traffico to avoid to reach maximun bandwidth

upvoted 1 times

Question #56 *Topic 1*

An engineer configures an access control rule that deploys file policy configurations to security zone or tunnel zones, and it causes the device to restart. What is the reason for the restart?

A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.

B. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the destination policy.

C. Source or destination security zones in the source tunnel zone do not match the security zones that are associated with interfaces on the target devices.

D. The source tunnel zone in the rule does not match a tunnel zone that is assigned to a tunnel rule in the source policy.

Suggested Answer: *A*

Community vote distribution

A (100%)

Gabranch Highly Voted 👍 1 year, 7 months ago

Selected Answer: A

I believe this question is mis-worded and is referring to a restart of the SNORT process, rather than the Device. Basically, it appears to be saying that if you adjust a file policy in the ACP, then the device that has interfaces in zones referenced in that ACP will have its SNORT process restarted.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/policy_management.html

"Note that access control rules that deploy these file policy configurations to security zones or tunnel zones cause a restart only when your configuration meets the following conditions:

Source or destination security zones in your access control rule must match the security zones associated with interfaces on the target devices.

Unless the destination zone in you access control rule is any, a source tunnel zone in the rule must match a tunnel zone assigned to a tunnel rule in the prefilter policy."

upvoted 5 times

gwb 10 months, 2 weeks ago

thanks for SNORT information. makes sense

upvoted 1 times

Dreng65 Most Recent ⊙ 1 year, 5 months ago

Selected Answer: A

nterruptions to Traffic Flow and Inspection During Deploy

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts the Snort process, which interrupts traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior and Configurations that Restart the Snort Process When Deployed or Activated.

upvoted 3 times

tanri04 1 year, 9 months ago

A. Source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices.

The reason for the device to restart is that the source or destination security zones in the access control rule matches the security zones that are associated with interfaces on the target devices. This can cause a routing loop that can overload the device and cause it to restart.

When configuring file policies and access control rules in Cisco FMC, it is important to ensure that the source and destination security zones do not match the security zones associated with interfaces on the target devices. This can be done by reviewing the zone assignments and making any necessary changes to prevent the routing loop.

The other options listed are not the reason for the device to restart in this scenario. B and D relate to tunnel zones and tunnel rules, which are not mentioned in the scenario. C relates to source and destination security zones in a source tunnel zone, which is not directly relevant to the scenario.

upvoted 1 times

⊟ **Doris8000** 3 years, 3 months ago

Note that access control rules that deploy these file policy configurations to security zones or tunnel zones cause a restart only when your configuration meets the following conditions:

Source or destination security zones in your access control rule must match the security zones associated with interfaces on the target devices.

Unless the destination zone in you access control rule is any, a source tunnel zone in the rule must match a tunnel zone assigned to a tunnel rule in the prefilter policy

upvoted 4 times

Question #57 *Topic 1*

An engineer is attempting to create a new dashboard within the Cisco FMC to have a single view with widgets from many of the other dashboards. The goal is to have a mixture of threat and security related widgets along with Cisco Firepower device health information. Which two widgets must be configured to provide this information? (Choose two.)

A. Intrusion Events

B. Correlation Information

C. Appliance Status

D. Current Sessions

E. Network Compliance

Suggested Answer: *AC*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/dashboards.html#ID-2206-00000283

Community vote distribution
AC (100%)

tanri04 Highly Voted 1 year, 3 months ago
To create a new dashboard within the Cisco FMC with a mixture of threat and security related widgets along with Cisco Firepower device health information, the two widgets that must be configured are:

C. Appliance Status - This widget displays the health status of the Cisco Firepower device, including hardware status, performance metrics, and system resource utilization. It provides an overview of the device's health and helps in identifying any issues that need attention.

A. Intrusion Events - This widget displays information on intrusion events detected by the Cisco Firepower device, including the source and destination IP addresses, severity level, and action taken. It provides information on the security posture of the network and helps identify potential threats.

While the other widgets listed, such as Correlation Information, Current Sessions, and Network Compliance, may provide valuable information, they may not necessarily provide a mixture of threat and security related widgets along with Cisco Firepower device health information. Therefore, options A and C are the two widgets that must be configured to provide this information.
upvoted 6 times

[Removed] Most Recent 9 months, 3 weeks ago
Selected Answer: AC
The Appliance Status Widget
The Appliance Status widget indicates the health of the appliance and of any appliances it is managing. Note that because the Firepower Management Center does not automatically apply a health policy to managed devices, you must manually apply a health policy to devices or their status appears as Disabled. This widget appears by default on the Status tabs of the Detailed Dashboard and the Summary Dashboard.

The Intrusion Events Widget
The Intrusion Events widget shows the intrusion events that occurred over the dashboard time range, organized by priority. This includes statistics on intrusion events with dropped packets and different impacts. This widget appears by default on the Intrusion Events tab of the Summary Dashboard.
Took it from
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/dashboards.html#ID-2206-0000918
upvoted 3 times

ureis 1 year, 1 month ago
seems to have many cha-gpt model answers here, be careful guys, is not totally trusted
upvoted 2 times

Grandslam 2 years, 3 months ago
Intrusion is an obvious answer for Intrusions...

However, Security.... That could be either:
The Current Sessions widget shows which users are currently logged into the appliance, the IP address associated with the machine where the session originated, and the last time each user accessed a page on the appliance
OR
The Network Compliance widget summarizes your hosts' compliance with the white lists you configured.

I have no idea... but If I had to choose I would choose "Network".... But I don't like it.
upvoted 1 times

⊟ **Cherster** 2 years, 3 months ago
Its asking about threat and security related widgets....I would say Intrusion events for threat and Network Compliance for security.
upvoted 1 times

⊟ **Doris8000** 2 years, 9 months ago
About Dashboards
Firepower System dashboards provide you with at-a-glance views of current system status, including data about the events collected and generated by the system. You can also use dashboards to see information about the status and overall health of the appliances in your deployment. Keep in mind that the information the dashboard provides depends on how you license, configure, and deploy the system.
upvoted 1 times

Question #58 *Topic 1*

There is an increased amount of traffic on the network and for compliance reasons, management needs visibility into the encrypted traffic. What is a result of enabling TLS/SSL decryption to allow this visibility?

A. It prompts the need for a corporate managed certificate.

B. It will fail if certificate pinning is not enforced.

C. It has minimal performance impact.

D. It is not subject to any Privacy regulations.

Correct Answer: *A*

tinyJoe 7 months, 1 week ago

Selected Answer: A

A. Perhaps this is correct, but I am not sure if it needs to be “corporately managed”. What is needed is a CA certificate to present to the client on behalf of the server.
B. Not possible.
C. Not possible. Firewall decryption usually consumes a very large amount of memory, and even if you strictly limit the traffic to be decrypted, you will still need to use one or two higher models.
D. Not possible. Law and company policy should be carefully considered when decrypting traffic.

See the following document for details.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/encrypted-traffic-overview.html?bookSearch=true

Translated with DeepL.com (free version)
upvoted 1 times

Question #59 *Topic 1*

An organization is setting up two new Cisco FTD devices to replace their current firewalls and cannot have any network downtime. During the setup process, the synchronization between the two devices is failing. What action is needed to resolve this issue?

A. Confirm that both devices are running the same software version.

B. Confirm that both devices are configured with the same types of interfaces.

C. Confirm that both devices have the same flash memory sizes.

D. Confirm that both devices have the same port-channel numbering.

Suggested Answer: *A*

Community vote distribution

C (50%) A (50%)

TECH3K3 1 month, 3 weeks ago

Selected Answer: A

The main thing that needs to match is Software, not flash size.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: A

The correct answer is:

A. Confirm that both devices are running the same software version.

Ensuring that both Cisco Firepower Threat Defense (FTD) devices are running the same software version is crucial for successful synchronization. Mismatched software versions can lead to compatibility issues and synchronization failures.

Option C, which involves confirming that both devices have the same flash memory sizes, is not typically a requirement for synchronization between Cisco FTD devices. The primary factor that affects synchronization is the software version. If the devices are running different software versions, they may not be able to communicate and synchronize properly.

While having the same flash memory sizes might be important for other aspects of device performance and storage capacity, it does not directly impact the synchronization process. Ensuring both devices are running the same software version is crucial for compatibility and successful synchronization.

upvoted 2 times

gwb 10 months, 2 weeks ago

what kind of questions is this? :(IF i need to choose one, I will go "memory" because below guys explained very well.

upvoted 2 times

Vlad_Is_Love_ua 1 year, 4 months ago

A & B is correct according to this
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html#ID-2107-00000019

...Hardware Requirements:
... - Have the same number and types of interfaces. ...

... Software Requirements
... - Have the same software version....

upvoted 1 times

SegaMasterSystemAdmin 1 year, 6 months ago

Selected Answer: C

The answer is C because if the flash memory is smaller on the secondary, then syncing will fail. Confirming that both devices are running the same code is a perquisite for HA and does not have anything to do with synchronization failure.

upvoted 4 times

Joninjimbo 1 year, 2 months ago

Confirmed via configuration guide:
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/high_availability_for_firepower_threat_defense.html

"If you are using units with different flash memory sizes in your High Availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail."

upvoted 2 times

Bbb78 1 year, 7 months ago

Selected Answer: C

synchronization is failing not HA pairing - C

upvoted 2 times

tanri04 1 year, 9 months ago

B. Confirm that both devices are running the same software version.

When setting up a pair of Cisco FTD devices for high availability, both devices must run the same software version. If the software versions are different, the synchronization between the two devices may fail, causing downtime. Therefore, ensuring that both devices are running the same software version should resolve the synchronization issue.

Confirming that both devices have the same port-channel numbering, configured with the same types of interfaces, and have the same flash memory sizes are not likely to affect the synchronization process between the two devices.

upvoted 1 times

Joe_Blue 1 year, 9 months ago

Selected Answer: A

A. Confirm that both devices are running the same software version.

Ensuring that both devices are running the same software version is critical for successful synchronization between the two devices. If the devices are running different software versions, the synchronization process will fail. The other options listed are not related to the synchronization process and are unlikely to cause synchronization issues.

upvoted 3 times

orotta 2 years, 10 months ago

The question is not asking the requirement of HA, but it is asking "During the setup process the synchronization between the HA fails"
so the answer is the synchronization fails due to less flash memory space in the second firewall

upvoted 4 times

orotta 2 years, 10 months ago

I agree with those select C. The keyword in the question is "synchronization"
The HA is created, but synchronization fails, so the reason is the second firewall has less flash memory.

Please read this paragraph from Cisco site
If you are using units with different flash memory sizes in your High Availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html

upvoted 1 times

ureis 1 year, 7 months ago

you dont need same exactly size flash to make HA, just need enought space, not exact space

upvoted 5 times

aalnman 2 years, 5 months ago

But, the paragraph you posted from Cisco says "make sure the unit with the smaller flash memory has enough space...." Answer C says "Confirm that both devices have the same flash memory sizes." There is a difference between "enough" and "same." According to your paragraph, they don't need to be the same, just the smaller unit has to have enough. So C could be wrong. This is splitting hairs I know, but I think worth pointing out.

upvoted 2 times

jamesque23 3 years ago

C

I agree with everyone, The devices must have the same type and number of interfaces and software needs to be on same version.

However, the question is specifically touching on synchronization issues, so the answer is C.

If you are using units with different flash memory sizes in your High Availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/firepower_threat_defense_high_availability.html

upvoted 4 times

cmonbruh 3 years ago

I agree, I would pick flash on the actual exam for the same reason, HA pair won't work at all if there is a version or interface type misconfiguration, however if it is a synchronization problem, it means that both of these requirements have been met.

upvoted 1 times

elliot67 3 years, 2 months ago

The devices also have to have the same version in order to create a HA...

upvoted 2 times

Doris8000 3 years, 2 months ago

Answer is B

High Availability Requirements

The devices must be the same hardware model.

The devices must have the same modules installed. ...

The devices must have the same type and number of interfaces.

To create an HA pair in CDO, both devices must have management interfaces configured.

upvoted 1 times

Cokamaniako 1 year, 7 months ago

Because not C?

upvoted 1 times

kplost 3 years, 3 months ago

B

The two units in a High Availability configuration must:

Be the same model.

Have the same number and types of interfaces.

For the Firepower 4100/9300 chassis, all interfaces must be preconfigured in FXOS identically before you enable High Availability. If you change the interfaces after you enable High Availability, make the interface changes in FXOS on the Standby unit, and then make the same changes on the Active unit.

If you are using units with different flash memory sizes in your High Availability configuration, make sure the unit with the smaller flash memory has enough space to accommodate the software image files and the configuration files. If it does not, configuration synchronization from the unit with the larger flash memory to the unit with the smaller flash memory will fail.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/firepower_threat_defense_high_availability.html

upvoted 1 times

4study 3 years, 1 month ago

On the same doc you mention it says that for Software requirements they need to be on the same version so I'm going with A

upvoted 1 times

Question #60 *Topic 1*

An organization wants to secure traffic from their branch office to the headquarters building using Cisco Firepower devices. They want to ensure that their Cisco
Firepower devices are not wasting resources on inspecting the VPN traffic. What must be done to meet these requirements?

A. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.

B. Tune the intrusion policies in order to allow the VPN traffic through without inspection.

C. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies.

D. Enable a flexconfig policy to re-classify VPN traffic so that it no longer appears as interesting traffic.

Suggested Answer: *A*

Community vote distribution

A (100%)

d0980cc 2 months, 2 weeks ago

Selected Answer: D

I believe the answer may be D
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_threat_defense_site_to_site_vpns.html#:~:text=When%20you%20want%20to%20bypass%20the%20inspection%20of%20decrypted%20traffic%2

upvoted 1 times

Silexis 4 months, 4 weeks ago

Selected Answer: C

"If you use FTD on FP4100/9300 and want the flow to completely bypass the Snort inspection then consider the Prefilter rule with Fastpath action (see the related section in this document)"
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html#toc-hId--311118177

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

the correct answer is C. Configure the Cisco Firepower devices to ignore the VPN traffic using prefilter policies. Prefilter policies are specifically designed to handle scenarios like this, where you want to bypass deeper inspection for certain types of traffic, such as VPN traffic, to conserve resources.

Option A, configuring the devices to bypass access control policies for VPN traffic, would not achieve the same result because access control policies are not designed to handle the bypassing of inspection processes in the same way prefilter policies do.

upvoted 1 times

gwb 10 months, 2 weeks ago

key "not wasting resources on inspecting the VPN traffic" prefilter is right before ACP, thus to save resources, prefilter is much effective although ACP is doing same but happens after prefilter. 5-Tuple ACL -- prefilter is recommended by Cisco. google 5 tuple with prefilter.

upvoted 2 times

gc999 1 year, 6 months ago

Selected Answer: A

Option C will be correct IF Site-to-site VPN traffic that is going through the device. That is, the device is not an endpoint in the VPN topology.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/access-prefilter.html#id_23357:~:text=Site%2Dto%2Dsite%20VPN%20traffic%20that%20is%20going%20through%20the%20device.%20That%20is%2C%20the%20devic

Flows cannot be offloaded if IPsec and TLS/DTLS VPN connections that terminate on the device
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/710/management-center-device-config-71/access-prefilter.html#id_23357:~:text=IPsec%20and%20TLS/DTLS%20VPN%20connections%20that%20terminate%20on%20the%20device

So I will choose A which is the easiest way to bypass VPN traffic for inspection.

upvoted 1 times

Silexis 4 months, 4 weeks ago

Cisco FTD has 2 engines: LINA and SNORT. In the VPN case, you are only going to spare the system of SNORT processing. The only way of a VPN offloadi
processing logic flow as any other traffic

upvoted 1 times

gc999 1 year, 5 months ago

After reviewing all the materials, I would choose C now.

upvoted 1 times

greeklover84 1 year, 6 months ago

Selected Answer: A

I would choose A

upvoted 1 times

ureis 1 year, 7 months ago

Just configure ACP to "Trust" and the traffic will not be inspected

upvoted 2 times

Joe_Blue 1 year, 9 months ago

Selected Answer: A

A. Configure the Cisco Firepower devices to bypass the access control policies for VPN traffic.

By configuring the Cisco Firepower devices to bypass the access control policies for VPN traffic, the devices will not perform security inspection on the VPN traffic, which will help to conserve resources. This can be done by creating an access control rule that matches the VPN traffic and then setting the action to "Trust". This will allow the traffic to bypass the access control policies and not consume resources.

upvoted 2 times

aadach 2 years, 11 months ago

A : inside VPN S2S config (tunnel) can you find option "Access Control for VPN Traffic" - Bypass Access Control policy for decrypted traffic (sysopt permit-vpn), that is it !!

upvoted 3 times

ThanosAth 2 years, 11 months ago

A is correct answer. Check the following article. https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/prefiltering_and_prefilter_policies.html#id_31063

According to the article there are limitations to what type of traffic can be offloaded to fastpath. In the above article it is stated that "IPsec and TLS/DTLS VPN connections that terminate on the device" cannot be offloaded.

upvoted 2 times

4study 3 years, 1 month ago

I agree with C. Prefilter policies fit what is asked better I think

upvoted 2 times

Sarbi 3 years, 2 months ago

C is more appreciate an answer

upvoted 1 times

netwguy 3 years, 4 months ago

Its either A or C - im going for C. The problem with A is that if we bypass ACPs, then we not only bypass inspection, but also "ACL" control of traffic - entire encryption domains will be allowed. My problem with C is the use of the word "ignore". We do not want to "ignore" the VPN traffic, we just want to pass it though without inspection. C seems to be more correct - im guessing "ignore" is supposed to mean "ignore inspection" - terrible phrasing once more from Cisco.

upvoted 2 times

Weyland 2 years, 1 month ago

VPN Filter ACL and authorization ACL downloaded from aaa server are still applied if we bypass access control. And Prefilter cannot offload IPsec.

upvoted 1 times

cryptofetti 3 years, 4 months ago

Could be A or C. 50/50 chance here

upvoted 1 times

cryptofetti 3 years, 4 months ago

Leaning more towards C, since you can create a prefilter and fastpath VPN traffic

upvoted 2 times

Question #61 *Topic 1*

An administrator is working on a migration from Cisco ASA to the Cisco FTD appliance and needs to test the rules without disrupting the traffic. Which policy type should be used to configure the ASA rules during this phase of the migration?

A. Prefilter

B. Intrusion

C. Access Control

D. Identity

Suggested Answer: *C*

Community vote distribution

C (53%) A (47%)

TECH3K3 4 weeks ago

Selected Answer: C

I will go with C.
When I migrated an ASA to a FTD, I used the migration tool convert the ASA ACL to FTD ACP. Then you sent the rules to monitor mode.
Remember affecting traffic are actions like permit or deny and so on, which monitor mode doesn't affect as you are see what rules are being used without affecting the traffic.

upvoted 1 times

Silexis 4 months, 4 weeks ago

Selected Answer: C

I am not sure you can test ASA rules on FTD without having an ACP (and use Prefilter to exclude everything)
I will go on C with ACP on TRUST, without SI, QoS and IP
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212321-clarify-the-firepower-threat-defense-acc.html#toc-hId--311118177

upvoted 1 times

TECH3K3 4 weeks ago

Use ACP and put in Monitor mode to evaluate what is being used/hit but not affecting the outcome

upvoted 1 times

14a1949 5 months, 2 weeks ago

Selected Answer: A

he correct answer is actually A. Prefilter.

Prefilter policies are designed to quickly filter traffic before it reaches the deeper inspection engines, allowing you to test rules without disrupting the traffic. This is particularly useful during a migration phase, as it ensures that the network's performance is not impacted while you configure and test the new rules.

Access Control policies (Option C) are used to define and enforce security rules, but they do not specifically provide the capability to test rules without affecting traffic in the same way that prefilter policies do.

upvoted 1 times

14a1949 5 months, 3 weeks ago

Selected Answer: C

the correct answer is actually A. Prefilter.

Prefilter policies are designed to quickly filter traffic before it reaches the deeper inspection engines, allowing you to test rules without disrupting the traffic. This is particularly useful during a migration phase, as it ensures that the network's performance is not impacted while you configure and test the new rules.

Access Control policies (Option C) are used to define and enforce security rules, but they do not specifically provide the capability to test rules without affecting traffic in the same way that prefilter policies do.

upvoted 1 times

rbrain 6 months, 3 weeks ago

Selected Answer: A

I change my mind to A after reading this document --> https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/prefiltering_and_prefilter_policies.html
Fastpath vs Trust discussion
Fastpath and there for prefilter wins because it bypasses all further inspection and handling instead of only exempt from deep inspection and discovery, aka Trust function in ACL.
On top of that you only have to configure it once in the ACL policy instead on per rule base

upvoted 2 times

Kris92 10 months, 1 week ago

Selected Answer: A

Both Prefilter and ACP are correct here, there are a bunch of discussions on the community around this topic, generally speaking I would probably go with ACP, but I believe that by default the migration tool will migrate the rules to prefilter and that's the answer they are going for here.
https://community.cisco.com/t5/network-security/firepower-prefilter-or-access-control-policy/td-p/3832096
https://community.cisco.com/t5/network-security/asa-to-ftd-policy-migration-best-practice/td-p/3081218
https://community.cisco.com/t5/network-security/asa-ftd-migration-prefilter-policy-or-access-control-policy/td-p/4587384

upvoted 1 times

gc999 1 year, 6 months ago

Selected Answer: A

I choose A

upvoted 4 times

SegaMasterSystemAdmin 1 year, 6 months ago

Selected Answer: C

I would use ACP in this case because you can "Allow" or "Trust" the traffic in the rules and you can turn off IPS if needed or use IDS which will not disrupt the traffic but personally to test the rules, I would allow the traffic with IDS added to the rules, and of course logging enabled. Prefilter would bypass inspection and just use the LINA process so it would be useless to keep the rules there and not get the benefits of using a FTD.

https://community.cisco.com/t5/network-security/asa-ftd-migration-prefilter-policy-or-access-control-policy/td-p/4587384

upvoted 3 times

> **SegaMasterSystemAdmin** 1 year, 6 months ago
>
> Based on the Cisco community thread you can multi-select all of your rules and edit common attributes in a single action, including the inspection policy. This would definitely be handy when you have hundreds of rules
>
> upvoted 1 times

Initial14 1 year, 8 months ago

Selected Answer: A

When you migrate from ASA to FTD you use prefilter. The question states: "to test the rules without disrupting the traffic" this is done with prefilter. With prefilter you only have rules based on L3 and L4, same as ASA. This is also in cisco's whitepaper regarding migration from ASA to FTD

upvoted 4 times

> **Initial14** 1 year, 8 months ago
>
> Agree 100%. This is also documented in Cisco WP regarding migration from ASA rules to FTD
>
> upvoted 1 times

Weyland 2 years, 1 month ago

Prefilter requires FTD, question is about ASA. That removes A as an answer.

upvoted 1 times

> **gc999** 1 year, 6 months ago
>
> It said ASA "rules", not "device. Besides, for the migration, it does not need to modify ASA device setting. I choose A
>
> upvoted 1 times

BorZol 2 years, 3 months ago

Using prefilter you do not have so granular filter possibilities. ACP with monitor can be your solution.

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: C

Correct answer is: C

upvoted 2 times

> **TECH3K3** 4 weeks ago

Correct, use ACP and put in Monitor mode

upvoted 1 times

kj2022 2 years, 7 months ago

A is the right answer

upvoted 2 times

Grandslam 2 years, 9 months ago

Selected Answer: C

Im not 100% sure but I would think ACP would be better than Prefilter... With ACP you set the action to "Monitor" wheresa Prefilter you can only fastpath or block... Fastpath could be an option for Prefilter but this only bypasses SNORT... "Monitor" with ACP sounds better.

ACP—Every access control rule has an action that determines how the system handles and logs matching traffic. You can either perform an allow, trust, monitor, block, or block with reset action on an access control rule.

Prefilter—A rule's action determines how the system handles and logs matching traffic. You can either perform a fastpath and block.

upvoted 4 times

Gabranch 1 year, 7 months ago

Monitor does not pass the traffic. It logs and keeps working its way down the ACP. You may be thinking of 'Trust'.

upvoted 1 times

SanchezEldorado 2 years, 8 months ago

Agreed

upvoted 1 times

Question #62 *Topic 1*

A network administrator is seeing an unknown verdict for a file detected by Cisco FTD. Which malware policy configuration option must be selected in order to further analyze the file in the Talos cloud?

A. malware analysis

B. dynamic analysis

C. sandbox analysis

D. Spero analysis

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **d0980cc** 2 months, 2 weeks ago

Selected Answer: B

B
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2199-000005fa:~:text=identification%20of%20malware.-,Dynamic%20analysis,-Thorough%20analysis%20of

upvoted 1 times

⊟ **Initial14** 9 months ago

Selected Answer: B

Only B. The sandbox env. in FMC is dynamic analysis. Spero is only for MSexe files.

upvoted 2 times

⊟ **tanri04** 9 months, 3 weeks ago

MY Answer: A

It is possible that A, "Malware analysis," could also be a valid option for further analyzing the file in the Talos cloud when an unknown verdict is encountered for a file detected by Cisco FTD. Malware analysis involves analyzing known malware to identify its characteristics and behavior, and this could also be useful in identifying unknown malware.

However, sandbox analysis is generally considered to be a more comprehensive option for analyzing unknown files, as it involves executing the file in a controlled environment and monitoring its behavior to detect any malicious activity.

So while A could be a valid option in some cases, C, "Sandbox analysis," is typically the more appropriate option for further analyzing unknown files in the Talos cloud.

upvoted 2 times

⊟ **japm1801** 1 year, 4 months ago

Selected Answer: B

Spero and dynamic analysis acomplish the file disposition and both goes to the cloud , but spero is only on exe files, the question says "a file", so i go to B

upvoted 1 times

⊟ **Maleck** 1 year, 5 months ago

Shouldn't it be D. Spero Analysis. The file is analyzed in the Cloud. As for me, they are referencing AMP Cloud right?

upvoted 1 times

Question #63 *Topic 1*

An engineer has been tasked with providing disaster recovery for an organization's primary Cisco FMC. What must be done on the primary and secondary Cisco
FMCs to ensure that a copy of the original corporate policy is available if the primary Cisco FMC fails?

A. Restore the primary Cisco FMC backup configuration to the secondary Cisco FMC device when the primary device fails.

B. Connect the primary and secondary Cisco FMC devices with Category 6 cables of not more than 10 meters in length.

C. Configure high-availability in both the primary and secondary Cisco FMCs.

D. Place the active Cisco FMC device on the same trusted management network as the standby device.

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html

Community vote distribution

C (100%)

greeklover84 1 year ago

Selected Answer: C

HA will help since A will fail...Stand by node will take over.

I will go for C

upvoted 1 times

BorZol 1 year, 9 months ago

What must be done on primary AND secondary FMC... answer A mention only one of them.

upvoted 1 times

hz033 2 years, 1 month ago

What about A in this case ?

upvoted 2 times

> **Grandslam** 2 years, 1 month ago
>
> A works... C is better.
>
> upvoted 2 times

Question #64 *Topic 1*

An engineer is attempting to add a new FTD device to their FMC behind a NAT device with a NAT ID of ACME001 and a password of Cisco0391521107. Which command set must be used in order to accomplish this?

A. configure manager add<FMC IP> <registration key>ACME001

B. configure manager add ACME001<registration key> <FMC IP>

C. configure manager add <FMC IP>ACME001<registration key>

D. configure manager add DONTRESOLVE <FMC IP> AMCE001<registration key>

Suggested Answer: *A*

Community vote distribution

A (100%)

14a1949 5 months, 3 weeks ago

Selected Answer: A

The DONTRESOLVE option is indeed necessary when the FMC is behind NAT and not directly reachable by the FTD. If the FTD is the one behind NAT, the command would be:

A. configure manager add ACME001

This command uses the NAT ID and registration key to register the FTD with the FMC.

upvoted 1 times

jewell2j 12 months ago

Selected Answer: A

I'd say A is correct, assuming the poor wording of the question is supposed to tell us that the FTD is behind NAT. The wording of the question seems to suggest that the FMC is behind the NAT, in which case, no answer is correct.

upvoted 1 times

Initial14 1 year, 3 months ago

There is no right answer... All the answers have <FMC IP>

upvoted 2 times

liqucika 2 years, 5 months ago

Selected Answer: A

A is correct. You can't have DONTRESOLVE and an FMC IP. It's either or.

upvoted 2 times

Bobster02 2 years, 11 months ago

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

upvoted 1 times

kakakayayaya 3 years ago

There are no any right answer.
That's the syntax:
configure manager add DONTRESOLVE reg_key nat_id

upvoted 4 times

SanchezEldorado 2 years, 2 months ago

I agree that there is no right answer. I read the question as if the FMC is behind nat. In this case Kaka is correct. If it means that the FTD is behind nat, then A is correct.

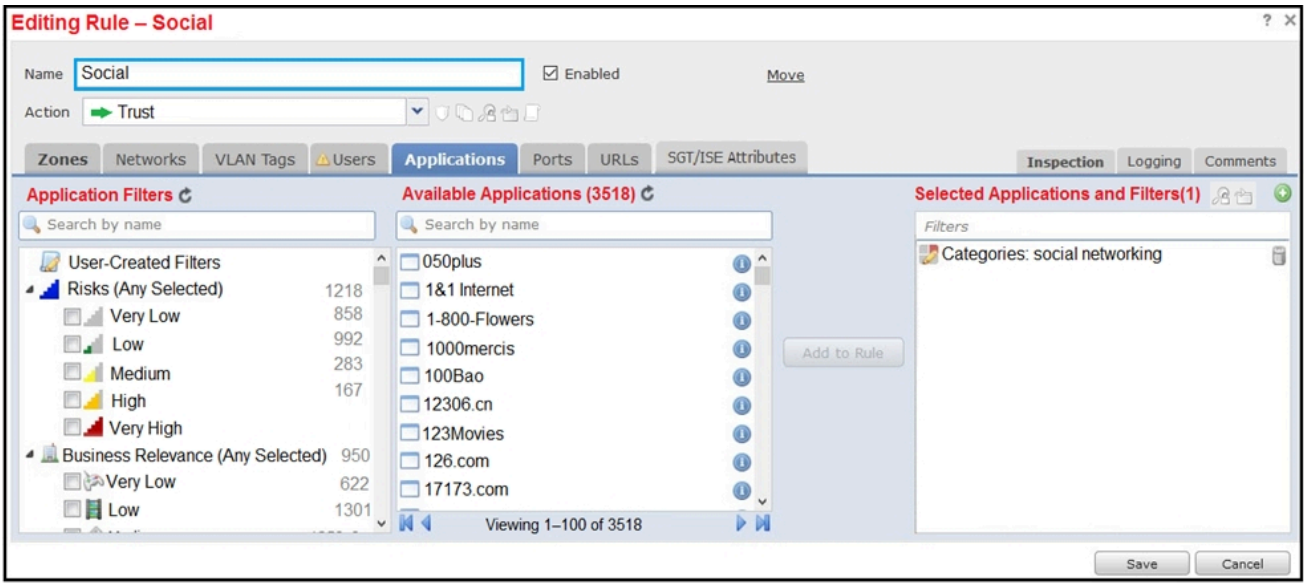
upvoted 2 times

essie007 2 years, 11 months ago

Your syntax is only required when FMC is NATted and unreachable from FTD. The provided answer is correct if the FTD is NATted.

upvoted 2 times

Question #65 Topic 1



Editing Rule – Social

Name: Social

☑ Enabled

Action: Trust

Selected Applications and Filters(1)

Categories: social networking

Refer to the exhibit. An organization has an access control rule with the intention of sending all social media traffic for inspection. After using the rule for some time, the administrator notices that the traffic is not being inspected, but is being automatically allowed. What must be done to address this issue?

A. Add the social network URLs to the block list.

B. Change the intrusion policy to connectivity over security.

C. Modify the selected application within the rule.

D. Modify the rule action from trust to allow.

Suggested Answer: *D*

Community vote distribution

D (100%)

⊟ **4study** Highly Voted 2 years, 1 month ago

Selected Answer: D

D is the correct answer as other have mentioned.

upvoted 8 times

⊟ **majid94** Highly Voted 2 years, 6 months ago

D is 100% correct

upvoted 6 times

⊟ **DID123** Most Recent 10 months, 2 weeks ago

Selected Answer: D

it's D 100%

upvoted 1 times

⊟ **aalnman** 1 year, 6 months ago

Selected Answer: D

D = 100% correct

upvoted 1 times

⊟ **xziomal9** 1 year, 6 months ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

⊟ **Reece_S** 1 year, 7 months ago

C is correct. Any Applications selected are being allowed regardless if the action is trust or allow. If this was a Block rule, then putting the category Social would be correct. In this rule, everything except social will need to be selected for it to work. URL filtering actually needs a Block rule or in an

Allow, allow everything except what you want to block.
upvoted 1 times

⊟ **BorZol** 1 year, 3 months ago
ur right. But it is application filtering not url. Check the screenshot.
upvoted 1 times

⊟ **liqucika** 1 year, 11 months ago
Selected Answer: D
Trust bypasses inspection. Allow will let traffic continue on for further inspection.
upvoted 2 times

⊟ **Sarbi** 2 years, 3 months ago
D is the
correct answer.
upvoted 2 times

⊟ **AS04** 2 years, 4 months ago
D is correct, In general ACP- the action "allow" will send the traffic to the snort engine to inspect and in pre-filter the action "analyze" will send it to ACP.
upvoted 3 times

⊟ **Bobster02** 2 years, 6 months ago
Correct answer is D indeed.

Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/access_control_rules.html
upvoted 4 times

⊟ **michingon** 2 years, 6 months ago
The right answer is "D"
upvoted 3 times

⊟ **kakakayayaya** 2 years, 6 months ago
Trust means no inspection.
We need to allow traffic.
upvoted 3 times

Question #66 *Topic 1*

A user within an organization opened a malicious file on a workstation which in turn caused a ransomware attack on the network. What should be configured within the Cisco FMC to ensure the file is tested for viruses on a sandbox system?

A. Spero analysis

B. capacity handling

C. local malware analysis

D. dynamic analysis

Suggested Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html#ID-2199-000005d8

tanri04 9 months, 3 weeks ago

D. Dynamic analysis.

To ensure that files are tested for viruses on a sandbox system, the Cisco FMC should be configured to perform dynamic analysis on files. Dynamic analysis is a security technique that involves executing files in a sandbox environment and observing their behavior to determine whether they are malicious.

The Cisco FMC supports dynamic analysis using its Advanced Malware Protection (AMP) feature, which includes a cloud-based sandbox for analyzing files. The AMP feature analyzes files in real-time to detect malware and other malicious activity.

Local malware analysis and spere analysis are not appropriate solutions for testing files for viruses on a sandbox system. Local malware analysis involves scanning files using antivirus software installed on the local system, which is not as effective as dynamic analysis. Sphere analysis involves analyzing files in a separate virtual environment, but it is not as comprehensive as dynamic analysis.

Capacity handling is a general term that refers to the ability of a system to handle a large volume of traffic or data, and is not related to testing files for viruses on a sandbox system.

upvoted 2 times

eazy99 1 year, 9 months ago

The answer is correct, and this link will explain each option in case you are interested to know the differences:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#ID-2199-000005fa

upvoted 3 times

Question #67 *Topic 1*

An engineer configures a network discovery policy on Cisco FMC. Upon configuration, it is noticed that excessive and misleading events are filling the database and overloading the Cisco FMC. A monitored NAT device is executing multiple updates of its operating system in a short period of time. What configuration change must be made to alleviate this issue?

A. Exclude load balancers and NAT devices.

B. Leave default networks.

C. Increase the number of entries on the NAT device.

D. Change the method to TCP/SYN.

Suggested Answer: *A*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Network_Discovery_Policies.html

14a1949 5 months, 3 weeks ago

Selected Answer: A

To alleviate the issue of excessive and misleading events filling the database and overloading the Cisco FMC, the recommended configuration change is to exclude load balancers and NAT devices from the network discovery policy. This will help reduce the number of unnecessary events generated by these devices.

So, the correct answer is: A. Exclude load balancers and NAT devices.

upvoted 1 times

Doris8000 9 months, 2 weeks ago

the answer is correct: The system can identify many load balancers and NAT devices by examining your network traffic.

upvoted 2 times

Question #68 *Topic 1*

A network administrator notices that remote access VPN users are not reachable from inside the network. It is determined that routing is configured correctly; however, return traffic is entering the firewall but not leaving it. What is the reason for this issue?

A. A manual NAT exemption rule does not exist at the top of the NAT table

B. An external NAT IP address is not configured

C. An external NAT IP address is configured to match the wrong interface

D. An object NAT exemption rule does not exist at the top of the NAT table

Suggested Answer: *A*

Community vote distribution

A (91%) 9%

⊟ **14a1949** 5 months, 3 weeks ago

Selected Answer: A

The issue described is likely due to the absence of a NAT exemption rule, which is necessary for allowing return traffic to pass through the firewall correctly. In this case, the most appropriate answer is:

A. A manual NAT exemption rule does not exist at the top of the NAT table

Without this rule, the firewall might be dropping the return traffic because it doesn't match any existing NAT rules, leading to the observed behavior where traffic enters the firewall but does not leave it.

upvoted 1 times

⊟ **houhou12322** 9 months, 3 weeks ago

I think its a problem of expression precession "object NAT exemption rule" is more precise than "manual NAT exemption rule" (it means that we are using objects)
i don't understand these kind of questions

upvoted 1 times

⊟ **Stevens0103** 1 year, 4 months ago

Selected Answer: A

"The NAT exemption is a preferred translation method used to prevent traffic to be routed to the internet when it is intended to flow over a VPN tunnel (Remote Access or Site-to-Site).

This is needed when the traffic from your internal network is intended to flow over the tunnels without any translation."

https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215875-configure-anyconnect-vpn-client-on-ftd.html#toc-hId-809586599

upvoted 2 times

⊟ **Cokamaniako** 2 years, 1 month ago

Selected Answer: A

According with jamp1801

upvoted 1 times

⊟ **Joe_Blue** 2 years, 3 months ago

Selected Answer: A

The reason for this issue is likely that an object NAT exemption rule does not exist at the top of the NAT table. This is necessary to allow return traffic to leave the firewall and reach the remote access VPN users. Without this rule, the firewall may perform NAT on the return traffic, causing it to be dropped or lost.

upvoted 1 times

⊟ **japm1801** 2 years, 10 months ago

Selected Answer: A

According to my knoledge about teminology, object nat does not exist in FTD, only in ASA

In FTD you have manual(before and after) and auto nat rules

in production enviroments it is common to create a manual nat rule before to do a NONAT for VPN Traffic, so i'll go with A

upvoted 3 times

xziomal9 3 years ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

xziomal9 3 years ago

Correct answer is: A

upvoted 1 times

cewe 3 years, 4 months ago

Selected Answer: A

Answer A seems to be correct

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

upvoted 2 times

liqucika 3 years, 5 months ago

Selected Answer: A

NAT exemptions can only be done with manual rules before Auto/Object NAT.

upvoted 1 times

dariol 3 years, 10 months ago

D can't be correct. What is needed is a NAT exemption rule and that can only be achieved with a manual NAT rule.

A is correct.

upvoted 4 times

dariol 3 years, 10 months ago

The only way D can be correct is if the answer is meant as an exemption rule for the existing object NAT rule does not exist. That exemption rule would then be a manual NAT rule.

upvoted 1 times

Bobster02 3 years, 11 months ago

I will take it back. Original answer D is correct!

upvoted 2 times

Bobster02 4 years ago

Confirmed A is correct:

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212702-configure-and-verify-nat-on-ftd.html

upvoted 1 times

kakakayayaya 4 years ago

I think A is right

upvoted 1 times

Question #69 *Topic 1*

An administrator is creating interface objects to better segment their network but is having trouble adding interfaces to the objects. What is the reason for this failure?

A. The interfaces are being used for NAT for multiple networks

B. The administrator is adding interfaces of multiple types

C. The administrator is adding an interface that is in multiple zones

D. The interfaces belong to multiple interface groups

Suggested Answer: *B*

Community vote distribution

B (100%)

dariol Highly Voted 3 years, 4 months ago

B is correct.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4

"All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains."

C can't be correct because you can't have one interface in multiple zones to begin with.

upvoted 10 times

achille5 Most Recent 8 months, 1 week ago

Selected Answer: B

All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4
The Interface Objects page of the object manager lists the security zones and interface groups configured on your managed devices. The page also displays the type of interfaces in each interface object, and you can expand each interface object to view which interfaces on which devices belong to each object.

upvoted 1 times

BorZol 2 years, 3 months ago

Selected Answer: B

B is correct.
All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: B

Correct answer is: B

upvoted 1 times

orotta 2 years, 11 months ago

I think the correct answer is B:

All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.

upvoted 2 times

liqucika 2 years, 11 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4

upvoted 2 times

⊟ **jamesque23** 3 years, 1 month ago

B - Dariol is right

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#ID-2243-000009b4

All interfaces in an interface object must be of the same type: all inline, passive, switched, routed, or ASA FirePOWER. After you create an interface object, you cannot change the type of interfaces it contains.

upvoted 1 times

⊟ **Sarbi** 3 years, 3 months ago

The correct answer is c.

upvoted 2 times

⊟ **Heorhiiyatskovskyi** 3 years, 4 months ago

Correct answer is C

Because - Security zones—An interface can belong to only one security zone.

Interface groups—An interface can belong to multiple interface groups (and to one security zone).

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html#:~:text=Security%20zones%E2%80%94An%20interface%20can%20belong%20to%20only%20one%20security%20zone.

upvoted 1 times

⊟ **Bobster02** 3 years, 5 months ago

NO, original D answer is correct!

upvoted 1 times

⊟ **kakakayayaya** 3 years, 6 months ago

B is more fit

upvoted 1 times

⊟ **kakakayayaya** 3 years, 6 months ago

Interface can belong to multiple groups. Odd answer.

upvoted 1 times

Question #70 *Topic 1*

An organization is using a Cisco FTD and Cisco ISE to perform identity-based access controls. A network administrator is analyzing the Cisco FTD events and notices that unknown user traffic is being allowed through the firewall. How should this be addressed to block the traffic while allowing legitimate user traffic?

A. Modify the Cisco ISE authorization policy to deny this access to the user

B. Modify Cisco ISE to send only legitimate usernames to the Cisco FTD

C. Add the unknown user in the Access Control Policy in Cisco FTD

D. Add the unknown user in the Malware & File Policy in Cisco FTD

Suggested Answer: *C*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-identity.html#concept_655B055575E04CA49B10186DEBDA301A

d0980cc 2 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-identity.html#concept_655B055575E04CA49B10186DEBDA301A:~:text=provide%20these%20users.-,Dealing%20with%20Unknown%20Users,-When%20you%20configure

upvoted 1 times

StewieFTW22 3 months, 2 weeks ago

Selected Answer: A

I would block it on ISE — The unknown user is passing aaa somehow, so even if they were blocked on FTD, they would still be able to communicate with internal resources.

upvoted 1 times

gwb 9 months ago

Handling Unknown Users:
Depending on your security requirements, you can configure the ACP to handle unknown users in different ways:
Block Action: You can create a rule in the ACP with a block action specifically for unknown users. This ensures that any traffic from unidentified sources is denied.

Example Configuration:
Let's say you want to block traffic from unknown users. Here's how you can set up an ACP rule:
Rule Name: Unknown User Block
Source: Any (since we're targeting unknown users)
Destination: Specific network or host (customize based on your requirements)
Services: Specify the relevant services (e.g., HTTP, HTTPS, etc.)
Action: Block
Logging: Enable logging for visibility

So, tehcnically it is possible for FMC to block unknown user through ACP rules. However, in real world, unknown user should be blocked (unauthorized) from ISE (port level). In that case A more makes sense, but from FMC perspective, C is ok. My choice is C

upvoted 2 times

cryptofetti 3 years, 4 months ago

-This one makes no sense. My guess is A or B
-How would you create an ACP and add an unknown user if ISE is currently profiling endpoints?

upvoted 1 times

dariol 3 years, 4 months ago

Unkown is a special identity that can be used in a rule if you use identity policies. C is correct.

upvoted 8 times

Question #71 *Topic 1*

What is the benefit of selecting the trace option for packet capture?

A. The option indicates whether the packet was dropped or successful.

B. The option indicates whether the destination host responds through a different path.

C. The option limits the number of packets that are captured.

D. The option captures details of each packet.

Suggested Answer: *A*

Community vote distribution

A (100%)

Heorhiiyatskovskyi Highly Voted 2 years, 10 months ago

Correct answer is A. Because - Packet capture is available with the trace option, which provides you with a verdict as to whether the packet is dropped or suc

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/troubleshooting_the_system.html#:~:text=Packet%20capture%20is%20available%20with%20the%20trace%20option%2C%20which%20provides%20you%

upvoted 9 times

bassfunk Most Recent 10 months, 3 weeks ago

I'm not sure how limiting the number of packets is a benefit. I'd go with A.

upvoted 2 times

THEODORABLE 1 year, 1 month ago

OK, I go with A, the trace option limits the number of packets to be traced, does not limit the amount of packets collected in the capture. tricky question. Plus the verbage in the referenced document says Packet capture is available with the trace option, which provides you with a verdict as to whether the packet is dropped or successful.

upvoted 1 times

xziomal9 2 years ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

xYanivDx 2 years, 1 month ago

Selected Answer: A

Packet capture is available with the trace option, which provides you with a verdict as to whether the packet is dropped or successful.

upvoted 1 times

harshal0408 2 years, 1 month ago

A & D looks me correct

upvoted 2 times

liqucika 2 years, 5 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/troubleshooting_the_system.html#:~:text=Packet%20capture%20is%20available%20with%20the%20trace%20option%2C%20which%20provides%20you%

upvoted 1 times

Sarbi 2 years, 9 months ago

Looks to me A.

he packet capture feature with trace option allows real packets that are captured on the ingress interface to be traced through the system. The trace information is displayed at a later stage. These packets are not dropped on the egress interface, as they are real data-path traffic. Packet capture for Firepower Threat Defense devices supports troubleshooting and analysis of data packets.

Once the packet is acquired, snort detects the tracing flag that is enabled in the packet. Snort writes tracer elements, through which the packet traverses. Snort verdict as a result of capturing packets can be one of DROP/ALLOW/Would DROP.

The file-size option is used when you need to capture packets with the size limit more than 32 MB.

upvoted 3 times

netwguy 2 years, 10 months ago

100% A - look at the link from Heorhiiyatskovskyi if in doubt. Trace just gives you packet-trace info - does not capture any packet-details - just provides packet processing info.

upvoted 2 times

AS04 2 years, 11 months ago

The answer is A, trace does provide detail but you ultimately look at the result portion to see if the packet allowed or dropped.

upvoted 3 times

Bobster02 2 years, 11 months ago

D is the only logical answer.

upvoted 2 times

jimmyjose 3 years, 2 months ago

Answer: D

Packet Capture Overview

The packet capture feature with trace option allows real packets that are captured on the ingress interface to be traced through the system. The trace information is displayed at a later stage. These packets are not dropped on the egress interface, as they are real data-path traffic. Packet capture for Firepower Threat Defense devices supports troubleshooting and analysis of data packets.

Reference:-

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

upvoted 1 times

thefiresays 3 years, 2 months ago

Enable the packet trace to check how the real TCP SYN packets are handled by the firewall. By default, only the first 50 ingress packets are traced:

firepower# capture CAPI trace

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215092-analyze-firepower-firewall-captures-to-e.html

upvoted 2 times

James3222 3 years, 3 months ago

Answer: D

The trace function provides additional details when doing a packet capture.

"Tracing a real packet can be very useful to troubleshoot connectivity issues. It allows you to see all the internal checks that a packet goes through."

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc13

upvoted 3 times

SanchezEldorado 2 years, 2 months ago

Trace doesn't capture details of the "packet". It shows the details of the Trace. Aka What NAT rule, Access Rule, Route lookup. It's the processing of the packet, not the packet details.

upvoted 1 times

Question #72 *Topic 1*

After deploying a network-monitoring tool to manage and monitor networking devices in your organization, you realize that you need to manually upload an MIB for the Cisco FMC. In which folder should you upload the MIB file?

A. /etc/sf/DCMIB.ALERT

B. /sf/etc/DCEALERT.MIB

C. /etc/sf/DCEALERT.MIB

D. system/etc/DCEALERT.MIB

Correct Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-External-

Responses.pdf

tinyJoe 5 months, 3 weeks ago

Selected Answer: C

It's C.

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/760/management-center-admin-76/report-alert-responses.html#:~:text=DCEALERT.MIB

upvoted 1 times

Question #73 *Topic 1*

Which command is run at the CLI when logged in to an FTD unit, to determine whether the unit is managed locally or by a remote FMC server?

A. system generate-troubleshoot

B. show configuration session

C. show managers

D. show running-config | include manager

Correct Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/c_3.html

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

Which command should be used on the Cisco FTD CLI to capture all the packets that hit an interface?

A. configure coredump packet-engine enable

B. capture-traffic

C. capture

D. capture WORD

Suggested Answer: *D*

Community vote distribution

D (78%) C (22%)

⊟ **James3222** Highly Voted 👍 3 years, 2 months ago

Answer: C

Reason: the command "capture-traffic" is used for SNORT Engine Captures. To capture a LINA Engine Capture, you use the "capture" command. Since the Lina Engine represents the actual physical interface of the device, "capture" is the only reasonable choice

Reference: https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc10

upvoted 13 times

⊟ **THEODORABLE** 1 year, 1 month ago

capture command syntax needs a "WORD"/filename after it so "D" is my choice

upvoted 1 times

⊟ **Grandslam** Highly Voted 👍 1 year, 10 months ago

Selected Answer: D

Capture [word]... You have to give the capture a name.

upvoted 5 times

⊟ **d0980cc** Most Recent ⊙ 3 months, 3 weeks ago

Selected Answer: D

The specific command to capture all traffic on an interface:

capture <capture-name> interface <interface-name>

I reluctantly choose D because the interface option is not given.

upvoted 1 times

⊟ **14a1949** 5 months, 2 weeks ago

Selected Answer: D

The correct command to capture all packets that hit an interface on the Cisco FTD CLI is:

D. capture WORD

This command allows you to specify the interface and capture parameters, making it versatile for different capture needs[1](https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html)[2](https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html).

upvoted 1 times

⊟ **14a1949** 5 months, 2 weeks ago

Selected Answer: D

The correct command to capture all packets that hit an interface on the Cisco FTD CLI is:

D. capture WORD

This command allows you to specify the interface and capture parameters, making it versatile for different capture needs[1](https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/ac_1.html)[2](https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html).

upvoted 1 times

LangaMos 11 months, 3 weeks ago

You all think too hard

To capture traffic from the Firewall Engine, you use the capture command.

The capture-traffic command captures the traffic from the Firepower engine.

upvoted 2 times

THEODORABLE 1 year, 1 month ago

D-- again check this out: https://community.cisco.com/t5/network-security/firepower-cli-capture-vs-capture-traffic/m-p/4145511#M1073545

upvoted 1 times

Cokamaniako 1 year, 1 month ago

Selected Answer: D

The key word is "that hit an interface" is necessary the interface name

The answer is D

upvoted 2 times

THEODORABLE 1 year, 1 month ago

Answer is B-

They are asking for the cli command on the FTD

upvoted 1 times

THEODORABLE 1 year, 1 month ago

i changed my mind D is my choice

upvoted 2 times

Joe_Blue 1 year, 3 months ago

Selected Answer: D

Here's the syntax: capture <WORD> interface <interface-name> [buffer <buffer-size>] [match <access-list>] [packet-length <packet-length>]

upvoted 4 times

Weyland 1 year, 7 months ago

Selected Answer: C

WORD is syntax, capture is the command

upvoted 3 times

Estebandido2022 1 year, 8 months ago

Selected Answer: D

I recently entered an FTD and when I put the capture command it forces me to give it a name later, so the capture command does not work without WORD

upvoted 2 times

johanhc20 1 year, 11 months ago

Selected Answer: D

Im going with D on this one. You cannot send the command "capture" from CLI - the command needs a name argument following "capture". You can send the command "capture [WORD]" with following <cr> , from both LINA and CLIish.

upvoted 3 times

xziomal9 2 years ago

Correct answer is: C

upvoted 1 times

xYanivDx 2 years, 1 month ago

Selected Answer: C

C Is the right answer

upvoted 1 times

harshal0408 2 years, 1 month ago

C is the correct answer. Here it is asking for Cisco command, not the syntax

upvoted 2 times

SanchezEldorado 2 years, 2 months ago

Selected Answer: D

James is right about the capture-traffic command, but D is a better answer than C. Go into the cli, type "capture" then hit the question mark. The only option is "WORD". WORD represents a capture name. D is more specific than C.

upvoted 3 times

Question #75 *Topic 1*

How many report templates does the Cisco Firepower Management Center support?

A. 20

B. 10

C. 5

D. unlimited

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Working_with_Reports.html

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

Which action should be taken after editing an object that is used inside an access control policy?

A. Delete the existing object in use.

B. Refresh the Cisco FMC GUI for the access control policy.

C. Redeploy the updated configuration.

D. Create another rule using a different object name.

Correct Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html

Currently there are no comments in this discussion, be the first to comment!

Question #77 Topic 1

Which Cisco Firepower feature is used to reduce the number of events received in a period of time?

A. rate-limiting

B. suspending

C. correlation

D. thresholding

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower-module-user-guide-v541/Intrusion-Global-

Threshold.html

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

Which report template field format is available in Cisco FMC?

A. box lever chart

B. arrow chart

C. bar chart

D. benchmark chart

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Working_with_Reports.html

⊟ **cryptofetti** Highly Voted 1 year, 4 months ago

C is correct

-Format - bar / pie / line / table view / detail view

- Table

-Preset

-Search or Filter

-X and y axis

upvoted 6 times

⊟ **xameno87** Most Recent 11 months, 2 weeks ago

I agree c is correct

upvoted 2 times

Question #79 *Topic 1*

Which group within Cisco does the Threat Response team use for threat analysis and research?

A. Cisco Deep Analytics

B. OpenDNS Group

C. Cisco Network Response

D. Cisco Talos

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/products/security/threat-response.html#~benefits

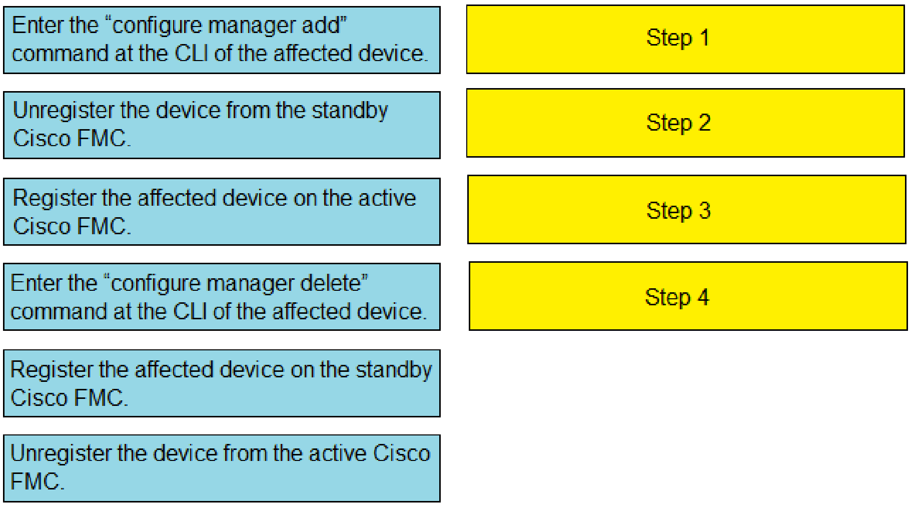
Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

DRAG DROP -

Drag and drop the steps to restore an automatic device registration failure on the standby Cisco FMC from the left into the correct order on the right. Not all options are used.

Select and Place:



Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

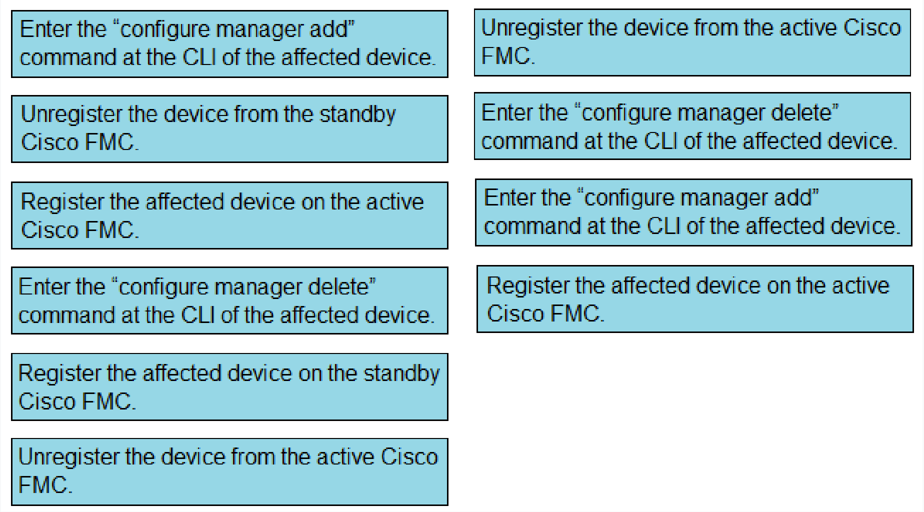
Step 1

Step 2

Step 3

Step 4

Suggested Answer:



Enter the "configure manager add" command at the CLI of the affected device.

Unregister the device from the standby Cisco FMC.

Register the affected device on the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Register the affected device on the standby Cisco FMC.

Unregister the device from the active Cisco FMC.

Unregister the device from the active Cisco FMC.

Enter the "configure manager delete" command at the CLI of the affected device.

Enter the "configure manager add" command at the CLI of the affected device.

Register the affected device on the active Cisco FMC.

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/firepower_management_center_high_availability.html#id_32288

THEODORABLE 7 months, 2 weeks ago

We always do any & all configuration on the active device. The active replicates to the standby.

upvoted 4 times

Question #81 *Topic 1*

Which CLI command is used to generate firewall debug messages on a Cisco Firepower?

A. system support firewall-engine-debug

B. system support ssl-debug

C. system support platform

D. system support dump-table

Suggested Answer: *A*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower-management-center-display-acc.html

THEODORABLE 7 months, 2 weeks ago

A is kinda a no-brainer-- https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212330-firepower-management-center-display-acc.html

upvoted 3 times

Question #82 *Topic 1*

Which command-line mode is supported from the Cisco FMC CLI?

A. privileged

B. user

C. configuration

D. admin

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/command_line_reference.pdf

netwguy 10 months ago

C is correct. Try logging on to a FMC CLI and do a "?" , and you will the the description for "configure" is "change to configuration mode"

upvoted 3 times

Bobster02 11 months, 3 weeks ago

Close enough....

upvoted 1 times

essie007 11 months, 3 weeks ago

According to docs, none of the answers are correct:

"The CLI encompasses four modes. The default mode, CLI Management, includes commands for navigating within the CLI itself. The remaining modes contain commands addressing three different areas of Firepower Management Center functionality; the commands within these modes begin with the mode name: system, show, or configure. "

upvoted 1 times

Question #83 *Topic 1*

Which command is entered in the Cisco FMC CLI to generate a troubleshooting file?

A. show running-config

B. show tech-support chassis

C. system support diagnostic-cli

D. sudo sf_troubleshoot.pl

Suggested Answer: *D*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

Community vote distribution

D (100%)

xYanivDx 7 months, 1 week ago

Selected Answer: D

Enter this command on the Firepower Management Center in order to generate a troubleshoot file:

```
admin@FMC:~$ sudo sf_troubleshoot.pl
```

upvoted 2 times

Question #84 *Topic 1*

Which CLI command is used to control special handling of ClientHello messages?

A. system support ssl-client-hello-tuning

B. system support ssl-client-hello-display

C. system support ssl-client-hello-force-reset

D. system support ssl-client-hello-reset

Suggested Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_command_line_reference.html

Community vote distribution

A (100%)

⊟ **Grandslam** Highly Voted 1 year, 9 months ago

Correct answer not listed :: ssl-client-hello-enabled

upvoted 5 times

⊟ **THEODORABLE** 7 months, 2 weeks ago

I would go with A as the closest correct answer-- ssl-client-hello-enabled

Controls special processing of the ClientHello message during the SSL handshake.

ssl-client-hello-tuning

Allows you to refine how the managed device modifies ClientHello messages during SSL handshakes. This command tunes the default lists of cipher suites, elliptic curves, and extensions that the system allows in ClientHello messages. This command only adds entries to or removes entries from the default lists of allowed values. It does not overwrite the default lists.

upvoted 2 times

⊟ **0000101100** Most Recent 7 months, 4 weeks ago

A, is the correct because it used to configure the different messages within the hello protocols.

upvoted 1 times

⊟ **Baumb** 10 months, 3 weeks ago

A is correct, since display only shows the current configuration.

That leaves tuning as the only viable option since -enabled is not an option

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/classic_device_command_line_reference.html#:~:text=system%20support%20ssl%2Dclient%2Dhello%2Dtuning%20setting%20value

upvoted 1 times

⊟ **xYanivDx** 1 year, 7 months ago

There are no correct answer:

Syntax

system support ssl-client-hello-enabled setting {true | false}

Possible setting values are:

feature

Controls all special handling of ClientHello messages.

upvoted 2 times

⊟ **kj2022** 1 year, 7 months ago

Selected Answer: A

ssl-client-hello-tuning seems to be bit of right

upvoted 2 times

Question #85 *Topic 1*

Which command is typed at the CLI on the primary Cisco FTD unit to temporarily stop running high-availability?

A. configure high-availability resume

B. configure high-availability disable

C. system support network-options

D. configure high-availability suspend

Suggested Answer: *D*

Community vote distribution

D (100%)

ASherbiny_1604 Highly Voted 3 years, 3 months ago

Correct answer should be "D" (Suspend).

If you choose disable, you will PERMANENTLY break the high availability connection.

The keyword here is "TEMPORARILY"

upvoted 10 times

pr0fectus Most Recent 8 months, 1 week ago

Selected Answer: D

Confirmed through FTD CLI:

> configure high-availability

disable Disable high-availability configuration

resume Resume temporarily suspended high-availability configuration

suspend Temporarily suspend high-availability configuration

upvoted 2 times

gc999 1 year ago

Selected Answer: D

I believe "D" is the closest answer. However, the command seems also not correct. The correct one should b e"configure failover suspend"

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/firepower_threat_defense_high_availability.html#id_14658:~:text=configure%20failover%20suspend

upvoted 1 times

matan24 1 year, 4 months ago

Selected Answer: D

What happens to the failover configuration if you manually disable the failover (configure high-availability suspend) and then you reload the device?

When you disable the failover it is not a permanent change (not saved in the startup-config unless you decide to do this explicitly).

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

upvoted 1 times

xziomal9 2 years ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

cewe 2 years, 4 months ago

Selected Answer: D

D is the correct Answer

upvoted 1 times

powerchiken 2 years, 6 months ago

Selected Answer: D

configure high-availability

disable Disable high-availability configuration

resume Resume temporarily suspended high-availability configuration

suspend Temporarily suspend high-availability configuration

upvoted 1 times

⊟ **4study** 2 years, 7 months ago

Selected Answer: D

D is the right one for sure

upvoted 1 times

⊟ **cryptofetti** 2 years, 10 months ago

D, is correct for sure

upvoted 2 times

⊟ **Bobster02** 2 years, 11 months ago

Confirmed: D is correct choice.

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

upvoted 4 times

Question #86 *Topic 1*

Which command must be run to generate troubleshooting files on an FTD?

A. system support view-files

B. sudo sf_troubleshoot.pl

C. system generate-troubleshoot all

D. show tech-support

Suggested Answer: *C*

Community vote distribution

C (100%)

matan24 Highly Voted 10 months ago

Selected Answer: C

C is the correct answer 100%.

Firepower Management Center
Enter this command on the Firepower Management Center in order to generate a troubleshoot file:

```
admin@FMC:~$ sudo sf_troubleshoot.pl

Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
Troubleshoot information successfully created at /var/common/xxxxxx.tar.gz
```

Firepower Devices
Enter this command on FirePOWER devices/modules and virtual managed devices in order to generate a troubleshoot file:

```
> system generate-troubleshoot all

Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient. This may take several minutes.
The troubleshoot option code specified is ALL.
Troubleshoot information successfully created at /var/common/xxxxxx.tar.gz
```

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html

upvoted 5 times

johanhc20 Most Recent 1 year, 5 months ago

Selected Answer: C

C for FTD.
B for FMC.

Ans. "C"

upvoted 1 times

xziomal9 1 year, 6 months ago

Selected Answer: C

Correct answer is: C

upvoted 1 times

SanchezEldorado 1 year, 8 months ago

B and C both seem to be right. I ran B on an FTD from expert mode and ran C from the FMC CLI and they both produce the same output. I'm sure C is preferable though since you don't have to go into expert mode.

upvoted 3 times

⊟ **Aarow** 1 year, 3 months ago

I noticed the exact same thing.

upvoted 2 times

⊟ **cewe** 1 year, 10 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#anc12

upvoted 1 times

⊟ **orotta** 1 year, 11 months ago

The answer is

C. system generate-troubleshoot all

Answer B: sudo sf_troubleshoot.pl is running on FMC

upvoted 1 times

⊟ **ERGEGA** 1 year, 11 months ago

B is the correct answer.

If go as expert user on CLI on FTD then you can run this command.

th e C option it can be run on normal console of FTD.

upvoted 1 times

⊟ **NoOn3x** 1 year, 11 months ago

Selected Answer: C

C for FTD.

B for FMC.

Ans. "C"

upvoted 4 times

⊟ **cryptofetti** 2 years, 4 months ago

Agree, C for sure

upvoted 2 times

⊟ **Bobster02** 2 years, 6 months ago

100% C is correct!

upvoted 4 times

⊟ **jmosilva** 2 years, 6 months ago

Correct answer is C (Tip: this is for FTD and not FMC)

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html#anc12

upvoted 3 times

Question #87 Topic 1

When is the file-size command needed while troubleshooting with packet capture?

A. when capture packets are less than 16 MB

B. when capture packets are restricted from the secondary memory

C. when capture packets exceed 10 GB

D. when capture packets exceed 32 MB

Suggested Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/troubleshooting_the_system.html

Community vote distribution

D (100%)

gwb 10 months ago

"The file-size option is used when you need to capture packets with the size limit more than 32 MB."

upvoted 1 times

greeklover84 1 year, 6 months ago

Selected Answer: D

the reference below is correct !!! thanks

upvoted 1 times

Question #88 *Topic 1*

What is a functionality of port objects in Cisco FMC?

A. to mix transport protocols when setting both source and destination port conditions in a rule

B. to represent protocols other than TCP, UDP, and ICMP

C. to represent all protocols in the same way

D. to add any protocol other than TCP or UDP for source port conditions in access control rules.

Suggested Answer: *B*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/reusable_objects.html

Community vote distribution

B (100%)

14a1949 5 months, 2 weeks ago

Selected Answer: B

B. to represent protocols other than TCP, UDP, and ICMP

This functionality allows port objects in Cisco FMC to include a wide range of additional protocols, providing flexibility in defining access control rules.

upvoted 1 times

trickbot 10 months, 2 weeks ago

Selected Answer: B

B to represent other protocols. In the FMC GUI, when you create a port object, the Protocol field allows: TCP, UDP, ICMP, IPv6-ICMP, OTHER. When you choose other, a drop down box becomes enabled, with 50+ additional protocols, none of which I recognized.

upvoted 2 times

NoOn3x 11 months, 2 weeks ago

According to the documentation, the answer is correct. Ans.B

"A port object can represent other protocols that do not use ports."

And the other options are casually mentioned in the documentation as being wrong.

A and D:
#
When using port objects, observe the following guidelines:
-"You cannot add any protocol other than TCP or UDP for source port conditions in access control rules. Also, you cannot mix transport protocols when setting both source and destination port conditions in a rule."

-"If you create a port object containing both TCP and UDP ports, then add it as a source port condition in a rule, you cannot add a destination port, and vice versa."
#

and answer C:
#Port objects represent different protocols in slightly different ways:
and start with the introduction

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/reusable_objects.html#ID-2243-00000364

upvoted 3 times

kakakayayaya 1 year, 7 months ago

Very vague question.

B - doesn't fit at all cos TCP/UDP/ICMP already exist as default objects.

So what does "other than" mean? Except?

C - fits better.

upvoted 1 times

essie007 1 year, 5 months ago

True but still probably B because of the following sentence in the guide: "A port object can represent other protocols that do not use ports."

upvoted 3 times

Question #89 *Topic 1*

Within Cisco Firepower Management Center, where does a user add or modify widgets?

A. dashboard

B. reporting

C. context explorer

D. summary tool

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using_Dashboards.html

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

A network engineer is configuring URL Filtering on Cisco FTD. Which two port requirements on the FMC must be validated to allow communication with the cloud service? (Choose two.)

A. outbound port TCP/443

B. inbound port TCP/80

C. outbound port TCP/8080

D. inbound port TCP/443

E. outbound port TCP/80

Suggested Answer: *AE*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Security__Internet_Access__and_Communication_Ports.html

cewe 10 months, 1 week ago
A&E are correct
upvoted 2 times

cryptofetti 1 year, 4 months ago
Confirmed, A and E are correct
upvoted 3 times

Question #91 *Topic 1*

What is the maximum bit size that Cisco FMC supports for HTTPS certificates?

A. 1024

B. 8192

C. 4096

D. 2048

Suggested Answer: *C*

Community vote distribution

C (100%)

bassfunk 10 months, 3 weeks ago

I don't feel like these types of questions should be asked as they will obviously change with future releases.

upvoted 4 times

SegaMasterSystemAdmin 1 year ago

Selected Answer: C

It is 4096, Cisco updates their exam questions and answers based on the current technology

upvoted 1 times

saad_SEIU 1 year, 2 months ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/system_configuration.html

upvoted 1 times

Gabranch 1 year, 1 month ago

While it's nice that Firepower is making improvements.... It's frustrating that both 4096 and 2048 are correct, depending on the version being used. Which version is being tested on?

upvoted 2 times

xziomal9 2 years ago

Selected Answer: C

Correct answer is: C

upvoted 1 times

cewe 2 years, 4 months ago

C is the correct Answer, but we are not sure if Cisco updates the answers. Because as the Question war written, it was only 2048

upvoted 1 times

orotta 2 years, 5 months ago

I can see FMC version 6.6 supports 4096

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/system_configuration.html

upvoted 2 times

cryptofetti 2 years, 10 months ago

Yes but when the exam was written I suspect it was still 2048

upvoted 1 times

kakakayayaya 3 years, 1 month ago

Since version 6.2 (incl) all FMC versions supports 4096 HTTPS Certificates.

This is important to know cos u will not be able to enter Web GUI at all.

upvoted 4 times

cryptofetti 2 years, 10 months ago

When the question was written I believe it was only 2048, so I am going with D

upvoted 1 times

trickbot 2 years, 4 months ago

Today the correct answer is 4096. If I fail, and I get such a question, I will contest the exam results.

upvoted 3 times

serse 3 years, 1 month ago

Correct Answer is 4096, after updating cisco website

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/system_configuration.html

upvoted 3 times

Question #92 *Topic 1*

Which limitation applies to Cisco FMC dashboards in a multi-domain environment?

A. Child domains are able to view but not edit dashboards that originate from an ancestor domain.

B. Child domains have access to only a limited set of widgets from ancestor domains.

C. Only the administrator of the top ancestor domain is able to view dashboards.

D. Child domains are not able to view dashboards that originate from an ancestor domain.

Correct Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using_Dashboards.html

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

Which two considerations must be made when deleting and re-adding devices while managing them via Cisco FMC? (Choose two.)

A. An option to re-apply NAT and VPN policies during registration is available, so users do not need to re-apply the policies after registration is completed.

B. Before re-adding the device in Cisco FMC, the manager must be added back.

C. Once a device has been deleted, it must be reconfigured before it is re-added to the Cisco FMC.

D. The Cisco FMC web interface prompts users to re-apply access control policies.

E. There is no option to re-apply NAT and VPN policies during registration available, so users need to re-apply the policies after registration is completed.

Suggested Answer: *BE*

Community vote distribution

BE (57%) DE (43%)

14a1949 5 months, 2 weeks ago

Selected Answer: DE

When a device is deleted and then re-added, the FMC web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/device_management_basics.html

upvoted 2 times

Samer0100 9 months, 1 week ago

Selected Answer: DE

copied from cisco configuration guide

When a device is deleted and then re-added, the FMC web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/device_management_basics.html

upvoted 1 times

freemen810 11 months ago

I have tested in my lab, answer is B and E, the FMC do not prompt user to re-apply policy so D is wrong

upvoted 1 times

Stevens0103 11 months, 2 weeks ago

Selected Answer: DE

It's D & E for sure.

"When a device is deleted and then re-added, the FMC web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete."

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-00000786

When a device is deleted from FMC, the manager is not automatically removed.

upvoted 2 times

bassfunk 1 year, 4 months ago

Selected Answer: BE

I would go with B & E. The manager must be added back before you can add the device.

upvoted 1 times

⊟ **gc999** 1 year, 5 months ago

Selected Answer: DE

D and E are correct.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html#ID-2242-00000786:~:text=When%20a%20device,registration%20is%20complete.

upvoted 1 times

⊟ **Bbb78** 1 year, 7 months ago

option B is also correct - the FTD needs to have the manager added after the FTD is deleted from the FMC(trust me it happened to me) ....but this question is more for FMC - so I would go with DE

upvoted 1 times

⊟ **THEODORABLE** 1 year, 7 months ago

D&E - right from the note in the doc! mid page

upvoted 1 times

⊟ **rcharger00** 2 years, 7 months ago

D&E is correct

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/device_management_basics.html?bookSearch=true

When a device is deleted and then re-added, the FMC web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

upvoted 2 times

⊟ **SanchezEldorado** 2 years, 8 months ago

Selected Answer: BE

E is definitely correct, though I think B is a better answer than C. When registering the device, it does have a box to select the ACP to apply, but it automatically deploys the configuration. When you delete a device from the FMC, you need to go to the FTD's CLI and add the manager before adding the device to the FMC.

upvoted 3 times

> ⊟ **trudint** 1 year, 6 months ago
>
> You don't have to add the manager back to the device *before* you add it in the FMC. I can add the device back in the FMC a year in advance if I want, it will simply sit there and wait for the device to reach out for registration. It's kind of a trick question.
>
> upvoted 1 times
>
> > ⊟ **bassfunk** 1 year, 4 months ago
> >
> > You're over analyzing. You cannot add a device to the FMC without a manager configured on the device. You will get a timeout error after a few minutes.
> >
> > upvoted 1 times
>
> ⊟ **iulianm** 2 years, 3 months ago
>
> I confirm B is corect I tested on cisco lab. Before re-adding the device in Cisco FMC, the manager must be added back. So the answer are BE.
>
> upvoted 1 times

⊟ **netwguy** 3 years, 4 months ago

D+E is correct:

"When a device is deleted and then re-added, the Firepower Management Center web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete. "

upvoted 2 times

Question #94 *Topic 1*

What is a behavior of a Cisco FMC database purge?

A. User login and history data are removed from the database if the User Activity check box is selected.

B. Data is recovered from the device.

C. The appropriate process is restarted.

D. The specified data is removed from Cisco FMC and kept for two weeks.

Suggested Answer: *C*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/management_center_database_purge.pdf

Community vote distribution

C (100%)

iulianm 1 year, 3 months ago

C is corect. https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/management_center_database_purge.pdf

upvoted 3 times

johanhc20 1 year, 5 months ago

DE is correct

When a device is deleted and then re-added, the Firepower Management Center web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Device_Management_Basics.html

upvoted 1 times

Gabranch 7 months, 1 week ago

Wrong question :)

upvoted 1 times

xYanivDx 1 year, 7 months ago

Selected Answer: C

You can use the database purge page to purge discovery, identity, connection, and Security Intelligence data files from the FMC databases. Note that when you purge a database, the appropriate process is restarted.

upvoted 2 times

Question #95 *Topic 1*

Which two packet captures does the FTD LINA engine support? (Choose two.)

A. Layer 7 network ID

B. source IP

C. application ID

D. dynamic firewall importing

E. protocol

Correct Answer: *BE*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

An engineer currently has a Cisco FTD device registered to the Cisco FMC and is assigned the address of 10.10.50.12. The organization is upgrading the addressing schemes and there is a requirement to convert the addresses to a format that provides an adequate amount of addresses on the network. What should the engineer do to ensure that the new addressing takes effect and can be used for the Cisco FTD to Cisco FMC connection?

A. Update the IP addresses from IPv4 to IPv6 without deleting from Cisco FMC.

B. Format and reregister the device to Cisco FMC.

C. Cisco FMC does not support devices that use IPv4 IP addresses.

D. Delete and reregister the device to Cisco FMC.

Suggested Answer: *D*

Community vote distribution

D (100%)

kakakayayaya Highly Voted 3 years, 6 months ago

D is better

upvoted 7 times

japm1801 Highly Voted 2 years, 4 months ago

Selected Answer: D

most people are talking about ipv4 to ipv6 upgrade, i don't think that "upgrading the addressing schemes" refers to change the the addressing to ipv6.

but

discarding wrong asnwers:

A. Update the IP addresses from IPv4 to IPv6 without deleting from Cisco FMC
you can't change management ip addressing while the FTD is still registered in
FMC
B. Format and reregister the device to Cisco FMC.
I don't think that formatting managed devices would be a correct way to do nothing

C. Cisco FMC does not support devices that use IPv4 IP addresses.
Simply false

D. Delete and reregister the device to Cisco FMC.
the best way to change management ip address is to deregister an reregister, this option doesn't fit well in the question but "is the least bad option"

upvoted 6 times

achille5 Most Recent 10 months, 2 weeks ago

Selected Answer: D

Delete and reregister the device to FMC is faster and correct way.

upvoted 1 times

paramar 1 year, 6 months ago

I think you can update the management ip address on the FMC. Edit the FTD under Devices > Device Management. Click the Device tab and update the ip address in the Management widget.

upvoted 1 times

> **paramar** 1 year, 6 months ago
>
> this looks to me like the quickest and easiest way to update the ip address. So I vote for A.
>
> upvoted 3 times

THEODORABLE 1 year, 7 months ago

D-- From the guide: If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.

upvoted 2 times

BorZol 2 years, 3 months ago

Selected Answer: D

japm1801 answer is correct

upvoted 1 times

johanhc20 2 years, 5 months ago

Selected Answer: D

D is correct

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

cewe 2 years, 10 months ago

Selected Answer: D

Correct Answer is D

If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/device_management_basics.html

upvoted 3 times

liqucika 2 years, 11 months ago

Selected Answer: D

If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/device_management_basics.html

upvoted 4 times

onefa 3 years, 1 month ago

A is correct, you are going from IPV4 to IPV6 which allows a better IP addressing scheme. The other options are half answers. IP change requires modify the config on both sides (
FTD and FMC)

upvoted 2 times

Sarbi 3 years, 2 months ago

Reestablish the Management Connection if You Change the FMC IP Address—If you change the FMC IP address or hostname, reestablishing the management connection depends on how you added the device to the FMC.

upvoted 1 times

Sarbi 3 years, 2 months ago

D is the correct option.

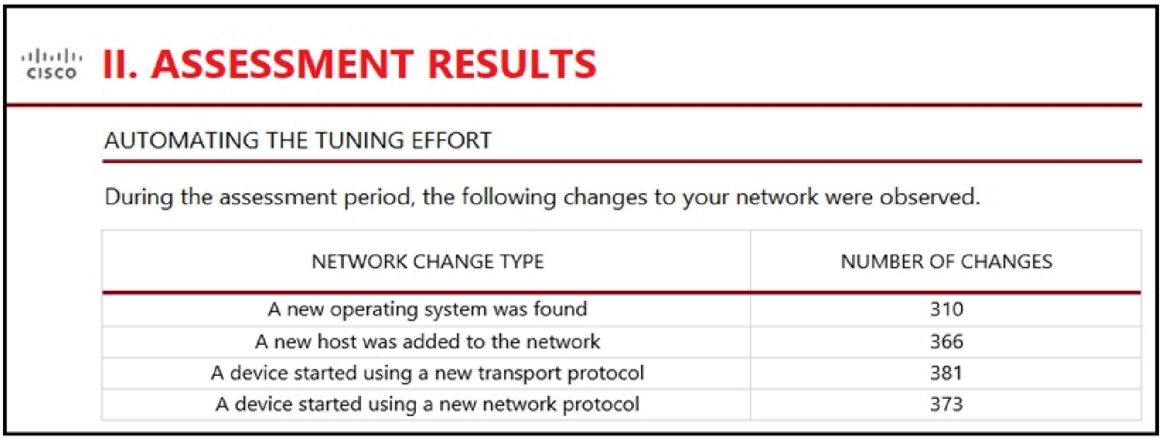
upvoted 4 times

Bobster02 3 years, 6 months ago

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/215540-configure-verify-and-troubleshoot-firep.html

upvoted 2 times

Question #97 *Topic 1*



II. ASSESSMENT RESULTS

AUTOMATING THE TUNING EFFORT

During the assessment period, the following changes to your network were observed.

NETWORK CHANGE TYPE	NUMBER OF CHANGES
A new operating system was found	310
A new host was added to the network	366
A device started using a new transport protocol	381
A device started using a new network protocol	373

Refer to the exhibit. An engineer is analyzing the Attacks Risk Report and finds that there are over 300 instances of new operating systems being seen on the network. How is the Firepower configuration updated to protect these new operating systems?

A. The administrator manually updates the policies.

B. The administrator requests a Remediation Recommendation Report from Cisco Firepower.

C. Cisco Firepower gives recommendations to update the policies.

D. Cisco Firepower automatically updates the policies.

Suggested Answer: *C*

Community vote distribution

C (100%)

japm1801 11 months ago

Selected Answer: C

Firepower Recommendations for IPS policies is a tool that work with network discovery to apply recommendations to IPS policies, but you have to apply that unless you configure your custom IPS policy to automatically take recommendations (not suggested for low end FW like 1010 because of the memory limit)

upvoted 2 times

4study 1 year, 7 months ago

Selected Answer: C

They might be refering to Firepower recomendations in the Intrusion policy, if so then C is correct

upvoted 2 times

cryptofetti 1 year, 10 months ago

I think B, fits better here

upvoted 1 times

Question #98 *Topic 1*

After using Firepower for some time and learning about how it interacts with the network, an administrator is trying to correlate malicious activity with a user. Which widget should be configured to provide this visibility on the Cisco Firepower dashboards?

A. Current Sessions

B. Correlation Events

C. Current Status

D. Custom Analysis

Suggested Answer: *B*

Community vote distribution

B (60%) D (40%)

14a1949 5 months, 2 weeks ago

Selected Answer: B

The Custom Analysis widget (Option D) allows for creating tailored views and reports based on specific criteria, which can be very useful for various types of analysis. However, it is not specifically designed for correlating malicious activity with users.

The Correlation Events widget (Option B) is specifically intended to provide visibility into events triggered by correlation rules, which are designed to detect and track malicious activities. This makes it the most suitable choice for correlating malicious activity with a user on the Cisco Firepower dashboards.

upvoted 1 times

gwb 9 months, 4 weeks ago

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/710/management-center-admin-71/events-correlation-compliance.html

user activity information can be seen from correlation event widget optionally.

upvoted 2 times

Joe_Blue 1 year, 9 months ago

Selected Answer: B

The Correlation Events widget should be configured to provide visibility of malicious activity correlated with a user on the Cisco Firepower dashboards.

upvoted 3 times

xziomal9 2 years, 6 months ago

Selected Answer: D

Correct answer is: D

upvoted 1 times

aadach 2 years, 9 months ago

Selected Answer: D

Only D, on that widget we can find "Malware" and "User"

upvoted 1 times

cryptofetti 3 years, 4 months ago

I think A, fits best here

upvoted 1 times

> **netwguy** 3 years, 4 months ago
>
> A is incorrect. It only displays users logged on to the appliance. D must be the correct answer
>
> upvoted 1 times

Bobster02 3 years, 6 months ago

My choice is answer D.

https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/dashboards.html#ID-2206-00000283

upvoted 4 times

⊟ **kakakayayaya** 3 years, 6 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/dashboards.html#ID-2206-00000283

The Correlation Events widget shows the average number of correlation events per second, by priority.

D - right answer

upvoted 4 times

Question #99 *Topic 1*

An engineer is troubleshooting application failures through an FTD deployment. While using the FMC CLI, it has been determined that the traffic in question is not matching the desired policy. What should be done to correct this?

A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly.

B. Use the system support firewall-engine-dump-user-identity-data command to change the policy and allow the application though the firewall.

C. Use the system support application-identification-debug command to determine which rules the traffic matching and modify the rule accordingly.

D. Use the system support network-options command to fine tune the policy.

Suggested Answer: *C*

Community vote distribution

C (60%) A (40%)

tanri04 Highly Voted 1 year, 9 months ago

Correct answer: A. Use the system support firewall-engine-debug command to determine which rules the traffic matching and modify the rule accordingly.

If traffic is not matching the desired policy, the engineer should use the system support firewall-engine-debug command to determine which rules the traffic is matching and modify the rule accordingly. This command provides detailed information about traffic processing, including the rule that the traffic is matching or not matching, and can help the engineer identify issues with the policy configuration.

Option B, using the system support application-identification-debug command, is not relevant to this scenario, as it is used for troubleshooting issues related to application identification.

Option C, using the system support firewall-engine-dump-user-fdensity-data command, is not relevant to this scenario, as it is used for dumping firewall user data and not related to troubleshooting policy matching issues.
Option D, using the system support network-options command, is not relevant to this scenario, as it is used for fine-tuning network settings and not related to troubleshooting policy matching issues.

upvoted 7 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: A

The system support application-identification-debug command (Option C) is used for debugging issues related to application identification, which can be useful in certain scenarios. However, it is not specifically designed for determining which rules traffic is matching.

The system support firewall-engine-debug command (Option A) is the correct choice because it directly helps identify the specific rules that the traffic is hitting. This allows you to modify the rules accordingly to ensure the traffic matches the desired policy.

upvoted 2 times

14a1949 5 months, 2 weeks ago

Selected Answer: A

The system support application-identification-debug command (Option C) is used for debugging issues related to application identification, which can be useful in certain scenarios. However, it is not specifically designed for determining which rules traffic is matching.

The system support firewall-engine-debug command (Option A) is the correct choice because it directly helps identify the specific rules that the traffic is hitting. This allows you to modify the rules accordingly to ensure the traffic matches the desired policy.

upvoted 1 times

achille5 8 months, 3 weeks ago

Selected Answer: A

Correct answer A

upvoted 3 times

Joninjimbo 1 year, 2 months ago

A confirmed under Scenario 3: Traffic Blocked by Application Tag. "The Connection Events, in conjunction with firewall-engine-debug output, shows the reason for the block."

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214577-firepower-data-path-troubleshooting-phas.html#anc9

upvoted 1 times

⊟ **NoUserName1234** 1 year, 8 months ago

I go with C as well...
In a TECSEC doc I found the following:
An incorrect AppID disposition can cause traffic to match
the wrong access control rule

upvoted 2 times

⊟ **Baumb** 1 year, 10 months ago

Selected Answer: C

Im leaning to C, since were troubleshooting application issues, and application-identification-debug shows the matched application in the FMC

upvoted 3 times

Question #100

Topic 1

An engineer has been asked to show application usages automatically on a monthly basis and send the information to management. What mechanism should be used to accomplish this task?

A. reports

B. context explorer

C. dashboards

D. event viewer

Suggested Answer: *A*

Community vote distribution

A (100%)

Fajoiuytredg 9 months, 1 week ago

Selected Answer: A

Schedule generation of future reports, either once or recurring. See Automating Report Generation. You can customize the schedule on a full range of time frames such as daily, weekly, monthly, and so on.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Working_with_Reports.html#ID-2250-000008dd

upvoted 1 times

Question #101

Topic 1

A network administrator is configuring SNORT inspection policies and is seeing failed deployment messages in Cisco FMC. What information should the administrator generate for Cisco TAC to help troubleshoot?

A. A ג€troubleshootג€ file for the device in question.

B. A ג€show techג€ file for the device in question.

C. A ג€troubleshootג€ file for the Cisco FMC.

D. A ג€show techג€ for the Cisco FMC.

Suggested Answer: *C*

Community vote distribution

C (100%)

Doris8000 11 months ago

C correct https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/troubleshooting_the_system.html#:~:text=Troubleshoot%20file%20generated%20from%20the%20FMC.

upvoted 2 times

japm1801 2 years, 11 months ago

Selected Answer: C

i'm almost 100% secure that is C because deployment failed messages are from FTD deployments from FMC, but the configuration error remains in the FMC, before calling TAC i would rather to look for the failed reasons, the common reasons are misconfigurations (changing names to objects and moving from existing policies, or flexconfig object with syntax errors)

upvoted 4 times

Cisco_2022 3 years, 3 months ago

I will go with C.

upvoted 1 times

NoOn3x 3 years, 5 months ago

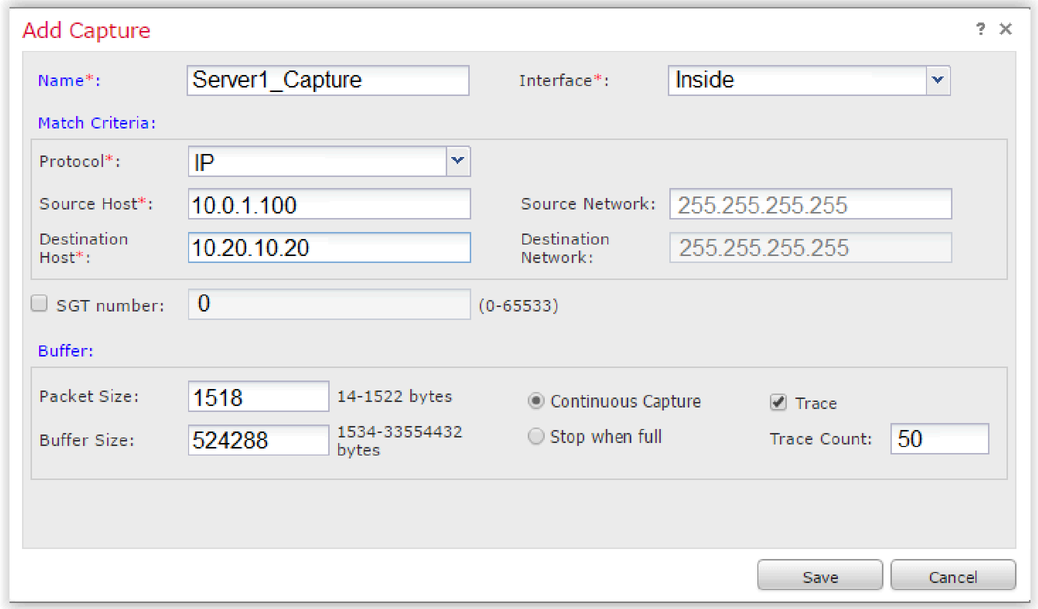
In my opinion, the question falls into ambiguity. If there is a display problem and the error is not specified, it may be due to a problem with the FMC or FTD.

It can be A or C

upvoted 1 times

An engineer is troubleshooting a device that cannot connect to a web server. The connection is initiated from the Cisco FTD inside interface and attempting to reach 10.0.1.100 over the non-standard port of 9443. The host the engineer is attempting the connection from is at the IP address of 10.20.10.20. In order to determine what is happening to the packets on the network, the engineer decides to use the FTD packet capture tool. Which capture configuration should be used to gather the information needed to troubleshoot the issue?

A.



Add Capture

Name*: Server1_Capture

Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.0.1.100

Source Network: 255.255.255.255

Destination Host*: 10.20.10.20

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

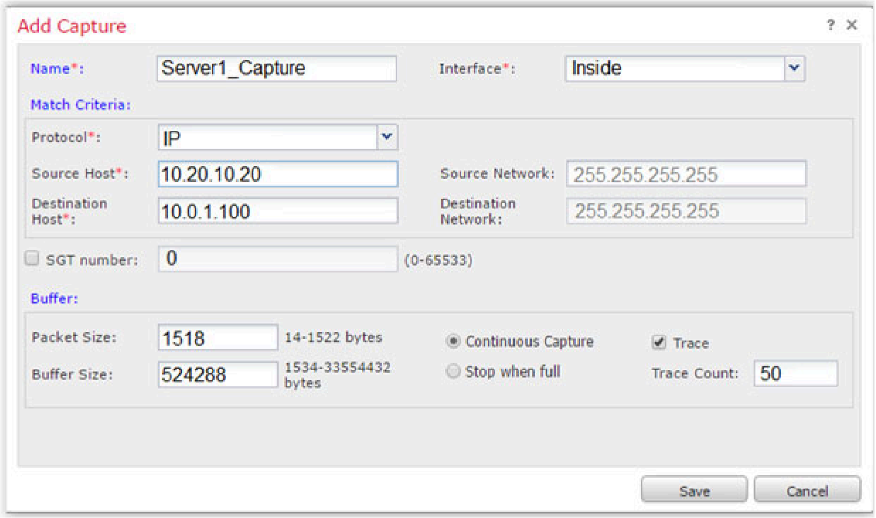
● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

B.



Add Capture

Name*: Server1_Capture

Interface*: Inside

Match Criteria:

Protocol*: IP

Source Host*: 10.20.10.20

Source Network: 255.255.255.255

Destination Host*: 10.0.1.100

Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes

Buffer Size: 524288 1534-33554432 bytes

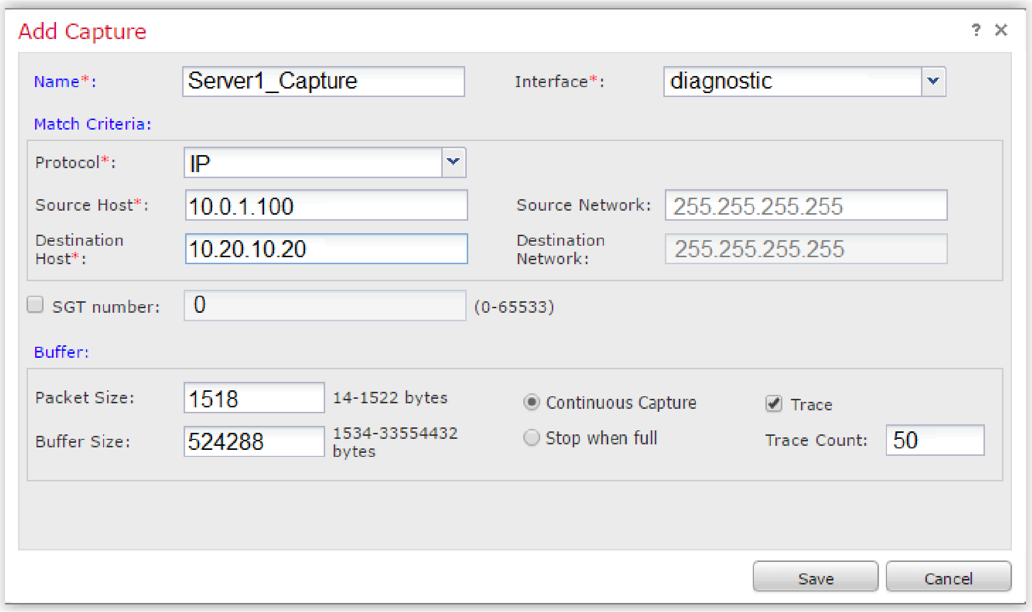
● Continuous Capture

○ Stop when full

☑ Trace

Trace Count: 50

C.



Add Capture

Name*: Server1_Capture
Interface*: diagnostic

Match Criteria:

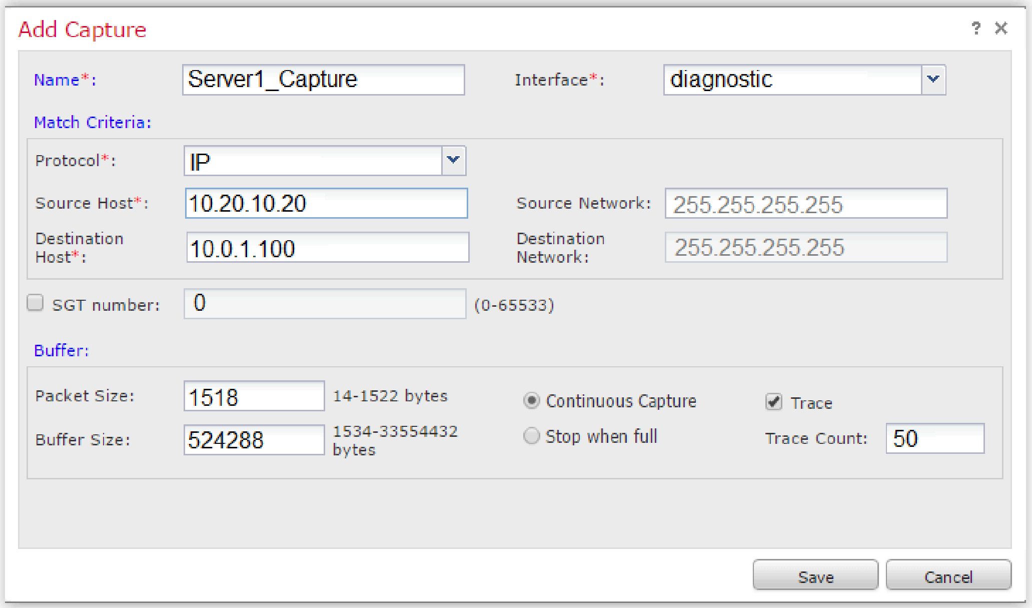
Protocol*: IP
Source Host*: 10.0.1.100
Source Network: 255.255.255.255
Destination Host*: 10.20.10.20
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

D.



Add Capture

Name*: Server1_Capture
Interface*: diagnostic

Match Criteria:

Protocol*: IP
Source Host*: 10.20.10.20
Source Network: 255.255.255.255
Destination Host*: 10.0.1.100
Destination Network: 255.255.255.255

□ SGT number: 0 (0-65533)

Buffer:

Packet Size: 1518 14-1522 bytes
Buffer Size: 524288 1534-33554432 bytes
● Continuous Capture
○ Stop when full
☑ Trace
Trace Count: 50

Suggested Answer: *B*

japm1801 11 months ago

B is correct

connection initiated from: Inside

source: 10.20.10.20

destination: 10.0.1.100

destination port: 9443 (irrelevant)

upvoted 2 times

xYanivDx 1 year, 1 month ago

the right answer is B

upvoted 1 times

Question #103 *Topic 1*

A network engineer is receiving reports of users randomly getting disconnected from their corporate applications which traverse the data center FTD appliance.
Network monitoring tools show that the FTD appliance utilization is peaking above 90% of total capacity. What must be done in order to further analyze this issue?

A. Use the Packet Export feature to save data onto external drives.

B. Use the Packet Capture feature to collect real-time network traffic.

C. Use the Packet Tracer feature for traffic policy analysis.

D. Use the Packet Analysis feature for capturing network data.

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html

Community vote distribution

C (100%)

tanri04 Highly Voted 1 year, 9 months ago

Correct answer: B. Use the Packet Capture feature to collect real-time network traffic.

In this scenario, since the FTD appliance utilization is peaking above 90% of total capacity, it is possible that the appliance is dropping packets and causing users to get disconnected from their corporate applications. To further analyze the issue, the network engineer can use the Packet Capture feature in the FTD to collect real-time network traffic and determine whether packets are being dropped, and if so, which packets are being dropped.

Option A, Packet Export feature, allows you to export captured packets to an external storage device. It does not help in analyzing the issue at hand.

Option C, Packet Tracer feature, is used to simulate and troubleshoot network traffic through the firewall. It does not help in capturing real-time network traffic for analysis.

Option D, Packet Analysis feature, provides a way to analyze packet captures taken with the Packet Capture feature. However, before analysis can be done, packets must first be captured with the Packet Capture feature.

upvoted 6 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: B

Using the Packet Tracer feature (option C) is indeed useful for traffic policy analysis. It helps you understand how traffic is being processed by the FTD appliance and can identify issues related to policy configurations.

However, to specifically analyze the issue of high utilization and user disconnections, the Packet Capture feature (option B) is more appropriate. Packet Capture allows you to collect real-time network traffic data, providing detailed insights into the actual traffic patterns and potential anomalies causing the high utilization and disconnections.

Both tools are valuable, but for real-time traffic analysis and identifying the root cause of performance issues, Packet Capture is the more suitable choice.

upvoted 2 times

tinyJoe 6 months, 2 weeks ago

Selected Answer: B

my answer is B.
Users are “randomly” disconnected, right? If the policy prevents the connection from going through, then it should not be random, but a complete disconnection.

upvoted 1 times

MB2222 8 months, 1 week ago

It should be answer "B", since we do have client connectivity (--> randomly disconnects clients). So the identify the source that is flooding the bandwidth, etc. packet captures are a good indication to do so.

upvoted 2 times

bassfunk 1 year, 4 months ago

Selected Answer: C

I would answer c. The traffic is not real but the point is to analyze the policy. When i hear connections are getting dropped, i think policy.

upvoted 1 times

gc999 1 year, 6 months ago

Selected Answer: C

They keyword here is the system is 90% overload, we should use the least CPU loading method for investigation. The first step is to use packet tracer to check if the policy is correct or not. For other option with capturing, it would not succeed and even cause impact to the system since the system is now 90% overload already.

upvoted 1 times

Bbb78 1 year, 7 months ago

This is the stupidest question ever. with CPU 90% last thing you need is a capture... show resources or cpu but capture will make the CPU 99%
NO real answer

upvoted 4 times

Baumb 1 year, 10 months ago

A. Use the Packet Export feature to save data onto external drives.
-> Exporting traffic doesnt help us understanding why the traffic lets the FTD peak

B. Use the Packet Capture feature to collect real-time network traffic.
-> Could be, we can see what traffic is traversing the firewall by inspecting the dump in packet analysis software

C. Use the Packet Tracer feature for traffic policy analysis.
-> Packet Tracer does not analyze real traffic, it generates virtual traffic, so a No.

D. Use the Packet Analysis feature for capturing network data.
-> Packet Analysis is not a feature to capture the traffic, but instead view the traffic. Since it explicitly says capture I would say this option is not valid.

So I think B is correct

upvoted 4 times

Question #104 *Topic 1*

An administrator is attempting to remotely log into a switch in the data center using SSH and is unable to connect. How does the administrator confirm that traffic is reaching the firewall?

A. by performing a packet capture on the firewall

B. by attempting to access it from a different workstation

C. by running Wireshark on the administrator's PC

D. by running a packet tracer on the firewall

Suggested Answer: *A*

Community vote distribution

A (88%) 13%

Bobster02 Highly Voted 👍 3 years, 5 months ago

A is a correct answer.

upvoted 8 times

14a1949 Most Recent 🕓 5 months, 2 weeks ago

Selected Answer: A

To confirm that traffic is reaching the firewall when an administrator is unable to connect via SSH, the best option is:

A. by performing a packet capture on the firewall

Performing a packet capture on the firewall allows the administrator to see if the SSH traffic is reaching the firewall and how it is being processed. This can help identify any issues with traffic flow or firewall rules that might be blocking the connection12.

upvoted 1 times

achille5 10 months, 1 week ago

Selected Answer: D

Basically if you want to ensure traffic pass or hit any firewall policy, you'll check packet tracer first.

upvoted 1 times

achille5 8 months, 3 weeks ago

Correct Answer is A

upvoted 1 times

gc999 1 year, 6 months ago

Selected Answer: A

My target is to make sure the traffic is "reaching" the firewall, NOT pass through the firewall. To make sure the traffic can successfully reach me, i.e. no routing issue, we should use packet capture on the outside interface

upvoted 1 times

NoUserName1234 1 year, 8 months ago

Key part here is 'packet reaching the firewall'.

This can only be done with a capture. -> A

upvoted 2 times

japm1801 2 years, 4 months ago

Selected Answer: A

A: packet capture is to see real traffic through the FW

b: could be the first option for a junior, but after that, they would go to option A

c: wireshark doesn't give any answer about the traffic reaching the firewall, only leaving the host

d: packet tracer only work in this case if you want to see if the routes and rules are properly configured

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

⊟ **aadach** 2 years, 9 months ago

Selected Answer: A

Packet Capture will show packets arriving to the interface on FW

upvoted 2 times

⊟ **cewe** 2 years, 10 months ago

Selected Answer: A

A is the right one

upvoted 1 times

⊟ **trickbot** 2 years, 10 months ago

Selected Answer: A

packet tracer is a simulation of a packet flowing through the device. Packet Capture is correct answer.

upvoted 1 times

⊟ **Sarbi** 3 years, 3 months ago

The correct answer is A.

upvoted 2 times

⊟ **kakakayayaya** 3 years, 6 months ago

Packet Tracer will not show that packet comes to FTD. We need to capture relevant traffic.

upvoted 2 times

Question #105 *Topic 1*

IT management is asking the network engineer to provide high-level summary statistics of the Cisco FTD appliance in the network. The business is approaching a peak season so the need to maintain business uptime is high. Which report type should be used to gather this information?

A. Risk Report

B. SNMP Report

C. Standard Report

D. Malware Report

Suggested Answer: *C*

Community vote distribution

C (50%) | A (40%) | 10%

cpdemo Highly Voted 3 years, 1 month ago

It's correct for choosing A. Because the report is for non security specialist and will come with recommendations that will help to anticipate on issues during a period of peaks.

The Firepower System offers two types of reports:
Risk Reports — High-level summaries of risks found on your network.
Standard Reports — Detailed, customizable reports about all aspects of your Firepower System.
Risk Reports
Risk reports are portable, high-level, easy-to-interpret summaries of risks found in your organization. You can use these reports to share information about areas of risk, and recommendations for addressing these risks, with people who do not have access to your system and who may not be network security experts. These reports are intended to facilitate discussion about areas for investment in the security of your network.

upvoted 5 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: C

The Risk Report does provide valuable insights into potential vulnerabilities and threats, which are important for maintaining security. However, for high-level summary statistics specifically related to the performance and uptime of the Cisco FTD appliance, the Standard Report is generally recommended.

upvoted 2 times

14a1949 5 months, 2 weeks ago

Selected Answer: C

Risk Reports (option A) are designed to provide high-level summaries of risks and the overall security posture of the network. They are useful for understanding potential vulnerabilities and threats.

However, for the specific need to provide high-level summary statistics of the Cisco FTD appliance's performance and status, Standard Reports (option C) are more appropriate. Standard Reports offer a comprehensive overview of various statistics and summaries related to the appliance, which is crucial for maintaining business uptime during peak seasons.

Both report types have their uses, but for the purpose of summarizing the appliance's performance and status, Standard Reports are the better choice.

upvoted 1 times

CC192024 5 months, 3 weeks ago

Selected Answer: C

The answer is C, risk Report focuses on potential vulnerabilities, compliance, and security risks rather than operational statistics.

upvoted 1 times

MB2222 8 months, 1 week ago

Yes, answer (C) makes most sense related to the question. The question tries to confuse because of saying "HIGH-LEVEL", and based on documentation definition you might go with "risk reports", but again this is more related to risks and not overall appliance health conditions.

Introduction to Reports (OFFICIAL CISCO DEFINITION):

The Firepower System offers two types of reports:

- Risk Reports — High-level summaries of risks found on your network.
- Standard Reports — Detailed, customizable reports about all aspects of your Firepower System.

upvoted 1 times

gwb 9 months, 4 weeks ago

answer C because of "high-level summary statistics of the Cisco FTD appliance" - Risk report also shows high level but more focusing security, not business uptime statistics.

upvoted 2 times

z6st2a1jv 1 year, 2 months ago

Selected Answer: C

The Standard Reports in Cisco Firepower Management Center (FMC) are detailed, customizable reports about all aspects of your system. They provide information on various topics, including:

IPS Attacks: Total number of IPS events, relevant attacks, hosts targeted, irrelevant attacks, and events requiring attention.

Network Risk: Summarizes network risks based on IPS events.

Advanced Malware Risk: Provides insights into malware-related risks.

Other Aspects: These reports cover various areas such as application usage, web traffic, and more.

upvoted 3 times

bassfunk 1 year, 4 months ago

Selected Answer: C

I would go with Standard Reports after reading the documentation.

upvoted 1 times

bobie 1 year, 6 months ago

Selected Answer: A

Because a network engineer is referenced, and according to the article below

"Risk Reports — High-level summaries of risks found on your network".

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/working_with_reports.html

upvoted 2 times

Initial14 1 year, 8 months ago

Selected Answer: C

The answer is C because it is asking for the FTD device, and this is on the standard report.

upvoted 1 times

Initial14 1 year, 8 months ago

Selected Answer: B

Standard report. So B

upvoted 1 times

tanri04 1 year, 9 months ago

Option D (Risk Report) may also provide some high-level summary statistics, but it primarily focuses on the risks and vulnerabilities present in the network. It may not provide the specific information that IT management is looking for in terms of the performance of the Cisco FTD appliance.

Option B (Standard Report) is a more appropriate choice as it provides a broad overview of the system's health and performance, including statistics such as device status, uptime, CPU usage, and memory usage. This information can help IT management make informed decisions about system maintenance and upgrades to ensure business uptime during peak season.

B. Standard Report would be the best option to gather high-level summary statistics of the Cisco FTD appliance in the network. Standard Reports provide summary-level data for different aspects of network security such as threats, applications, web usage, network discovery, and more. They offer a quick way to get an overview of the network's security posture and can be customized to focus on specific aspects of interest to IT management. SNMP Reports, on the other hand, are used to monitor network performance and availability, while Malware Reports and Risk Reports focus on specific aspects of network security.

upvoted 1 times

tanri04 1 year, 9 months ago

C). Standard Report would be the best option to gather high-level summary statistics of the Cisco FTD appliance in the network. Standard Reports provide summary-level data for different aspects of network security such as threats, applications, web usage, network discovery, and more. They offer a quick way to get an overview of the network's security posture and can be customized to focus on specific aspects of interest to IT management. SNMP Reports, on the other hand, are used to monitor network performance and availability, while Malware Reports and Risk Reports focus on specific aspects of network security.

upvoted 4 times

trickbot 2 years, 10 months ago

Selected Answer: A

I have to go with A -Risk Reports. The use of the term "High-level" in both the question and the Cisco documentation makes me think the question writer came up with the question directly from the documentation. I've been noticing questions that are based off the very first paragraph/description summary found at the beginning of sections in the documentation. This feels like one of them.

upvoted 4 times

cpdemo 3 years, 1 month ago

It's correct for choosing A. Because the report is for non security specialist and will come with recommendations that will help to issues during a period of peaks.

The Firepower System offers two types of reports:
Risk Reports — High-level summaries of risks found on your network.
Standard Reports — Detailed, customizable reports about all aspects of your Firepower System.
Risk Reports
Risk reports are portable, high-level, easy-to-interpret summaries of risks found in your organization. You can use these reports to share information about areas of risk, and recommendations for addressing these risks, with people who do not have access to your system and who may not be network security experts. These reports are intended to facilitate discussion about areas for investment in the security of your network.

upvoted 2 times

Sarbi 3 years, 2 months ago

It should be a standard report
My opinion the answer is c

upvoted 1 times

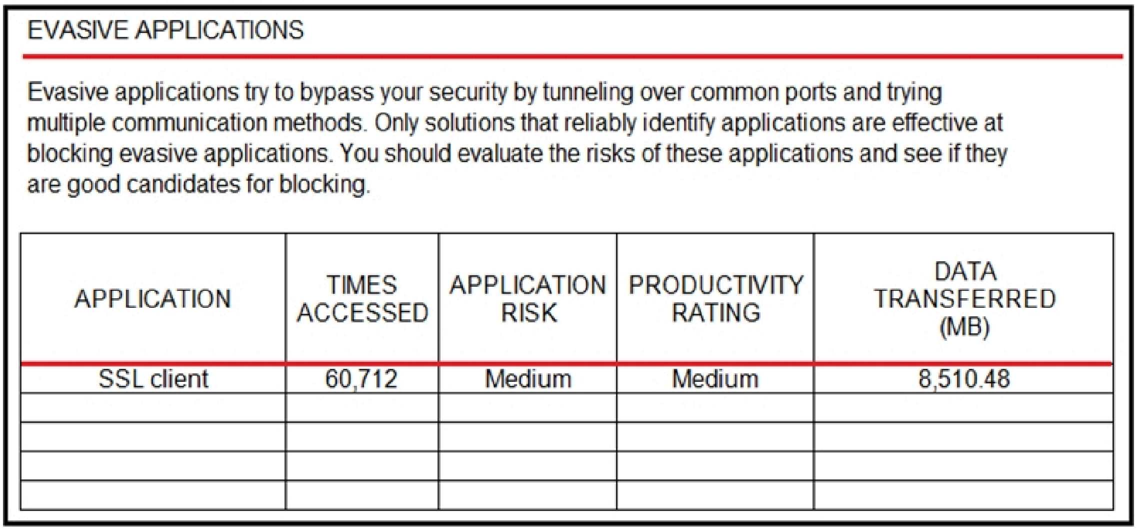
pioo1979 3 years, 3 months ago

I think the answer is "C" Standard report.
https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/working_with_reports.html

upvoted 1 times

Question #106

Topic 1



EVASIVE APPLICATIONS

Evasive applications try to bypass your security by tunneling over common ports and trying multiple communication methods. Only solutions that reliably identify applications are effective at blocking evasive applications. You should evaluate the risks of these applications and see if they are good candidates for blocking.

APPLICATION	TIMES ACCESSED	APPLICATION RISK	PRODUCTIVITY RATING	DATA TRANSFERRED (MB)
SSL client	60,712	Medium	Medium	8,510.48

Refer to the exhibit. An administrator is looking at some of the reporting capabilities for Cisco Firepower and noticed this section of the Network Risk Report showing a lot of SSL activity that could be used for evasion. Which action will mitigate this risk?

A. Use SSL decryption to analyze the packets.

B. Use Cisco Tetration to track SSL connections to servers.

C. Use encrypted traffic analytics to detect attacks.

D. Use Cisco AMP for Endpoints to block all SSL connection.

Correct Answer: *A*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/fdm/fptd-fdm-config-guide-623/fptd-fdm-ssl-decryption.html

Currently there are no comments in this discussion, be the first to comment!

Question #107 *Topic 1*

An administrator is setting up Cisco FirePower to send data to the Cisco Stealthwatch appliances. The NetFlow_Set_Parameters objet is already created, but
NetFlow is not being sent to the flow collector. What must be done to prevent this from occurring?

A. Create a service identifier to enable the NetFlow service.

B. Add the NetFlow_Send_Destination object to the configuration.

C. Create a Security Intelligence object to send the data to Cisco Stealthwatch.

D. Add the NetFlow_Add_Destination object to the configuration.

Suggested Answer: *D*

Community vote distribution

D (80%) B (20%)

⊟ **14a1949** 5 months, 2 weeks ago

Selected Answer: D

Based on the information and the documentation, the correct answer is to add the NetFlow_Add_Destination object to the configuration (Option D). This step ensures that the NetFlow data is directed to the appropriate flow collector.

upvoted 1 times

⊟ **tinyJoe** 6 months, 2 weeks ago

Selected Answer: D

I guess correct answer is D.
Unfortunately, these objects have been removed in FTD ver 7.4...
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/760/management-center-device-config-76/flex-config.html?bookSearch=true

upvoted 1 times

⊟ **c946f3e** 9 months, 2 weeks ago

Selected Answer: D

NetFlow_Add_Destination object.

upvoted 1 times

⊟ **SegaMasterSystemAdmin** 1 year ago

Selected Answer: D

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html

upvoted 1 times

⊟ **Joe_Blue** 1 year, 3 months ago

Selected Answer: D

Sorry, correct answer is D. Looking at the FTD FlexConfig Object I see no NetFlow_Send_Destination object.
Only option is NetFlow_Add_Destination object.

upvoted 2 times

⊟ **Joe_Blue** 1 year, 3 months ago

Selected Answer: B

To enable the Cisco FirePower appliance to send NetFlow data to the Cisco Stealthwatch appliances, the NetFlow_Send_Destination object needs to be added to the configuration.

The NetFlow_Send_Destination object specifies the IP address of the Cisco Stealthwatch flow collector that will receive the NetFlow data from the Cisco FirePower appliance. Without this object, the Cisco FirePower appliance does not know where to send the NetFlow data. Adding the NetFlow_Add_Destination object is not a valid option, as there is no such object in the Cisco FirePower configuration. The correct object to add is NetFlow_Send_Destination.

upvoted 1 times

⊟ **Baumb** 1 year, 4 months ago

Netflow_Set_Parameters only sets timers etc.

Unfortunately I dont have a good explanation to exclude A and C but B does not exist and you need to configure D, so I would go with D.

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html
upvoted 1 times

Question #108 Topic 1

With a recent summer time change, system logs are showing activity that occurred to be an hour behind real time. Which action should be taken to resolve this issue?

A. Manually adjust the time to the correct hour on all managed devices.

B. Configure the system clock settings to use NTP with Daylight Savings checked.

C. Configure the system clock settings to use NTP.

D. Manually adjust the time to the correct hour on the Cisco FMC.

Suggested Answer: *C*

Community vote distribution

C (100%)

14a1949 5 months, 2 weeks ago

Selected Answer: C

If there is no option to enable Daylight Savings Time in the FMC GUI, then configuring the system clock settings to use NTP (Option C) is indeed the correct action. This will ensure that the system time is synchronized with a reliable time source, keeping the logs accurate.

upvoted 1 times

bassfunk 1 year, 4 months ago

Selected Answer: C

Only with a timezone object can you select DST.

upvoted 2 times

Gabranch 1 year, 7 months ago

Selected Answer: C

C - FMC is UTC, per user one can change the localization for time zone.

upvoted 1 times

xziomal9 2 years, 5 months ago

Selected Answer: C

Correct answer is: C

upvoted 1 times

Reece_S 2 years, 7 months ago

Tricky question. The fmc uses ntp with utc time however in platform settings there is a timezone field that uses an ntp object that does have the dst check box, if you created an ntp object for your local time zone.

upvoted 2 times

trickbot 2 years, 10 months ago

Selected Answer: C

C is the answer because there is no option to enable daylight savings time in the FMC GUI>settings>time* or device>platform>time*

upvoted 2 times

NoOn3x 2 years, 11 months ago

I found this. My opinion, the answer would be C.

#

Note that the time displayed on most pages on the web interface is the local time, which is determined by using the time zone you specify in your local configuration. Further, the Firepower Management Center automatically adjusts its local time display for daylight saving time (DST), where appropriate. However, recurring tasks that span the transition dates from DST to standard time and back do not adjust for the transition. That is, if you create a task scheduled for 2:00 AM during standard time, it will run at 3:00 AM during DST. Similarly, if you create a task scheduled for 2:00 AM during DST, it will run at 1:00 AM during standard time.

#

Documentation: Configuring a Recurring Task

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Scheduling_Tasks.html

upvoted 3 times

⊟ **moh_d_muh** 3 years, 1 month ago

Which answer right B or C

upvoted 1 times

⊟ **elliot67** 3 years, 2 months ago

The Daylight Saving settings are set by default. You have the option to edit them, but they are already configured. So, C is the answer

upvoted 2 times

⊟ **Sarbi** 3 years, 2 months ago

I will go for C.As it is function of NTP server to adjust daylight saving

upvoted 4 times

⊟ **gwb** 9 months, 4 weeks ago

answer C agree. daylight saving time check up is usually not synced with any NTP server.

upvoted 1 times

⊟ **Doris8000** 3 years, 3 months ago

Daylight Saving is not part of ntp config list:

Set the Time Zone and Daylight Saving Dates

Set the Date and Time Using an NTP Server

Set the Date and Time Manually

Configure Precision Time Protocol (ISA 3000)

https://www.cisco.com/c/en/us/td/docs/security/asa/asa913/configuration/general/asa-913-general-config/basic-hostname-pw.html#ID-2130-000001c3

upvoted 3 times

⊟ **netwguy** 3 years, 4 months ago

This is a terrible question. I guess the correct answer is C, but we dont know what time-zone the mentioned NTP server is in, so we have no way of knowing if using NTP will display the correct time. By default UTC is being used for NTP, and UTC has no summer time, meaning a NTP server with default setup, will not solve any "summertime problem". However, if the NTP server used is correcting the received UTC time received from stratum servers, to the local timezone, then C is correct. Its a lot of presumptions though, which is why this question is terrible :/

upvoted 3 times

⊟ **bassfunk** 1 year, 4 months ago

"system logs are showing activity that occurred to be an hour behind real time." This implies that local time is being used.

upvoted 1 times

⊟ **cryptofetti** 3 years, 4 months ago

After further analysis it really doesnt apply and I am going back with my original answer, C

upvoted 1 times

⊟ **cryptofetti** 3 years, 4 months ago

This is correct. Found this under Objects -> Time Zone w/ the Daylight Savings Time and Allow overrides - checkboxes for the Time Zone object

upvoted 1 times

Question #109 *Topic 1*

A network administrator notices that SI events are not being updated. The Cisco FTD device is unable to load all of the SI event entries and traffic is not being blocked as expected. What must be done to correct this issue?

A. Restart the affected devices in order to reset the configurations.

B. Redeploy configurations to affected devices so that additional memory is allocated to the SI module.

C. Replace the affected devices with devices that provide more memory.

D. Manually update the SI event entries to that the appropriate traffic is blocked.

Suggested Answer: *B*

Community vote distribution

B (100%)

ERGEGA Highly Voted 2 years, 3 months ago

Answer is B.
Memory limitations. Cisco Intelligence Feeds are based on the latest threat intelligence from Cisco Talos Intelligence Group (Talos). These feeds tend to get larger as time passes. When a Firepower device receives a feed update, it loads as many entries as it can into the memory it has allocated for Security Intelligence. When a device cannot load all the entries, it may not block traffic as expected. Some connections that should be blocked by a Block list instead continue to be evaluated by access control rules.

If you think this is happening, redeploy configurations to the affected devices.

upvoted 8 times

Bobster02 Highly Voted 3 years ago

Troubleshooting Memory Use:

Symptoms: Connections that should be blocked by a Security Intelligence Block list are instead evaluated by access control rules. The Security Intelligence health module alerts that it is out of memory.

Cause: Memory limitations. Cisco Intelligence Feeds are based on the latest threat intelligence from Cisco Talos Intelligence Group (Talos). These feeds tend to get larger as time passes.

Workaround: If you think this is happening, redeploy configurations to the affected devices. This can allocate more memory to Security Intelligence.

upvoted 6 times

bassfunk Most Recent 10 months, 3 weeks ago

Selected Answer: B

Going with B.

upvoted 1 times

partyzan06 1 year ago

Selected Answer: B

B. Redeploy configurations to affected devices so that additional memory is allocated to the SI module.

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: B

To correct the issue of SI events not being updated and the Cisco FTD device being unable to load all of the SI event entries, the network administrator should redeploy configurations to affected devices so that additional memory is allocated to the SI module.

upvoted 1 times

xziomal9 2 years ago

Selected Answer: B

Correct answer is: B

upvoted 1 times

aadach 2 years, 3 months ago

Selected Answer: B

Correct B

upvoted 1 times

⊟ **Bobster02** 3 years ago

B is correct, confirmed.

upvoted 2 times

⊟ **kakakayayaya** 3 years ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/security_intelligence_blacklisting.html

Workaround: If you think this is happening, redeploy configurations to the affected devices.

B - right answer

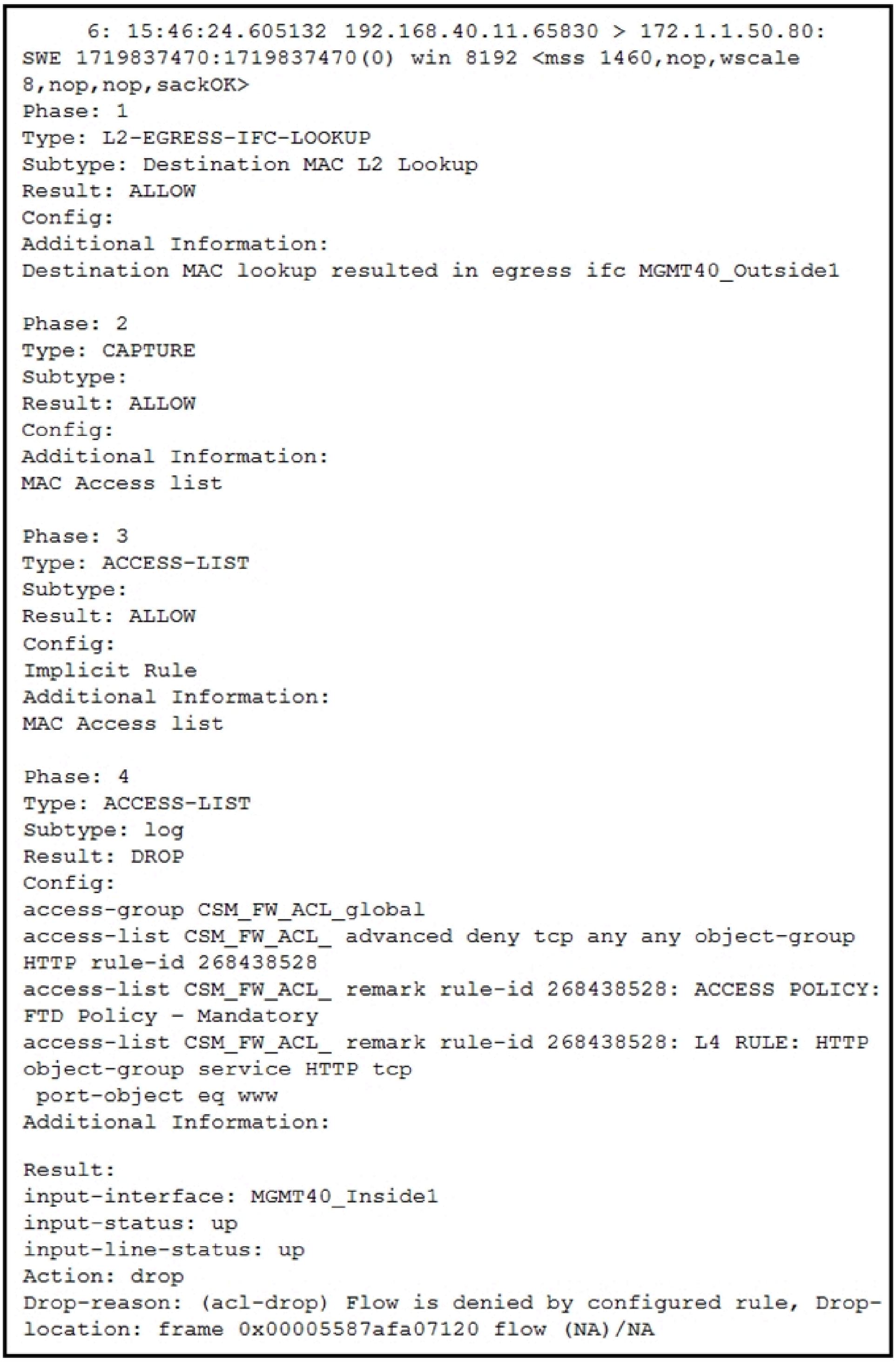
upvoted 3 times

⊟ **kakakayayaya** 3 years ago

Does someone give explanation? How does Intelligence EVENTS affect Intelligence process. It is just logging.

upvoted 1 times

Question #110 *Topic 1*



```
     6: 15:46:24.605132 192.168.40.11.65830 > 172.1.1.50.80:
SWE 1719837470:1719837470(0) win 8192 <mss 1460,nop,wscale
8,nop,nop,sackOK>
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC lookup resulted in egress ifc MGMT40_Outside1

Phase: 2
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_ advanced deny tcp any any object-group
HTTP rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY:
FTD Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: HTTP
object-group service HTTP tcp
 port-object eq www
Additional Information:

Result:
input-interface: MGMT40_Inside1
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-
location: frame 0x00005587afa07120 flow (NA)/NA
```

Refer to the exhibit. What must be done to fix access to this website while preventing the same communication to all other websites?

A. Create an intrusion policy rule to have Snort allow port 80 to only 172.1.1.50.

B. Create an intrusion policy rule to have Snort allow port 443 to only 172.1.1.50.

C. Create an access control policy rule to allow port 443 to only 172.1.1.50.

D. Create an access control policy rule to allow port 80 to only 172.1.1.50.

Suggested Answer: *D*

⊟ **gwb** 9 months, 4 weeks ago

http 80 is key

upvoted 2 times

Question #111 *Topic 1*

A connectivity issue is occurring between a client and a server which are communicating through a Cisco Firepower device. While troubleshooting, a network administrator sees that traffic is reaching the server, but the client is not getting a response. Which step must be taken to resolve this issue without initiating traffic from the client?

A. Use packet-tracer to ensure that traffic is not being blocked by an access list

B. Use packet capture to ensure that traffic is not being blocked by an access list

C. Use packet capture to validate that the packet passes through the firewall and is NATed to the corrected IP address

D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the corrected IP address

Suggested Answer: *D*

Community vote distribution

D (70%) C (30%)

d0980cc 2 months ago

Selected Answer: A

Other have stated, why are we assuming this is a NAT issue. Traffic could be dropped by a rule or a misconfiguration. Initial I thought A, but if it's an external client, sure D.
So I'll go against the grain and say A.

upvoted 1 times

14a1949 5 months, 2 weeks ago

Selected Answer: D

so which one is the correct answer
The correct answer to resolve the connectivity issue between a client and a server without initiating traffic from the client is:

D. Use packet-tracer to validate that the packet passes through the firewall and is NATed to the correct IP address.

The packet-tracer tool simulates the path of a packet through the firewall, providing insights into how the traffic is processed, including NAT and firewall rules. This helps identify any configuration issues that might be preventing the client's response from reaching the server.

Packet capture (option C) is also useful for verifying actual traffic, but packet-tracer is more comprehensive for simulating and diagnosing potential problems in the configuration without needing live traffic.

upvoted 1 times

Vijay1234 8 months, 2 weeks ago

I think A is correct answer. packet tracer not able to validate traffic pass trough..i can validate policy configure correctly or not.

upvoted 1 times

MB2222 8 months, 1 week ago

Not excactly, since it says in the question that the client is reaching the server which implies that the ACP is working correctly, and not blocking the request. Since the return traffic somehow is affected, it is most likely NAT that causes the issue. So, packet-tracer with an eye on the NAT section within packet-tracer would be a good fit. My answer is (D).

upvoted 1 times

spambox730 1 year, 5 months ago

Selected Answer: C

A and B is a straight NO.
D gives you all the steps the firewall would do with the packet in theory.
C taken for ingress and egress traffic show wat happens in real life.
We know the packet reaches the server so packet tracer should not provide much new information but packet capture can tell if the response from the server reaches the firewall or not, it can also tell if the packet was sent out on the right interface with the expected IP addresses etc.

upvoted 3 times

spambox730 1 year, 5 months ago

Nope, disregard it. My brain did not process the "without initiating traffic from the client" part.
Correct is D.

upvoted 5 times

Markl3ver 2 years, 8 months ago

If it is statefull firewall, then ACL can not block the response from server this exesting connection, only wrong NAT rule for this server could be the issue. My opinion the answer is D.

upvoted 3 times

wernervv32 2 years, 9 months ago

Selected Answer: D

if the traffic was being blocked by an access list, then the traffic would not be reaching the server, so it discards A answer.

correct Answer is D

upvoted 4 times

cewe 2 years, 10 months ago

Selected Answer: D

i would go with D because packet-tracer checkes the ACP AND NAT, Routing and all the stuff.

So D will include A

upvoted 2 times

trickbot 2 years, 10 months ago

Selected Answer: D

D-Packet-tracer/NAT "without generating traffic from the client", makes this a packet tracer answer. The only problem is that packet tracer doesnt track the return packet from the server, and therefor wont tell you if it is being dropped by an ACL in the return path. What I have seen in my real-life packet tracer use, is packet tracer dropping the initial packet because the return packet would hit an unexpected NAT rule, causing asymmetrical NAT and the connection failing anyways. As such, my answer is

upvoted 1 times

trawa05 3 years, 1 month ago

FTD is a statefull firewall, so A is out of the table

D is correct

upvoted 4 times

pioo1979 3 years, 3 months ago

A is the correct answer. If it wouldn't NAT-et (if there is a NAT) the traffic wouldn't reach the server, But the ACL still can block the traffic FROM the Server to the Client.

upvoted 2 times

BorZol 2 years, 3 months ago

because ftd is stateful ur not right. Because of established connection trafic from server back to the client can not reach ACP in that direction.

upvoted 1 times

SanchezEldorado 2 years, 8 months ago

If you are natting the source address, traffic will still reach the server, but then it will be sent back to the incorrect IP address for the client. Answer is D.

upvoted 1 times

Bobster02 3 years, 5 months ago

There is nothing says that NAT was configured in this scenario. A is a valid answer.

upvoted 4 times

kakakayayaya 3 years, 6 months ago

It seems that A and D are valid answers depend on architecture.

upvoted 2 times

essie007 3 years, 5 months ago

In the case it would be blocked (A), the traffic would not reach the server.

upvoted 2 times

gwb 9 months ago

well, a big assumption is stateful - returnning traffic is allowed automatically in that case. yeah I will go with D, but A is kind of right answer depending on how to interpret

upvoted 2 times

Question #112 *Topic 1*

A VPN user is unable to connect to web resources behind the Cisco FTD device terminating the connection. While troubleshooting, the network administrator determines that the DNS response are not getting through the Cisco FTD. What must be done to address this issue while still utilizing Snort IPS rules?

A. Uncheck the ג€Drop when Inlineג€ box in the intrusion policy to allow the traffic

B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users

C. Disable the intrusion rule thresholds to optimize the Snort processing

D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

Suggested Answer: *B*

Community vote distribution

B (100%)

Initial14 8 months, 2 weeks ago

Selected Answer: B

The only answer here that is the closest to correct is B. All other can't be right. A--> You transform IPS to IDS, B ---> There might be some problems in request/reply in DNS communication and IPS will block it. C---> This does not make sense, if you disable Threshold, the rule will be triggered X times more. D ----> No sense in that

upvoted 4 times

Joe_Blue 9 months, 3 weeks ago

Selected Answer: B

To address the issue of DNS responses not getting through the Cisco FTD while still utilizing Snort IPS rules, the network administrator should modify the Snort rules to allow legitimate DNS traffic to the VPN users.

Snort is an intrusion detection and prevention system that can be used to detect and prevent malicious traffic. However, in some cases, Snort rules may block legitimate traffic, such as DNS responses, causing connectivity issues for VPN users.

upvoted 4 times

tanri04 10 months, 1 week ago

correct answer???which?

upvoted 1 times

Baumb 10 months, 3 weeks ago

A. Uncheck the "Drop when Inline" box in the intrusion policy to allow the traffic

-> Seems to be the best option, since it only will generate an event afterwards but lets the traffic pass

B. Modify the Snort rules to allow legitimate DNS traffic to the VPN users

-> Traffic is already allowed, as the response is not getting to the VPN user

C. Disable the intrusion rule thresholds to optimize the Snort processing

-> This doesnt make any sense for the shown problem

D. Decrypt the packet after the VPN flow so the DNS queries are not inspected

-> The packet is already decrypted, since the FTD is the vpn endpoint

I would go with A

upvoted 1 times

netwguy 2 years, 4 months ago

All answers are a bit strange to me. We know that the DNS query is going through the firewall, since the problem is the DNS response not going through the firewall. B makes the most sense, but it would then be the DNS response that triggers the snort triggered drop(?). Thats a bit strange, but plausible.

upvoted 3 times

cryptofetti 2 years, 4 months ago

Sorry I mean why is the answer not D?

upvoted 1 times

⊟ **cryptofetti** 2 years, 4 months ago

Why would'nt it be B?

upvoted 1 times

Question #113 *Topic 1*

An engineer is restoring a Cisco FTD configuration from a remote backup using the command restore remote-manager-backup location 1.1.1.1 admin /
Volume/home/admin BACKUP_Cisc394602314.zip on a Cisco FMC. After connecting to the repository, an error occurred that prevents the FTD device from accepting the backup file. What is the problem?

A. The backup file is not in .cfg format

B. The backup file is too large for the Cisco FTD device

C. The backup file extension was changed from .tar to .zip

D. The backup file was not enabled prior to being applied

Correct Answer: *C*
Reference:
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3455.pdf

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 1*

An organization has a Cisco IPS running in inline mode and is inspecting traffic for malicious activity. When traffic is received by the Cisco IPS, if it is not dropped, how does the traffic get to its destination?

A. It is retransmitted from the Cisco IPS inline set

B. The packets are duplicated and a copy is sent to the destination

C. It is transmitted out of the Cisco IPS outside interface

D. It is routed back to the Cisco ASA interfaces for transmission

Suggested Answer: *A*

Community vote distribution

A (100%)

eazy99 Highly Voted 👍 1 year, 9 months ago

Selected Answer: A

The Answer is absolutely A.
"Inline interfaces receive all traffic unconditionally, but all traffic
received on these interfaces is retransmitted out of an inline set unless explicitly dropped."
You can verify my answer here: https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v60_chapter_01011010.pdf
The third page, under (Inline IPS Deployments)

upvoted 7 times

d0980cc Most Recent 3 months, 3 weeks ago

Selected Answer: C

If the Cisco IPS in inline mode does not drop the traffic after inspection, it forwards the traffic directly to its destination via its outbound interface, but after reading the article below I will select A.

upvoted 1 times

THEODORABLE 7 months, 2 weeks ago

I believe D is correct, its just a poor choice of words....go figure. No matter if it is the Cisco IPS or and FTD the traffic is handed back to the LINA engine to be put out on the wire based on the SNORT verdict. Although the CISCO IPS no longer exist (TG!)

upvoted 3 times

Silexis 4 months, 4 weeks ago

I was on the same line of thoughts with but they used the word "routed", which is not the case. Unfortunately these kind of questions are no longer testing candidates knowledge but are testing the focus capacity on phrasing, which in my opinion it is bad!

upvoted 1 times

Joe_Blue 9 months, 3 weeks ago

Selected Answer: A

If traffic is not dropped by the Cisco IPS running in inline mode, the packets are retransmitted from the IPS inline set to the original destination. So, the correct option is A.

upvoted 1 times

xziomal9 1 year, 6 months ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

Reece_S 1 year, 8 months ago

I believe D is correct. The fact the question says Cisco IPS and not Cisco Firepower, it is probably an ASA. I don't think it has inline set interfaces as an option, only inline and tap mode. Traffic that's not dropped goes Lina -> Snort -> and back to Lina for transmission to the destination even in FTD. And the question is asking how it reaches the destination as well. If the question said Cisco FTD, it would definitely be onboard with A as the answer.

upvoted 4 times

Gabranch 7 months, 1 week ago

Perhaps - But the test outline has all Firepower topics, not ASA+FP

upvoted 2 times

⊟ **ERGEGA** 1 year, 10 months ago

In an FTD in inline mode, if the traffic is not droped is retransmited out from the inlineset pair interfaces.

upvoted 1 times

⊟ **NoOn3x** 1 year, 11 months ago

And why not C?

It mentions that the IPS transmits it through the outside interface, which would be the interface through which the traffic belonging to the Inline-set will go out.

upvoted 1 times

⊟ **trickbot** 1 year, 10 months ago

C is not the best answer. You have to make a couple unconventional assumptions about the outside interface for C to correct. Such as, "Outside" interface kind of implies the connection to your ISP, which is a routed interface. (see others below on that.)

upvoted 1 times

⊟ **ion123** 1 year, 11 months ago

Selected Answer: A

The IPS-only (inline mode) does not have routing possibilities.

So, A is correct

upvoted 2 times

⊟ **onefa** 2 years, 1 month ago

Must be A

IPS-only interfaces can be deployed as the following types:

Inline Set, with optional Tap mode—An inline set acts like a bump on the wire, and binds two interfaces together to slot into an existing network. This function allows the FTD to be installed in any network environment without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, but all traffic received on these interfaces is retransmitted out of an inline set unless explicitly dropped.

upvoted 3 times

⊟ **elliot67** 2 years, 2 months ago

The IPS-only (inline mode) does not have routing possibilities.

So, A is correct

upvoted 3 times

Question #115 *Topic 1*

An engineer is investigating connectivity problems on Cisco Firepower that is using service group tags. Specific devices are not being tagged correctly, which is preventing clients from using the proper policies when going through the firewall. How is this issue resolved?

A. Use traceroute with advanced options

B. Use Wireshark with an IP subnet filter

C. Use a packet capture with match criteria

D. Use a packet sniffer with correct filtering

Suggested Answer: *C*

Community vote distribution

C (100%)

d0980cc 2 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos231/web-guide/b_GUI_FXOS_ConfigGuide_231/troubleshooting.html#:~:text=34525%2C%20ARP%20%3D%202054%2C-,and%20SGT%20%3D%2035081),-.

upvoted 1 times

houhou12322 9 months, 2 weeks ago

I think it has something to do with AMP for endpoint and cisco secure client because in the question they say "preventing clients from using the proper policies"

upvoted 1 times

THEODORABLE 2 years, 1 month ago

My choice is C, this is a Cisco Exam, why would we choose WireShark instead of a native Cisco process on a cisco device for the same purpose? Plus with Wireshark you would need to span a port for data flow.

upvoted 3 times

Joe_Blue 2 years, 3 months ago

Selected Answer: C

Yes, using a packet capture with match criteria would be a good way to troubleshoot this issue. The packet capture can be set up to capture traffic only from the specific devices that are not being tagged correctly. The match criteria can be set to filter for traffic that is associated with the service group in question, allowing the engineer to see if the traffic is being tagged correctly or not. Based on the results of the packet capture, the engineer can then take appropriate actions to resolve the issue.

upvoted 2 times

Baumb 2 years, 4 months ago

Im voting for C, because a packet capture on the FW always makes more sense than doing something on the client

upvoted 3 times

dique 2 years, 10 months ago

Selected Answer: C

Correct answer is: C

upvoted 2 times

xziomal9 2 years, 11 months ago

Selected Answer: C

Correct answer is: C

upvoted 2 times

aadach 3 years, 3 months ago

Answer C

upvoted 2 times

trickbot 3 years, 4 months ago

C, Using the built in Packet Capture feature is the best answer.

B is NOT the best answer because:

This is not a test on Wireshark

You wouldnt necessarily use a subnet filter

If B were right, than D would be even more right.

We can do packet captures right in FMC, including filtering for specific SGTs.

upvoted 2 times

netwguy 3 years, 10 months ago

C also makes sense. Capture could just be exported and imported in wireshark. Also, you would be able to use match argument to specify devices instead of subnet, and also SGTs if you want to. I will go for C if this comes up during test.

upvoted 3 times

cryptofetti 3 years, 10 months ago

B, Wireshark makes the most sense

upvoted 1 times

kakakayayaya 4 years ago

Why don't we use packet capture? Arguable answer...

upvoted 2 times

Question #116 *Topic 1*

An organization must be able to ingest NetFlow traffic from their Cisco FTD device to Cisco Stealthwatch for behavioral analysis. What must be configured on the
Cisco FTD to meet this requirement?

A. flexconfig object for NetFlow

B. interface object to export NetFlow

C. security intelligence object for NetFlow

D. variable set object for NetFlow

Suggested Answer: *A*

Doris8000 Highly Voted 👍 3 years, 3 months ago

correct:

Step 4. Configure the Netflow Destination
In order to configure the Netflow Destination, navigate to Objects > FlexConfig > FlexConfig Objects

https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/netflow/216126-configure-netflow-secure-event-logging-o.html#anc14

upvoted 7 times

gwb Most Recent ⏱ 9 months, 4 weeks ago

flexconfig for NetFlow

upvoted 2 times

tanri04 1 year, 9 months ago

To export NetFlow traffic from a Cisco FTD device to Cisco Stealthwatch, the correct configuration is to use a FlexConfig object to enable NetFlow export on the device. Therefore, the answer is A.

upvoted 3 times

Question #117 *Topic 1*

An engineer must build redundancy into the network and traffic must continuously flow if a redundant switch in front of the firewall goes down.
What must be configured to accomplish this task?

A. redundant interfaces on the firewall cluster mode and switches

B. redundant interfaces on the firewall noncluster mode and switches

C. vPC on the switches to the interface mode on the firewall cluster

D. vPC on the switches to the span EtherChannel on the firewall cluster

Suggested Answer: *A*

Community vote distribution

D (50%) A (50%)

Doris8000 Highly Voted 3 years, 9 months ago

The answer is correct:
Virtual Port Channels (vPC) are common EtherChannel
deployments, especially in the data center, and allow
multiple devices to share multiple interfaces

EtherChannel Interface requires stack, VSS or vPC when connected to multiple switches

upvoted 8 times

14a1949 Most Recent 5 months, 2 weeks ago

Selected Answer: D

Option A, which involves creating redundant interfaces on the firewall in cluster mode and on the switches, does provide redundancy. However, it is not as specific and comprehensive as option D for ensuring continuous traffic flow in the context of the problem described.

Using Virtual Port Channel (vPC) on the switches to the span EtherChannel on the firewall cluster (option D) is specifically designed to provide both redundancy and load balancing. This method ensures that links from both switches are seen as a single port channel by the firewall cluster, allowing for seamless failover and continuous traffic flow even if one switch fails.

So while option A addresses redundancy, it does not explicitly mention the configuration techniques (vPC and Spanned EtherChannel) that are best suited to achieve the desired outcome of uninterrupted traffic flow

upvoted 1 times

Doris8000 11 months ago

Answer is D
https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/clustering/asa-cluster-solution.html#:~:text=Virtual%20Port%20Channel%20(vPC

upvoted 2 times

MB2222 1 year, 2 months ago

Correct answer is (D), since EtherChannel with vPC utilize all for this connection dedicated firewall interfaces simultaniously. Redundant interface configurations are getting out-dated in present times due to the disadvantage of only utilizing one instead of 2 interfaces that belong to the SLA monitor setup.

upvoted 1 times

c946f3e 1 year, 9 months ago

Selected Answer: D

When you place the cluster in your network, the upstream and downstream routers need to be able to load-balance the data coming to and from the cluster using Spanned EtherChannels. Interfaces on multiple members of the cluster are grouped into a single EtherChannel; the EtherChannel performs load balancing between units.

upvoted 2 times

dique 2 years, 10 months ago

Selected Answer: D

Answer: D

upvoted 1 times

⊟ **Grandslam** 3 years ago

Selected Answer: D

D is correct.

upvoted 1 times

⊟ **trickbot** 3 years, 4 months ago

Selected Answer: A

Answer A seems perfectly fine to me. I dont trust answer D because it's unintelligible. Answer A seems to say the same thing as answer D anyhow.

upvoted 3 times

⊟ **gwb** 1 year, 3 months ago

I am with you. Answer A. first vPC - this can be done by VSS, Virtual StackWise, etc.... any clustering techniques can be used. For me, A is more general cover

upvoted 2 times

Question #118 *Topic 1*

A network administrator notices that inspection has been interrupted on all non-managed interfaces of a device. What is the cause of this?

A. The value of the highest MTU assigned to any non-management interface was changed

B. The value of the highest MSS assigned to any non-management interface was changed

C. A passive interface was associated with a security zone

D. Multiple inline interface pairs were added to the same inline interface

Suggested Answer: *A*

Community vote distribution

A (100%)

c946f3e 9 months, 2 weeks ago

Selected Answer: A

Configurations that Restart the Snort Process When Deployed or Activated

- MTU: Change the highest MTU value among all non-management interfaces on a device.

upvoted 3 times

Doris8000 2 years, 9 months ago

The answer is correct

Caution :

Changing the highest MTU value among all non-management interfaces on the device restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Inspection is interrupted on all non-management interfaces, not just the interface you modified. Whether this interruption drops traffic or passes it without further inspection depends on the model of the managed device and the interface type. See Snort® Restart Traffic Behavior for more information.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01101010.html

upvoted 4 times

Question #119 *Topic 1*

A network administrator needs to create a policy on Cisco Firepower to fast-path traffic to avoid Layer 7 inspection. The rate at which traffic is inspected must be optimized. What must be done to achieve this goal?

A. Enable the FXOS for multi-instance

B. Configure a prefilter policy

C. Configure modular policy framework

D. Disable TCP inspection

Suggested Answer: *B*

Doris8000 Highly Voted 👍 3 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/prefiltering_and_prefilter_policies.html

upvoted 5 times

gwb Most Recent 🕘 9 months, 4 weeks ago

B. prefilter. Key words are "The rate at which traffic is inspected must be optimized". optimization can be done by prefilter because it reduces the process of inspection

upvoted 3 times

tanri04 1 year, 9 months ago

B. Configure a prefilter policy.

A prefilter policy allows you to bypass certain rules for certain types of traffic, thus fast-pathing the traffic to avoid Layer 7 inspection. By configuring a prefilter policy, you can optimize the rate at which traffic is inspected by selectively bypassing rules that are not needed for certain types of traffic.

upvoted 3 times

Question #120 *Topic 1*

A network engineer is tasked with minimizing traffic interruption during peak traffic times. When the SNORT inspection engine is overwhelmed, what must be configured to alleviate this issue?

A. Enable IPS inline link state propagation

B. Enable Pre-filter policies before the SNORT engine failure

C. Set a Trust ALL access control policy

D. Enable Automatic Application Bypass

Suggested Answer: *D*

Community vote distribution

D (100%)

pr0fectus 8 months, 2 weeks ago

Selected Answer: D

Enabling AAB - if the Snort processes are causing a performance degradation, certain traffic can bypass these Snort processes to alleviate the bottleneck when a performance threshold is crossed.

upvoted 3 times

tanri04 1 year, 3 months ago

When the SNORT inspection engine is overwhelmed, to minimize traffic interruption during peak traffic times, a network engineer can configure the IPS (Intrusion Prevention System) to alleviate this issue by enabling Automatic Application Bypass. Therefore, the correct answer is D, Enable Automatic Application Bypass.

When the SNORT inspection engine is overwhelmed, enabling Automatic Application Bypass allows the IPS to bypass specific applications or protocols that are causing the bottleneck. This ensures that critical traffic is not dropped, and network performance is not degraded during peak traffic times.

Enabling IPS inline link state propagation (Option A) is a mechanism that ensures link state information is propagated to the inline security device, such as IPS. It helps ensure that the IPS does not forward traffic to an interface that is down. However, it does not directly address the issue of SNORT engine overload.

upvoted 4 times

Doris8000 2 years, 9 months ago

Automatic Application Bypass (AAB) allows packets to bypass detection if Snort is down or if a packet takes too long to process. AAB causes Snort to restart within ten minutes of the failure, and generates troubleshooting data that can be analyzed to investigate the cause of the Snort failure.
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/device_management_basics.html

upvoted 4 times

Question #121 *Topic 1*

Which two features of Cisco AMP for Endpoints allow for an uploaded file to be blocked? (Choose two.)

A. application blocking

B. simple custom detection

C. file repository

D. exclusions

E. application allow listing

Suggested Answer: *AB*

d0980cc 2 months, 2 weeks ago

Selected Answer: BC

Lengthy document but search File Repository and Custom Detect

https://docs.amp.cisco.com/en/SecureEndpoint/Secure%20Endpoint%20User%20Guide.pdf

upvoted 1 times

gwb 9 months, 3 weeks ago

Cisco's AMP for Endpoints is a separate malware-protection product that can supplement malware protection provided by the Firepower system and be integrated with your Firepower deployment.

AMP for Endpoints is Cisco's enterprise-class Advanced Malware Protection solution that runs as a lightweight connector on individual users' endpoints (computers and mobile devices) to discover, understand, and block advanced malware outbreaks, advanced persistent threats, and targeted attacks.

Benefits of AMP for Endpoints include:

My answers are A and D

configure multiple aspects of outbreak control, including
1 automatic quarantines,
2 application blocking to stop non-quarantined executables from running
3 exclusion lists

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

upvoted 2 times

Doris8000 3 years, 3 months ago

answers are correct:
configure custom malware detection policies and profiles for your entire organization, as well as perform flash and full scans on all your users' files

perform malware analysis, including view heat maps, detailed file information, network file trajectory, and threat root causes

configure multiple aspects of outbreak control, including automatic quarantines, application blocking to stop non-quarantined executables from running, and exclusion lists

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html#id_96014

upvoted 4 times

Question #122 *Topic 1*

Which action should you take when Cisco Threat Response notifies you that AMP has identified a file as malware?

A. Add the malicious file to the block list.

B. Send a snapshot to Cisco for technical support.

C. Forward the result of the investigation to an external threat-analysis engine.

D. Wait for Cisco Threat Response to automatically block the malware.

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 1*

Which Cisco AMP for Endpoints policy is used only for monitoring endpoint activity?

A. Windows domain controller

B. audit

C. triage

D. protection

Suggested Answer: *B*

Reference:

https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/214933-amp-for-endpoints-deployment-methodology.html

gwb 9 months, 4 weeks ago

Audit

Policy Configuration Planning - Protection Engines

Other protection engines (such as Offline engines, Malicious Activity Protection, etc.) provide protection against additional malicious behaviors. Enabling each engine will improves the efficacy of Secure Endpoint. Depending on the engine or configurations enabled, the efficacy is improved at the cost of performance. When enabling or changing settings on an engine, it is recommended to test changes before deploying them to production endpoints.

Note: When activating a new Engine on a sensitive system which is divergent to the recommended settings, a good option is to start in Audit Mode. In Audit Mode, the connector generates an Event, but does not block in any way.

https://www.cisco.com/c/en/us/products/collateral/security/fireamp-endpoints/secure-endpoint-og.html

upvoted 3 times

Doris8000 3 years, 3 months ago

The answer is correct: Log the detection: In this mode, the identified malicious process is not blocked by MAP, but the detection is logged in the AMP for Endpoints console. (This is Audit mode, where no blocking or quarantine action happens, but the detection is logged.)

https://www.cisco.com/c/en/us/products/collateral/security/amp-for-endpoints/white-paper-c11-740980.html

upvoted 4 times

Question #124 *Topic 1*

What is a valid Cisco AMP file disposition?

A. non-malicious

B. malware

C. known-good

D. pristine

Suggested Answer: *B*

Community vote distribution

B (100%)

Doris8000 Highly Voted 1 year, 3 months ago

Disposition: malware, clean or unknown

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_malware_events_and_network_file_trajectory.html

upvoted 6 times

trickbot Highly Voted 10 months, 2 weeks ago

Selected Answer: B

malware

upvoted 5 times

Question #125 *Topic 1*

In a Cisco AMP for Networks deployment, which disposition is returned if the cloud cannot be reached?

A. unavailable

B. unknown

C. clean

D. disconnected

Suggested Answer: *A*

Community vote distribution

A (100%)

matan24 9 months, 3 weeks ago

Selected Answer: A

correct is A

upvoted 2 times

trickbot 1 year, 10 months ago

Selected Answer: A

unavailable

upvoted 2 times

Doris8000 2 years, 3 months ago

correct:

Unavailable indicates that the system could not query the AMP cloud

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_malware_events_and_network_file_trajectory.html

upvoted 3 times

Question #126 *Topic 1*

Which two remediation options are available when Cisco FMC is integrated with Cisco ISE? (Choose two.)

A. dynamic null route configured

B. DHCP pool disablement

C. quarantine

D. port shutdown

E. host shutdown

Suggested Answer: *CD*

Community vote distribution

CD (100%)

d0980cc 3 months, 3 weeks ago

Selected Answer: CD

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/710/management-center-admin-71/correlation-remediations.html

"the following Mitigation Actions on the source or destination host involved in a correlation policy violation:
*quarantine—Limits or denies an endpoint's access the network
*unquarantine—Reverses an endpoint's quarantine status and allows full access to the network
*shutdown—Deactivates an endpoint's network attached system (NAS) port to disconnect it from the network"

upvoted 1 times

c946f3e 9 months, 2 weeks ago

Selected Answer: CD

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/210524-configure-firepower-6-1-pxgrid-remediati.html#:~:text=Firepower%206.1%20Remediation%20module%20allows,not%20available%20for%20wireless%20deployments.

upvoted 4 times

Doris8000 2 years, 9 months ago

Firepower 6.1 Remediation module allows Firepower system to use ISE EPS capabilities (quarantine, unquarantine, port shutdown) as a remediation when correlation rule is matched.

upvoted 3 times

Question #127 *Topic 1*

Which connector is used to integrate Cisco ISE with Cisco FMC for Rapid Threat Containment?

A. pxGrid

B. FTD RTC

C. FMC RTC

D. ISEGrid

Suggested Answer: *A*

Doris8000 9 months, 2 weeks ago

ignore the previous one

the FireSIGHT Management Center (FMC) is configured for using self-signed certificates for ISE
pxGrid node operation.

upvoted 2 times

Doris8000 9 months, 2 weeks ago

This article does not cover initial configuration of ISE integration with Firepower, ISE integration with Active Directory (AD), Firepower integration with AD. For this information navigate to references section. Firepower 6.1 Remediation module allows Firepower system to use ISE EPS capabilities (quarantine, unquarantine, port shutdown) as a remediation when correlation rule is matched.

upvoted 1 times

Question #128 *Topic 1*

What is the maximum SHA level of filtering that Threat Intelligence Director supports?

A. SHA-1024

B. SHA-4096

C. SHA-512

D. SHA-256

Suggested Answer: *D*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html

gwb 9 months, 4 weeks ago

D.

TID and Security Intelligence

As part of your access control policy, Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domains. Security Intelligence uniquely provides access to industry-leading threat intelligence from Cisco Talos Intelligence Group (Talos). For more information on Security Intelligence, see About Security Intelligence.

TID enhances the system's ability to block connections based on security intelligence from third-party sources as follows:

TID supports additional traffic filtering criteria—Security Intelligence allows you to filter traffic based on IP address, URL, and (if DNS policy is enabled) domain name. TID also supports filtering by these criteria and adds support for filtering on SHA-256 hash values.

upvoted 3 times

Question #129 *Topic 1*

What is the advantage of having Cisco Firepower devices send events to Cisco Threat Response via the security services exchange portal directly as opposed to using syslog?

A. Firepower devices do not need to be connected to the Internet.

B. An on-premises proxy server does not need to set up and maintained.

C. All types of Firepower devices are supported.

D. Supports all devices that are running supported versions of Firepower

Suggested Answer: *B*
Reference:
https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide.pdf

Crazy_Creator Highly Voted 8 months, 2 weeks ago
Nope.
The correct answer is B -> for sure !
See the following link to feel confident :)
https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/CTR/Firepower_and_Cisco_Threat_Response_Integration_Guide/about_integrating_
upvoted 15 times

tinyJoe 5 months, 2 weeks ago
I have been confused all this time because your link was a list page.
For the opening sentence of the following link, B is correct. I finally understood.
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/integrations/xdr/secure-firewall-threat-defense-and-xdr-integration-guide/send_events_to_the_cloud_using_syslog.html#:~:text=configure%20your%20devices%20to%20send%20syslog%20messages%20to%20this%20prox
upvoted 2 times

Sarbi Most Recent 8 months, 4 weeks ago
The correct answer is D.
Thisintegration sendssupported eventsfrom Firepower devicesto CiscoSecureX threat response for analysis
alongside data from your other products and other sources
upvoted 3 times

Question #130 *Topic 1*

Which license type is required on Cisco ISE to integrate with Cisco FMC pxGrid?

A. apex

B. plus

C. base

D. mobility

Suggested Answer: *B*

Community vote distribution

B (71%) C (29%)

tinyJoe 6 months, 1 week ago

Selected Answer: B

From past documentation, I agree that the correct answer is B.

However, according to the following document, licenses containing ISE's PLUS are no longer sold and supported.
https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/identity-services-engine-base-plus-apex- license-pids-eol.html

upvoted 3 times

whysohardwhy 4 months, 2 weeks ago

Current - in the old license term it was PLUS.
Moving towards the new license Cisco's logic behind this is that integrations for example API uses would be advantage.
- from past Cisco training I attended.

upvoted 1 times

whysohardwhy 4 months, 2 weeks ago

With that being said I think this question should be retired or updated.

upvoted 1 times

MB2222 8 months, 4 weeks ago

Yes, (B) should be it regarding https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/admin_guide/b_ise_admin_guide_22/b_ise_admin_guide_22_chapter_0101.html

Please refer to section:
"Table 1. Cisco ISE License Packages":

- ISE License Packages == Plus AND
- ISE Functionality Covered == Cisco pxGrid

ALSO:

Within chapter "Traditional License Consumption" it says:

"pxGrid is used to share context collected by ISE with other products. A Plus license is required to enable pxGrid functionality. There is no session count decrement when context for session is shared. However, to use pxGrid, the number of Plus sessions licensed must be equal to the number of Base sessions licensed. For more information, see Cisco ISE Licenses and Services section in Cisco Identity Services Engine Ordering Guide."

upvoted 2 times

bassfunk 1 year, 4 months ago

Selected Answer: B

Going with B. See link and scroll to the license section.

https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/ise-licensing-guide-og.html#3CiscoISELicenses

upvoted 4 times

artgen 1 year, 4 months ago

This link explains it clearly. B is the right answer

upvoted 1 times

⊟ **Joe_Blue** 1 year, 9 months ago

Selected Answer: B

The license type required on Cisco ISE to integrate with Cisco FMC pxGrid is "Plus" license.

The Cisco Identity Services Engine (ISE) uses the Platform Exchange Grid (pxGrid) to integrate with other security products, such as the Cisco Firepower Management Center (FMC). To use pxGrid, a Plus license is required on Cisco ISE. The Plus license provides advanced network access control and security features, including integration with third-party products via pxGrid.

upvoted 2 times

⊟ **Baumb** 1 year, 10 months ago

Selected Answer: C

Im going with C, because of this thread:
https://community.cisco.com/t5/network-access-control/pxgrid-licensing/td-p/3563181

upvoted 2 times

⊟ **SanchezEldorado** 2 years, 8 months ago

This question should be more specific. I think C is the correct answer with the way it's worded. Only base licensing is required for pxGrid integration. You can use PassiveID with just base licensing which passes that onto the FMC through pxGrid. If you want to use context sharing and Rapid Threat Containment, THEN you need Plus licensing.

https://www.routexp.com/2017/11/cisco-ise-base-plus-and-apex-licenses.html

upvoted 3 times

Question #131 *Topic 1*

What is a feature of Cisco AMP private cloud?

A. It disables direct connections to the public cloud.

B. It supports security intelligence filtering.

C. It support anonymized retrieval of threat intelligence.

D. It performs dynamic analysis.

Suggested Answer: *A*

Community vote distribution

A (58%) D (42%)

Bobster02 Highly Voted 3 years, 11 months ago

Correct Answer is A. Please, read this line from the referenced article:
"Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud."

upvoted 15 times

Silexis Most Recent 4 months, 4 weeks ago

Selected Answer: A

The Cisco AMP Private Cloud do not perform Dynamic Malware Analysis. It is just storing the TI from Cisco Cloud and is sending anonymized information to that for analysis. To perform Dynamic Analysis, a Threat Grid appliance on-prem, is required to do the sandboxing part, which can be integrated with the AMP Private Cloud
At least, this is my understanding from the documentation

upvoted 1 times

squirrelzzz 11 months, 1 week ago

Selected Answer: D

key feature

upvoted 2 times

abf4823 1 year, 1 month ago

Selected Answer: A

Dynamic analysis relates to Thread Grid and this is a different appliance if on-prem is needed.

upvoted 1 times

Kris92 1 year, 4 months ago

Selected Answer: D

both A and D are correct, but performs dynamic analysis sounds more like a feature to me than disables direct connections to public AMP, don't get me wrong this can be seen as a feature also, it's just the way they said it

upvoted 2 times

bds90 1 year, 4 months ago

Selected Answer: D

https://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-742267.html

Powered by Cisco Threat Grid (TG), file analysis is available as an on-premises appliance. It provides static and dynamic analysis of unknown files to identify if a file is malicious and, if so, why.

upvoted 1 times

ffaiz 2 years ago

Selected Answer: A

Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/file_policies_and_amp_for_firepower.html#:~:text=Connecting%20a%20Firepower%20Management%20Center%20to%20an%20AMP%20private%20cloud

upvoted 2 times

Joe_Blue 2 years, 3 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/file_policies_and_amp_for_firepower.html

upvoted 1 times

Joe_Blue 2 years, 3 months ago

Selected Answer: D

The feature of Cisco AMP Private Cloud is that it performs dynamic analysis.

Cisco Advanced Malware Protection (AMP) is a comprehensive solution that provides continuous monitoring and analysis of network traffic, endpoints, and cloud applications to detect and prevent malware threats. Cisco AMP Private Cloud is a deployment option for AMP that allows organizations to deploy AMP in their private cloud environment while maintaining complete control over their data and security policies.

One of the key features of Cisco AMP Private Cloud is its ability to perform dynamic analysis. Dynamic analysis involves running a suspicious file or code in a virtual environment to observe its behavior and identify any malicious activities. Cisco AMP Private Cloud can also perform static analysis, sandboxing, and file reputation analysis to detect and block malware threats.

upvoted 1 times

pr0fectus 1 year, 8 months ago

D is not an option because on-prem dynamic analysis is performed by Threat-Grid on-prem.

upvoted 1 times

Baumb 2 years, 4 months ago

Selected Answer: A

https://www.cisco.com/c/en/us/products/collateral/security/fireamp-private-cloud-virtual-appliance/datasheet-c78-742267.html

upvoted 2 times

johanhc20 2 years, 11 months ago

Selected Answer: A

Your organization may have privacy or security concerns that make frequent or direct connections between your monitored network and the AMP cloud difficult or impossible. In these situations, you can set up a Cisco AMP Private Cloud, a proprietary Cisco product that acts as a compressed, on-premises version of the AMP cloud, as well as a secure mediator between your network and the AMP cloud. Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.

Correct A

upvoted 1 times

xziomal9 3 years ago

Selected Answer: A

Correct answer is: A

upvoted 1 times

ERGEGA 3 years, 4 months ago

Selected ANswer is A. Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud. The AMP private cloud does not perform dynamic analysis, nor does it support anonymized retrieval of threat intelligence for other features that rely on Cisco Collective Security Intelligence (CSI), such as URL and Security Intelligence filtering.

upvoted 1 times

liqucika 3 years, 5 months ago

Selected Answer: A

The whole point of having a private cloud is to avoid going out to the public one.

upvoted 1 times

orotta 3 years, 5 months ago

It looks the answer is A. please see below, I excerpted the following from the link

"The AMP private cloud does not perform dynamic analysis, nor does it support anonymized retrieval of threat intelligence for other features that rely on Cisco Collective Security Intelligence (CSI), such as URL and Security Intelligence filtering."

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Reference_a_wrapper_Chapter_topic_here.html

upvoted 1 times

Sarbi 3 years, 8 months ago

A is the correct answer. That is why we use the private Amp cloud.

upvoted 2 times

Doris8000 3 years, 9 months ago

this is the new link:

Connecting a Firepower Management Center to an AMP private cloud disables existing direct connections to the public AMP cloud.
https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/file_policies_and_amp_for_firepower.html

upvoted 1 times

Question #132 *Topic 1*

Which feature within the Cisco FMC web interface allows for detecting, analyzing, and blocking malware in network traffic?

A. intrusion and file events

B. Cisco AMP for Networks

C. file policies

D. Cisco AMP for Endpoints

Suggested Answer: *B*

Community vote distribution

B (100%)

⊟ **Nian** 2 months, 1 week ago

Selected Answer: C

In the FMC web interface: Policies -> Malware & File Policy - this allows detection, analysis and blocking file transfers across the network

upvoted 1 times

⊟ **z6st2a1jv** 1 year, 2 months ago

Selected Answer: B

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/file_policies_and_advanced_malware_protection.html#concept_5DC63E0AC3794E3FB7D59A52D7A337C2

About File Policies and Advanced Malware Protection

To detect and block malware, use file policies. You can also use file policies to detect and control traffic by file type.

Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Firepower Management Center web interface, this feature is called AMP for Networks, formerly called AMP for Firepower.

Since they also want to analyse, AMP is needed.

upvoted 3 times

⊟ **krellkrypto** 1 year, 4 months ago

" feature within the Cisco FMC web interface"

Im going with C. B is not a feature of the web portal, but of the system itself

upvoted 1 times

⊟ **gwb** 9 months, 4 weeks ago

I think it is dependent on the interpretation. For me, file policies are NOT feature, but Cisco AMP for Network sounds like more feature. so my answer is B

upvoted 1 times

⊟ **xziomal9** 2 years, 6 months ago

Selected Answer: B

Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Firepower Management Center web interface, this feature is called AMP for Networks, formerly called AMP for Firepower. Advanced Malware Protection identifies malware using managed devices deployed inline and threat data from the Cisco cloud.

upvoted 4 times

⊟ **Joninjimbo** 1 year, 2 months ago

Updated link, still same answer:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/file_policies_and_advanced_malware_protection.html

upvoted 2 times

⊟ **xziomal9** 2 years, 6 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/file_policies_and_advanced_malware_protection.html

upvoted 2 times

⊟ **Bobster02** 3 years, 5 months ago

B is my choice.

upvoted 4 times

⊟ **Bobster02** 3 years, 6 months ago

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/file_policies_and_advanced_malware_protection.html

upvoted 2 times

⊟ **kakakayayaya** 3 years, 6 months ago

Cisco AMP for Networks is a good and expensive feature but we do not need it to catch malware.
Just file policies and apply them to access polices.
C - right answer.

upvoted 1 times

⊟ **Stevens0103** 11 months ago

It's B.

"Advanced Malware Protection (AMP) for Firepower can detect, capture, track, analyze, log, and optionally block the transmission of malware in network traffic. In the Firepower Management Center web interface, this feature is called AMP for Networks, formerly called AMP for Firepower."

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/file_policies_and_advanced_malware_protection.html

upvoted 1 times

Question #133 *Topic 1*

A network administrator discovers that a user connected to a file server and downloaded a malware file. The Cisco FMC generated an alert for the malware event, however the user still remained connected. Which Cisco AMP file rule action within the Cisco FMC must be set to resolve this issue?

A. Malware Cloud Lookup

B. Reset Connection

C. Detect Files

D. Local Malware Analysis

Suggested Answer: *B*

Community vote distribution

B (100%)

Bobster02 Highly Voted 👍 3 years, 6 months ago

Reset Connection indeed.

upvoted 12 times

Heorhiiyatskovskyi Highly Voted 👍 3 years, 4 months ago

Cisco recommends that you enable Reset Connection for the Block Files and Block Malware actions to prevent blocked application sessions from remaining open until the TCP connection resets. If you do not reset connections, the client session will remain open until the TCP connection resets itself.

Answer - Reset connection

upvoted 9 times

bds90 Most Recent 11 months ago

Selected Answer: B

Action Resets Connection?

Block Files yes (recommended)

Block Malware yes (recommended)

Detect Files no

Malware Cloud Lookup no

upvoted 1 times

z6st2a1jv 1 year, 1 month ago

Selected Answer: B

It cannot be A:

Malware Cloud Lookup: This action queries the AMP cloud to determine if files traversing your network contain malware. It allows you to obtain and log the file's disposition based on its SHA-256 hash value. However, it allows the file through regardless of the disposition

upvoted 1 times

Cokamaniako 1 year, 7 months ago

Selected Answer: B

"Cisco recommends that you enable Reset Connection for the Block Files and Block Malware actions to prevent blocked application sessions from remaining open until the TCP connection resets. If you do not reset connections, the client session will remain open until the TCP connection resets itself. "

https://www.examtopics.com/discussions/cisco/view/54536-exam-300-710-topic-1-question-133-discussion/

upvoted 2 times

saad_SEIU 1 year, 8 months ago

it is A, The question is (Which Cisco AMP file rule action within the Cisco FMC must be set to resolve this issue?) there is no Reset Connection option.

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: B

Correct answer is: B

upvoted 2 times

trickbot 2 years, 10 months ago

Selected Answer: B

What they said

upvoted 1 times

liqucika 2 years, 11 months ago

Selected Answer: B

Reset connection

upvoted 1 times

Sarbi 3 years, 3 months ago

It is understood should be reset connection.

upvoted 3 times

kakakayayaya 3 years, 6 months ago

Reset Connection

upvoted 3 times

Question #134 *Topic 1*

An engineer has been tasked with using Cisco FMC to determine if files being sent through the network are malware. Which two configuration tasks must be performed to achieve this file lookup? (Choose two.)

A. The Cisco FMC needs to include a SSL decryption policy.

B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.

D. The Cisco FMC needs to connect with the FireAMP Cloud.

E. The Cisco FMC needs to include a file inspection policy for malware lookup.

Suggested Answer: *AE*

Community vote distribution

DE (33%) AE (33%) CE (17%) Other

netwguy Highly Voted 3 years, 4 months ago

I believe the correct answers are A and E. Bobster is referencing local malware analysis requirements, but we have no information that local malware analysis is begin used. By default theat grid is used, and threat grid needs no configuration on the FMC to connect to the cloud. The question states "which configuration tasks" - we dont need to do anything related to threat grid afaik. Also, if all file downloads going through the firewall are encrypted, then C and E would accomplish nothing.

upvoted 13 times

z6st2a1jv Highly Voted 1 year, 2 months ago

Selected Answer: DE

A. The Cisco FMC needs to include a SSL decryption policy.

> NO, this is Optional

B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

> NO these connect to "secure endpoint console", not to FMC. Tointegrate with AMP, they can send their data to AMP cloud (private or public),but not to FMC

C. The Cisco FMC needs to connect to the Cisco ThreatGrid service directly for sandboxing.

> NO direct connection is needed. Connection through a proxy is also possible

D. The Cisco FMC needs to connect with the FireAMP Cloud.

> YES - cloud can be private or public, but a connection IS required

E. The Cisco FMC needs to include a file inspection policy for malware lookup.

> YES - without filie policies, no files will be scanned.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/file_policies_and_advanced_malware_protection.html#ID-2193-00000132

upvoted 5 times

z6st2a1jv 1 year, 2 months ago

sorry need to correct a typo:

NO - direct connection is NOT needed. Connection through a proxy is also possible.

upvoted 1 times

gwb 9 months, 3 weeks ago

My answer are D and E. D should be adjusted from FireAMP to AMP Private Cloud

If your organization has high privacy requirements that restrict using a public cloud, the Cisco Advanced Malware Protection (AMP) Private Cloud Virtual Appliance is an on-premises, air-gapped option.

upvoted 1 times

bds90 Most Recent 11 months ago

Selected Answer: AE

A: because you can't inspect any traffic that it's encrypted (majority of the traffic):

You can use SSL decryption policies to turn encrypted traffic into plain text traffic, so that you can then apply URL filtering, intrusion and malware control

upvoted 1 times

whysohardwhy 4 months, 2 weeks ago

What about unencrypted traffic? It's not a "must"

upvoted 1 times

Dreng65 1 year, 5 months ago

Selected Answer: BE

Option E is mandatory.
A can be, but not necessary (i still can inspect malware in http and ftp protocols whitout ssl inspection)
C seems more precise.
Cisco Threat Grid runs the file in a sandbox environment, analyzes the file's behavior to determine whether the file is malicious, and returns a threat score that indicates the likelihood that a file contains malware. From the threat score, you can view a dynamic analysis summary report with the reasons for the assigned threat score. You can also look in Cisco Threat Grid to view detailed reports for files that your organization submitted, as well as scrubbed reports with limited data for files that your organization did not submit.
https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/file_policies_and_advanced_malware_protection.html

upvoted 1 times

SegaMasterSystemAdmin 1 year, 6 months ago

Selected Answer: CE

Make most sense.

upvoted 1 times

THEODORABLE 1 year, 7 months ago

D&E - the operative key in the question: "To achieve this file lookup". SSL decryption is not needed to perform the lookup. SSL Decryption -To be able to test the traffic if encrypted--yes but not to perform the lookup.

upvoted 2 times

Silexis 4 months, 4 weeks ago

You can't perform any file lookul if the connection is TLS-ed!
Try yourself to pass an EICAR file through a SSL connection and see if it is stopped. The only protection you can apply on SSL flows are URL categories and DNS Reputation check

upvoted 1 times

Joe_Blue 1 year, 9 months ago

Selected Answer: BE

The two configuration tasks that must be performed in order to use Cisco FMC to determine if files being sent through the network are malware are:

E. The Cisco FMC needs to include a file inspection policy for malware lookup.
B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

Explanation:

E. The Cisco FMC needs to include a file inspection policy for malware lookup:
A file inspection policy can be used to inspect and analyze files that are transmitted over the network to determine if they contain malware. By configuring a file inspection policy in Cisco FMC, you can specify the types of files that should be inspected, the types of malware to look for, and the actions to take when malware is detected.

B. The Cisco FMC needs to connect to the Cisco AMP for Endpoints service:
By connecting to the Cisco AMP for Endpoints service, Cisco FMC can leverage the advanced threat intelligence provided by AMP to analyze and identify potential malware threats in network traffic.

upvoted 1 times

matan24 1 year, 9 months ago

B is saying "AMP for Endpoints" - the firepower uses AMP for networks

upvoted 2 times

ureis 1 year, 7 months ago

this guys are copy an dpasting chat gpt here, sad

upvoted 3 times

Baumb 1 year, 10 months ago

Selected Answer: DE

You dont NEED SSL decryption, as files can be transmitted over literally any port in cleartext.

You also dont need sandboxing, but what you DO need is a connection to the public AMP or a private AMP cloud. So Im choosing DE

upvoted 4 times

Joninjimbo 1 year, 2 months ago

Agreed.

Its not B. From the config guide "(Optional) Malware Protection with AMP for Endpoints", B is optional.

A is also optional

It's clearly D because of the following from the guide:

"If a file rule is configured with a Malware Cloud Lookup or Block Malware action and the Firepower Management Center cannot establish connectivity with the AMP cloud, the system cannot perform any configured rule action options until connectivity is restored."

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/file_policies_and_advanced_malware_protection.html#id_96014

upvoted 5 times

Jmonteiro33 2 years, 3 months ago

I think its C and D. Please take a look at this ciscolive doc at page 22

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2019/pdf/BRKSEC-2890.pdf

upvoted 1 times

dique 2 years, 4 months ago

Selected Answer: CE

Correct answer : C and E

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: CE

Correct answer is: C and E

upvoted 1 times

xYanivDx 2 years, 7 months ago

Selected Answer: AE

A & E

You need to decrypt the traffic

upvoted 3 times

hz033 2 years, 7 months ago

Selected Answer: BE

B and E

The Cisco FMC needs to connect to the Cisco AMP for Endpoints service.

upvoted 1 times

trickbot 2 years, 10 months ago

Selected Answer: AE

A and E. Focusing on configurations needed.

upvoted 2 times

Sarbi 3 years, 2 months ago

The correct answer is A and E.

upvoted 4 times

Bobster02 3 years, 6 months ago

I would go with original C and E. Cisco configuration guide stipulates that:

Local malware analysis does not require establishing communications with the Cisco Threat Grid cloud. However, you must configure communications with the cloud to submit files pre classified as malware for dynamic analysis, and to download updates to the local malware analysis rule set.

upvoted 1 times

⊟ **kakakayayaya** 3 years, 6 months ago

I would chose A and E

upvoted 3 times

Question #135 *Topic 1*

A network engineer wants to add a third-party threat feed into the Cisco FMC for enhanced threat detection. Which action should be taken to accomplish this goal?

A. Enable Rapid Threat Containment using REST APIs.

B. Enable Rapid Threat Containment using STIX and TAXII.

C. Enable Threat Intelligence Director using REST APIs.

D. Enable Threat Intelligence Director using STIX and TAXII.

Suggested Answer: *D*

Reference:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html

Community vote distribution

D (100%)

greeklover84 9 months, 2 weeks ago

Selected Answer: D

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/cisco_threat_intelligence_director__tid_.html

upvoted 2 times

Question #136 *Topic 1*

A network engineer is logged into the Cisco AMP for Endpoints console and sees a malicious verdict for an identified SHA-256 hash. Which configuration is needed to mitigate this threat?

A. Add the hash to the simple custom detection list

B. Use regular expressions to block the malicious file

C. Enable a personal firewall in the infected endpoint

D. Add the hash from the infected endpoint to the network block list

Suggested Answer: *A*

Community vote distribution

A (100%)

greeklover84 9 months, 2 weeks ago

Selected Answer: A

https://www.cisco.com/c/en/us/support/docs/security/amp-endpoints/215176-configure-a-simple-custom-detection-list.html

upvoted 3 times

LangaMos 11 months, 2 weeks ago

Simple Custom Detection is a method for identifying and quarantining a specific file by its SHA-256 hash

upvoted 3 times

Question #137 *Topic 1*

A network administrator is concerned about the high number of malware files affecting users' machines. What must be done within the access control policy in
Cisco FMC to address this concern?

A. Create an intrusion policy and set the access control policy to block

B. Create an intrusion policy and set the access control policy to allow

C. Create a file policy and set the access control policy to allow

D. Create a file policy and set the access control policy to block

Suggested Answer: *C*

Community vote distribution

C (80%) D (20%)

⊟ **Doris8000** Highly Voted 3 years, 3 months ago

correct it should be C

Access control rules:

Rule 3: Block evaluates traffic third. Matching traffic is blocked without further inspection. Traffic that does not match continues to the final rule.

Rule 4: Allow is the final rule. For this rule, matching traffic is allowed; however, prohibited files, malware, intrusions, and exploits within that traffic are detected and blocked. Remaining non-prohibited, non-malicious traffic is allowed to its destination, though it is still subject to identity requirements and rate limiting. You can configure Allow rules that perform only file inspection, or only intrusion inspection, or neither.

upvoted 6 times

⊟ **dariol** Highly Voted 3 years, 4 months ago

C should be correct, but the word policy makes it unclear. If the ACP itself has the default action of block all traffic then it has no bearing on the individual rules and the file policy can trigger.

If the rule is set to block then the file policy will never trigger.

upvoted 5 times

⊟ **gwb** Most Recent 9 months, 3 weeks ago

my answer is D. blocking

upvoted 1 times

⊟ **Joe_Blue** 1 year, 9 months ago

Selected Answer: D

To address the concern of high number of malware files affecting users' machines, a network administrator should create a file policy within Cisco FMC. A file policy allows the administrator to control the type of files that are allowed or blocked from entering the network.

To reduce the number of malware files affecting users' machines, the access control policy should be set to block the files that are known to carry malware. This can be achieved by creating a file policy that includes a list of file types and attributes that are associated with malware. By setting the access control policy to block, the system will automatically prevent any incoming files that match the criteria set in the file policy.

upvoted 2 times

⊟ **tanri04** 1 year, 9 months ago

D. Create a file policy and set the access control policy to block.

To address the concern of malware files affecting users' machines, the network administrator should create a file policy in Cisco FMC and set the access control policy to block. This will prevent the malware files from being downloaded or executed on users' machines.

Creating an intrusion policy and setting the access control policy to block or allow may help with preventing network-based attacks, but it may not be effective in preventing malware files from being downloaded or executed on users' machines.

Therefore, the best approach would be to create a file policy that can inspect and block malicious files and set the access control policy to block any attempt to download or execute these files.

upvoted 3 times

tanri04 1 year, 9 months ago

Creating a file policy and setting the access control policy to allow would allow users to download files without restrictions, but the file policy would still be able to inspect the files for malware and block them if necessary. This could be a valid option if the network administrator wants to allow users more freedom to download files while still maintaining some level of security.

However, the best approach would still be to create a file policy and set the access control policy to block, as this would provide the highest level of security against malware files

upvoted 2 times

matan24 1 year, 9 months ago

Selected Answer: C

clearly C

upvoted 1 times

HideFury 2 years ago

Selected Answer: C

Correct answer is: C

upvoted 1 times

BorZol 2 years, 3 months ago

Selected Answer: C

blocking in ACP will never use file policy and block everything.
Creating a file policy adding it to the ACP and block within file policy is a good solution.

upvoted 1 times

dique 2 years, 4 months ago

Selected Answer: C

Correct answer is C

upvoted 1 times

xziomal9 2 years, 6 months ago

Selected Answer: C

Correct answer is: C

upvoted 1 times

liqucika 2 years, 11 months ago

Selected Answer: C

Can't further inspect traffic on a block action in ACP.

upvoted 4 times

cryptofetti 3 years, 4 months ago

can't*

upvoted 1 times

cryptofetti 3 years, 4 months ago

Wouldnt this be C, since you can inspect a file its set to a block action?

upvoted 4 times

Question #138 *Topic 1*

Within an organization's high availability environment where both firewalls are passing traffic, traffic must be segmented based on which department it is destined for. Each department is situated on a different LAN. What must be configured to meet these requirements?

A. redundant interfaces

B. span EtherChannel clustering

C. high availability active/standby firewalls

D. multi-instance firewalls

Suggested Answer: *D*

d0980cc 3 months, 3 weeks ago

Selected Answer: C

2 Options:
On the FTD devices in the HA pair, configure interfaces to handle traffic for each department's VLAN:
*Option 1: Subinterfaces for VLANs
If the FTD is connected to a trunk port, configure subinterfaces on a physical interface for each VLAN.
Example:
Interface GigabitEthernet0/0.10 for VLAN 10 (Department A)
Interface GigabitEthernet0/0.20 for VLAN 20 (Department B)
Interface GigabitEthernet0/0.30 for VLAN 30 (Department C)
Assign IP addresses to each subinterface in the corresponding subnet (e.g., 192.168.10.1 for VLAN 10).
*Option 2: Separate Physical Interfaces
If each department's traffic arrives on a dedicated physical interface, configure those interfaces with the appropriate IP addresses and security zones.

Sorry, but have to go against the grain on this one. I choose C.

upvoted 1 times

d0980cc 2 months, 2 weeks ago

Retract, I choose B
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/740/management-center-device-config-74/device-op
3100.html?
bookSearch=true#concept_txk_fnz_pz:~:text=to%20load%2Dbalance%20the%20data%20coming%20to%20and%20from%20the%20cluster%20using%20Sp

upvoted 1 times

tinyJoe 5 months, 2 weeks ago

Selected Answer: D

This is a very unclear question, but I guess it would be D.

I assume that the author's intended configuration is similar to the "Network Diagram" in the following document:
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-management-center-virtual/221625-configure-ftd-multi-instance-high-availa.html#toc-hId--1943291811

We will configure an HA with two FTDs, each with two instances.
Then, for instance A, Unit 1 is Active - Unit 2 is Passive, and for instance B, Unit 1 is Passive - Unit 2 is Active.
In this way, even with Active/Passive HA, the "both firewalls are passing traffic" requirement of the question can be satisfied.

upvoted 1 times

gwb 9 months, 4 weeks ago

segmentation means separation. Redundant interface is backup, not separation. EtherChannel is to bump up throughput and redundant path. HA active/standby - does NOT allow both firewalls passing traffic

upvoted 3 times

Question #139

Topic 1

An engineer is configuring a Cisco IPS to protect the network and wants to test a policy before deploying it. A copy of each incoming packet needs to be monitored while traffic flow remains constant. Which IPS mode should be implemented to meet these requirements?

A. routed

B. passive

C. transparent

D. inline tap

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #140 *Topic 1*

A network security engineer must replace a faulty Cisco FTD device in a high availability pair. Which action must be taken while replacing the faulty unit?

A. Ensure that the faulty Cisco FTD device remains registered to the Cisco FMC

B. Shut down the active Cisco FTD device before powering up the replacement unit

C. Shut down the Cisco FMC before powering up the replacement unit

D. Unregister the faulty Cisco FTD device from the Cisco FMC

Suggested Answer: *D*

Community vote distribution

D (83%) A (17%)

achille5 9 months, 4 weeks ago

Selected Answer: A

This is an example of RMA'd process, unregistering the faulty kind of easy pick here. But it is not the first to consideration in real scenario when RMA'd an HA FTD. Need to retain first the faulty FTD for back restoration purposes. You can register the new device first using different IP. ..

upvoted 1 times

achille5 8 months, 2 weeks ago

https://community.cisco.com/t5/network-security/replace-primary-ftd-with-new-ftd/td-p/4403671

upvoted 1 times

Bbb78 1 year, 7 months ago

Taking as reference the steps to Replace a Primary FTD HA Unit from cisco (https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/fpmc-config-guide-v601_chapter_01100110.pdf) page 21. The right answer is D. Unregister the faulty Cisco FTD device from the Cisco FMC.

Step 1 Choose Force Break to separate the high availability pair; see Separate Units in a High Availability Pair, on
page 22.
The break operation removes all the configuration related to HA from Firepower Threat Defense
and Firepower Management Center, and you need to recreate it manually later. To successfully
configure the same HA pair, ensure that you save the IPs, MAC addresses, and monitoring
configuration of all the interfaces/subinterfaces prior to executing the HA break operation.
Note
Step 2 Unregister the failed primary Firepower Threat Defense device from the Firepower Management Center; see
Deleting Devices from the Firepower Management Center.
Step 3 Register the replacement Firepower Threat Defense to the Firepower Management Center; see Add Devices
to the Firepower Management Center

upvoted 2 times

Initial14 1 year, 8 months ago

Selected Answer: D

Only D makes sense

upvoted 1 times

Baumb 1 year, 10 months ago

Selected Answer: D

unregistering is the only logical option

upvoted 2 times

Baumb 1 year, 10 months ago

Selected Answer: D

It should be D why A?

upvoted 1 times

Dolby58 1 year, 10 months ago

Selected Answer: D

It's D.

A makes no sense.

upvoted 1 times

Question #141 *Topic 1*

An administrator is optimizing the Cisco FTD rules to improve network performance, and wants to bypass inspection for certain traffic types to reduce the load on the Cisco FTD. Which policy must be configured to accomplish this goal?

A. intrusion

B. prefilter

C. URL filtering

D. identity

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #142 *Topic 1*

A Cisco FTD has two physical interfaces assigned to a BVI. Each interface is connected to a different VLAN on the same switch. Which firewall mode is the Cisco FTD set up to support?

A. high availability clustering

B. active/active failover

C. transparent

D. routed

Suggested Answer: *D*

Community vote distribution

D (59%) C (41%)

Joe_Blue Highly Voted 👍 2 years, 3 months ago

Selected Answer: C

The Cisco FTD configured with two physical interfaces assigned to a BVI and connected to different VLANs on the same switch is set up to support the transparent firewall mode.

In transparent mode, the firewall operates at Layer 2, and does not modify the IP address or MAC address of the packets passing through it. In this mode, the firewall is transparent to the devices on either side of it, and can be inserted into the network without changing the IP addressing or topology.

upvoted 6 times

d0980cc Most Recent ⊙ 3 months, 3 weeks ago

Selected Answer: C

Transparent Mode the FTD acts as a "bump in the wire" or a Layer 2 bridge between network segments. It does not route traffic (like in Routed Mode) but instead forwards traffic between interfaces based on Layer 2 information (MAC addresses). The use of a BVI allows the FTD to bridge traffic between the two physical interfaces while applying security policies.

upvoted 1 times

achille5 1 year, 2 months ago

Selected Answer: C

Transparent. This mean 2 brigde group, 2 BVI IPs.

upvoted 2 times

devildog 9 months, 3 weeks ago

D.

If you are passing traffic between multiple VLANs, those are separate networks entirely. In order for them to communicate, there needs to be routing in place.

upvoted 2 times

Bubu3k 1 year, 5 months ago

Selected Answer: D

About Transparent Firewall Mode:

Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the FTD device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a Bridge Virtual Interface (BVI) to which you assign an IP address on the network. You can have multiple bridge groups for multiple networks. In transparent mode, these bridge groups cannot communicate with each other.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

upvoted 4 times

aalnman 1 year, 10 months ago

Selected Answer: C

Actually, BVI can run in both routed and transparent. In this situation I think it is transparent. Here is what AI has to say about it:

On the Cisco Firepower Threat Defense (FTD) device, you can use a Bridge Virtual Interface (BVI) in both transparent and routed firewall modes. In transparent mode, Layer 2 connectivity is achieved by using a "bridge group" where you group together the inside and outside interfaces for a network, and the FTD device uses bridging techniques to pass traffic between the interfaces. Each bridge group includes a BVI to which you assign an IP address on the network¹. In routed mode, the FTD device routes between BVIs and regular routed interfaces. If you do not need clustering or EtherChannel member interfaces, you might consider using routed mode instead of transparent mode². Is there anything else you would like to know? 😊

upvoted 2 times

⊟ **aalnman** 1 year, 10 months ago

Selected Answer: D

A bridge group is a group of interfaces that the FTD device bridges instead of routes. All interfaces are on the same network. The bridge group is represented by a Bridge Virtual Interface (BVI) that has an IP address on the bridge network.

You can route between routed interfaces and BVIs, if you name the BVI. In this case, the BVI acts as the gateway between member interfaces and routed interfaces. If you do not name the BVI, traffic on the bridge group member interfaces cannot leave the bridge group. Normally, you would name the interface so that you can route member interfaces to the internet.

One use for a bridge group in routed mode is to use extra interfaces on the FTD device instead of an external switch. You can attach endpoints directly to bridge group member interfaces. You can also attach switches to add more endpoints to the same network as the BVI.

upvoted 3 times

⊟ **SegaMasterSystemAdmin** 2 years ago

Selected Answer: D

To me routed is the right answer because each interface is on a different VLAN, if you have a regular bump in the wire configuration like transparent mode you won't be able to route traffic to each other, so you will need to have a bridge group in routed mode.

upvoted 4 times

⊟ **spambox730** 1 year, 11 months ago

The 2 VLANs can use the same IP subnet so routing is not required. We used this setup.

upvoted 4 times

⊟ **gwb** 1 year, 3 months ago

yeah. technically possible. but not recommended. what if I change the question like that "Each interface is connected to a same VLAN on the same switch) - this is definietely transparent. but Q is asking a different vlan (usually different subnets), so my choice is D

Layer 2 Segmentation: VLANs provide layer 2 segmentation, meaning they separate broadcast domains. Each VLAN operates as if it were a separate physical network. Devices within the same VLAN can communicate directly with each other at the data link layer (using MAC addresses). while it's technically possible for two VLANs to use the same IP subnet, it's generally better to keep them separate to avoid potential issues.

upvoted 1 times

⊟ **saad_SEIU** 2 years, 2 months ago

Selected Answer: C

C for sure

upvoted 1 times

Question #143 *Topic 1*

An organization is migrating their Cisco ASA devices running in multicontext mode to Cisco FTD devices. Which action must be taken to ensure that each context on the Cisco ASA is logically separated in the Cisco FTD devices?

A. Configure a container instance in the Cisco FTD for each context in the Cisco ASA.

B. Add the Cisco FTD device to the Cisco ASA port channels.

C. Configure the Cisco FTD to use port channels spanning multiple networks.

D. Add a native instance to distribute traffic to each Cisco FTD context.

Suggested Answer: *A*

tinyJoe 6 months, 1 week ago

Selected Answer: A

answer is A. see this:
https://community.cisco.com/t5/security-blogs/migrating-asa-multi-context-to-ftd-multi-instance/ba-p/3893465

upvoted 2 times

Baumb 10 months, 3 weeks ago

A, see:
https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2019/pdf/BRKSEC-3035.pdf

upvoted 3 times

Question #144 *Topic 1*

An engineer wants to change an existing transparent Cisco FTD to routed mode. The device controls traffic between two network segments. Which action is mandatory to allow hosts to reestablish communication between these two segments after the change?

A. Remove the existing dynamic routing protocol settings.

B. Configure multiple BVIs to route between segments.

C. Assign unique VLAN IDs to each firewall interface.

D. Implement non-overlapping IP subnets on each segment.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #145 *Topic 1*

An engineer installs a Cisco FTD device and wants to inspect traffic within the same subnet passing through a firewall and inspect traffic destined to the Internet. Which configuration will meet this requirement?

A. transparent firewall mode with IRB only

B. routed firewall mode with BVI and routed interfaces

C. transparent firewall mode with multiple BVIs

D. routed firewall mode with routed interfaces only

Suggested Answer: *C*

Community vote distribution

C (67%) B (33%)

tinyJoe 6 months, 1 week ago

Selected Answer: C

I dont want to agree, but I guess the answer is C.
The question seems to have been created by imagining Fig. 1 of the following document.
https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html

upvoted 1 times

TodaniTE 11 months ago

Selected Answer: C

I go with C here.

upvoted 3 times

z6st2a1jv 1 year, 2 months ago

Selected Answer: B

Transparent firewall will not allow the traffic out to the intenet, because it does not do routing between inside and outside subnets. Routed firewall with a bvi that acts as a switch for the inside hosts and a a routed interface with the public subnet is needed here

upvoted 1 times

Kris92 10 months, 1 week ago

it doesn't say the traffic needs to be routed by the FTD, just traffic destined to the Internet needs to be inspected, so it could be transparent

upvoted 2 times

gwb 9 months, 4 weeks ago

agree with Kris92. destination internet does not mean FTD needs to be routed mode

upvoted 1 times

rbrain 6 months, 2 weeks ago

Destination internet needs a gateway and routing. I assume this means on the same FTD. B would be my choice

upvoted 1 times

wordisbondkid 9 months ago

I agree with B. It can fulfill requirements of both.

upvoted 2 times

Question #146 *Topic 1*

A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. It must also collect data to provide a baseline of unwanted traffic before being reconfigured to drop it. Which Cisco IPS mode meets these requirements?

A. failsafe

B. inline tap

C. promiscuous

D. bypass

Suggested Answer: *B*

Community vote distribution

B (52%) C (48%)

Initial14 Highly Voted 1 year, 9 months ago

Selected Answer: B

The question states:
A network administrator is deploying a Cisco IPS appliance and needs it to operate initially without affecting traffic flows. IT NEEDS TO OPERATE INITIALY, meaning inline tap, because in the future, we willgo from not affecting traffic, to activating IPS. if you use passive deployment, meaning you copy data to IPS in the future you can't implement IPS rule blocking. For me It's B

upvoted 9 times

achille5 Most Recent 8 months, 2 weeks ago

Selected Answer: C

https://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliinter.html#wp1033759

upvoted 2 times

aalnman 1 year, 4 months ago

Selected Answer: C

I believe C as well.

upvoted 1 times

SegaMasterSystemAdmin 1 year, 6 months ago

Selected Answer: C

This is talking about a Cisco IPS appliance and not a FTD so leaning towards promiscuous mode

upvoted 2 times

bobie 1 year, 6 months ago

Selected Answer: C

https://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliinter.html#wp1033699

upvoted 1 times

ureis 1 year, 7 months ago

"It must also collect data" meaning copy the data, only tap mode copy data without affect the network

upvoted 1 times

> **ureis** 1 year, 7 months ago
>
> OBS: TAP cant drop packets, so C is correct
>
> upvoted 1 times

Joe_Blue 1 year, 9 months ago

Selected Answer: C

The promiscuous mode of the Cisco IPS meets these requirements. It can be configured to operate initially without affecting traffic flows and collects data to provide a baseline of unwanted traffic before being reconfigured to drop it. In promiscuous mode, the IPS is configured to monitor traffic only and does not affect the flow of packets.

upvoted 2 times

Dolby58 1 year, 10 months ago

Selected Answer: C

C is correct!

upvoted 2 times

Dolby58 1 year, 10 months ago

Selected Answer: B

B is correct.

Promiscuous mode doesn't exist.

upvoted 3 times

ureis 1 year, 7 months ago

Promiscuous = Transparent Mode

upvoted 1 times

Dolby58 1 year, 10 months ago

I stand corrected. It's not B.

The question is about Cisco IPS which has three modes: Promiscuous, Inline and Bypass. So C is correct.

https://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliinter.html#wp1033938

upvoted 1 times

Question #147 *Topic 1*

A network administrator is implementing an active/passive high availability Cisco FTD pair. When adding the high availability pair, the administrator cannot select the secondary peer. What is the cause?

A. The second Cisco FTD is not the same model as the primary Cisco FTD.

B. An high availability license must be added to the Cisco FMC before adding the high availability pair.

C. The failover link must be defined on each Cisco FTD before adding the high availability pair.

D. Both Cisco FTD devices are not at the same software version.

Suggested Answer: *C*

Community vote distribution

C (50%) A (25%) D (25%)

Vlad_Is_Love_ua 10 months, 2 weeks ago

From this:
https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html

....
Conditions
In order to create an HA between 2 FTD devices, these conditions must be met:

Same model
Same version- this applies to FXOS and to FTD - major (first number), minor (second number), and maintenance (third number) must be equal.
Same number of interfaces
Same type of interfaces
Both devices as part of the same group/domain in FMC.
Have identical Network Time Protocol (NTP) configuration.
Be fully deployed on the FMC without uncommitted changes.
Be in the same firewall mode: routed or transparent.
....

So both A & D are CORRECT
upvoted 3 times

d0980cc 2 months, 2 weeks ago

Why does Cisco do this? There are many questions that have two correct answers, or in some cases several correct answers. Who knows how they're splitting hairs on a question like this!
upvoted 2 times

SegaMasterSystemAdmin 1 year ago

Selected Answer: A

The hardware and software version needs to be the same before HA can be implemented, hardware is the first requirement. The failover link cannot be defined if the administrator cannot select the secondary peer so the answer is A.
upvoted 3 times

Cokamaniako 1 year, 1 month ago

Selected Answer: A

Before of configure the failover link you must add the devices inside HA
The first step is check the model

https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212699-configure-ftd-high-availability-on-firep.html
upvoted 2 times

Initial14 1 year, 2 months ago

Selected Answer: D

tested in LAB: FMC version 7.3, one FTD 7.0.4 and another 7.3: When you select Primary peer, you can't select secondary. So D is the one.

upvoted 2 times

Bbb78 1 year, 1 month ago

yes, but what if they are different models ? you cannot make HS from 2100 and 4100 ?

so IT CAN BE BOTH a AND d

upvoted 2 times

Initial14 1 year, 2 months ago

You do not select HA - link until you add HA Pair. In HA pair you select devices that will be Active/Passive. After you add devices as HA, then you configure what will be Failover and state link.

upvoted 3 times

matan24 1 year, 3 months ago

I think It's C as well.

A+D are required but the question said he can't even see the second appliance, so I believe it's the failover link:

"Configuring high availability requires two identical FTD devices connected to each other through a dedicated failover link"

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-ha.html

upvoted 1 times

Baumb 1 year, 4 months ago

Selected Answer: C

A. The second Cisco FTD is not the same model as the primary Cisco FTD.

-> A and D are requirements that have to be fulfilled, so it cannot be one of those

B. An high availability license must be added to the Cisco FMC before adding the high availability pair.

You dont need a HA license, only the FTD licenses for both

C. The failover link must be defined on each Cisco FTD before adding the high availability pair.

-> That leaves C as the only viable answer

D. Both Cisco FTD devices are not at the same software version.

-> See A

upvoted 4 times

Initial14 1 year, 2 months ago

The trick here is : The administrator cannot select the secondary peer. You are selecting secondary peer before any Failover/state link, and if you cant see secondary peer, then it is A or D.

upvoted 1 times

Question #148 *Topic 1*

An administrator is configuring their transparent Cisco FTD device to receive ERSPAN traffic from multiple switches on a passive port, but the Cisco FTD is not processing the traffic. What is the problem?

A. The switches do not have Layer 3 connectivity to the FTD device for GRE traffic transmission.

B. The switches were not set up with a monitor session ID that matches the flow ID defined on the Cisco FTD.

C. The Cisco FTD must be in routed mode to process ERSPAN traffic.

D. The Cisco FTD must be configured with an ERSPAN port not a passive port.

Suggested Answer: *C*

Community vote distribution

C (50%) A (40%) 10%

Silexis 4 months, 4 weeks ago

Selected Answer: C

ERSPAN can be configured only when FTD is in ROUTED MODE

upvoted 1 times

MB2222 8 months, 1 week ago

Answer is (C).
See section "Guidelines for Inline Sets and Passive Interfaces"
Firewall Mode
- ERSPAN interfaces are only allowed when the device is in routed firewall mode.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html#id_19616

upvoted 4 times

achille5 9 months, 4 weeks ago

Selected Answer: C

The Cisco ERSPAN feature allows you to monitor traffic on ports or VLANs and send the monitored traffic to destination ports. The ERSPAN feature requires IP routing to be enabled in the Global Configuration Mode.
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/16-6/configuration_guide/nmgmt/b_166_nmgmt_9400_cg/b_166_nmgmt_9400_cg_chapter_01000.pdf

upvoted 2 times

cla8829 1 year, 6 months ago

A & C
Passive or ERSPAN Passive—Passive interfaces monitor traffic flowing across a network using a switch SPAN or mirror port. The SPAN or mirror port allows for traffic to be copied from other ports on the switch. This function provides the system visibility within the network without being in the flow of network traffic. When you configure the FTD in a passive deployment, the FTD cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally. and no traffic received on these interfaces is retransmitted. Encapsulated remote switched port analyzer (ERSPAN) interfaces allow you to monitor traffic from source ports distributed over multiple switches, and uses GRE to encapsulate the traffic. ERSPAN interfaces are only allowed when the FTD is in routed firewall mode.

upvoted 3 times

Bbb78 1 year, 7 months ago

Selected Answer: D

Not sure its C ....
"
To process ERSPAN traffic, an FTD device should have an ERSPAN interface configured. The ERSPAN interface is specifically designed to receive and decode ERSPAN traffic. The ERSPAN interface can be connected to an ERSPAN source port on a switch or other devices to capture and analyze the encapsulated ERSPAN traffic."

upvoted 1 times

Bbb78 1 year, 7 months ago

Disregard - this FTD is in transparent mode ....sorry did not saw that. Option C is correct.

upvoted 2 times

⊟ **Initial14** 1 year, 9 months ago

Selected Answer: C

The firewall must be in routed mode for ERSPAN

upvoted 2 times

⊟ **Joe_Blue** 1 year, 9 months ago

Selected Answer: C

Guidelines for Inline Sets and Passive Interfaces Firewall Mode

ERSPAN interfaces are only allowed when the device is in routed firewall mode.

upvoted 2 times

⊟ **lapsi** 1 year, 10 months ago

Isn't it C.

refer:
https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/inline_sets_and_passive_interfaces_for_firepower_threat_defense.html

"ERSPAN interfaces are only allowed when the FTD is in routed firewall mode"

upvoted 2 times

⊟ **Seawanderer** 1 year, 11 months ago

Selected Answer: A

It's A. If not already in routed mode, the interfaced couldn't be configured

upvoted 4 times

Question #149 *Topic 1*

What is an advantage of adding multiple inline interface pairs to the same inline interface set when deploying an asynchronous routing configuration?

A. Allows the IPS to identify inbound and outbound traffic as part of the same traffic flow.

B. The interfaces disable autonegotiation and interface speed is hard coded set to 1000 Mbps.

C. Allows traffic inspection to continue without interruption during the Snort process restart.

D. The interfaces are automatically configured as a media-independent interface crossover.

Suggested Answer: *A*

Community vote distribution

A (100%)

c946f3e 9 months, 2 weeks ago

Selected Answer: A

Adding multiple inline interface pairs to the same inline interface set allows the system to identify the inbound and outbound traffic as part of the same traffic flow. For passive interfaces only, you can also achieve this by including the interface pairs in the same security zone.
https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01011010.html

upvoted 4 times

Question #150 *Topic 1*

A network administrator cannot select the link to be used for failover when configuring an active/passive HA Cisco FTD pair. Which configuration must be changed before setting up the high availability pair?

A. An IP address in the same subnet must be added to each Cisco FTD on the interface.

B. The interface name must be removed from the interface on each Cisco FTD.

C. The name Failover must be configured manually on the interface on each Cisco FTD.

D. The interface must be configured as part of a LACP Active/Active EtherChannel.

Suggested Answer: *B*

Community vote distribution

B (100%)

Initial14 Highly Voted 8 months, 2 weeks ago

Selected Answer: B

B 100%. tested in LAB

upvoted 5 times

tinyJoe Most Recent 6 months, 1 week ago

Selected Answer: B

absolutely B.

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/fdm/fptd-fdm-config-guide-660/fptd-fdm-ha.html#concept_8C628FB71F0444A6BAC6D33FD72FB2EE#:~:text=you%20cannot%20specify%20an%20interface%20that%20is%20currently%20configured

upvoted 3 times

Tonymopar 8 months, 2 weeks ago

I've actually had this happen while setting HA pairing. B is 100%

upvoted 4 times

tanri04 9 months, 3 weeks ago

No, the correct answer is B.

The interface name must be removed from the interface on each Cisco FTD when configuring an active/passive HA pair. This is because when configuring failover, a dedicated interface is used for the failover link, and the interface name cannot be used for this purpose. Therefore, the interface name must be removed to allow the failover link to be configured properly.

upvoted 3 times

Mevijil 10 months, 4 weeks ago

Selected Answer: B

Definitely B - can't use a named interface for the Failover Link or Stateful Failover Link

upvoted 2 times

Seawanderer 11 months ago

Selected Answer: B

It's B

upvoted 2 times

Question #151 *Topic 1*

An engineer must configure the firewall to monitor traffic within a single subnet without increasing the hop count of that traffic. How would the engineer achieve this?

A. Configure Cisco Firepower as a transparent firewall.

B. Set up Cisco Firepower as managed by Cisco FDM.

C. Configure Cisco Firepower in FXOS monitor only mode.

D. Set up Cisco Firepower in intrusion prevention mode.

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #152 *Topic 1*

Which firewall design will allow it to forward traffic at layers 2 and 3 for the same subnet?

A. routed mode

B. Cisco Firepower Threat Defense mode

C. transparent mode

D. integrated routing and bridging

Suggested Answer: *D*

Community vote distribution

D (45%) C (36%) Other

d0980cc 3 months, 3 weeks ago

Selected Answer: A

The design would be to setup the FTD in Routed Mode, create a bridge group and assign an IP address to the BVI (IRB).

So the "design" would incorporate both A and D.

upvoted 1 times

Silexis 4 months, 4 weeks ago

Selected Answer: A

Firewall Designs are 2 in case of FTD:

Routed and Transparent.

Routed mode acts like a Layer 3 hop in the path BUT it can also act as a layer 2 device, functioning like a L2 switch through Bridge Groups, eliminating the need for an external switch (for example 3 pc's connected to 3 firewall ports and having configured the L3 gateway the same firewall).

This is why, I think that the correct answer is actually A

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/transparent_or_routed_firewall_mode_for_firepower_threat_defense.html#id_37129

upvoted 1 times

achille5 8 months, 1 week ago

Selected Answer: D

L2=mac addressing, L3=ip routing, IRB feature can forward both.

upvoted 3 times

z6st2a1jv 1 year, 2 months ago

Selected Answer: B

transparent firewall does not route L3 traffic even with rbi. Routed firewall with bvi works on L2 and L3.

upvoted 2 times

z6st2a1jv 1 year, 2 months ago

sorry, I meant to answer A

upvoted 1 times

pr0fectus 1 year, 2 months ago

Selected Answer: D

Try looking up Firepower IRB configuration in youtube. There's tons of examples there where such use case has been tackled. So I'd go for D.

upvoted 1 times

c946f3e 1 year, 3 months ago

What is IRB in FTD?

IRB stands for Integrated Routing and Bridging and is a feature that enables bridging between two or more VLANs and routing between these VLANs as well. Therefore, the feature supported by IRB on Cisco FTD devices is D

upvoted 1 times

THEODORABLE 1 year, 7 months ago

I am thinking D, IRB. They are asking which will allow the device to forward traffic at layer 2 or layer 3 for the same subnet not specifically within the same subnet. Forwarding traffic within the subnet at layer 2 and when it needs to leave the subnet it can forward at layer 3 to another IP destinations. I think the term “design” is being used incorrectly in the question—darn ESL question writers!

upvoted 1 times

⊟ **Cokamaniako** 1 year, 7 months ago

Selected Answer: C

Firewall design is not IRB, IRB is technology to route/switch traffic. Firewall design is either transparent and routed and in this case the correct answer is Transparent

upvoted 2 times

⊟ **Kris92** 10 months ago

Agree, but transparent and routed are firewall modes, haven't seen them called designs anywhere in documentation.

upvoted 1 times

⊟ **minik** 1 year, 8 months ago

Selected Answer: C

Firewall design is routed vs transparent. The question is about forwarding in L2 and L3 for the same subnet (not forwarding in L2 and routing in L3) - so the correct answer is Transparent. Thank you :)

upvoted 2 times

⊟ **Initial14** 1 year, 8 months ago

Selected Answer: A

Firewall design is not IRB, IRB is technology to route/switch traffic. Firewall design is either transparent and routed and in this case the correct answer is Routed

upvoted 1 times

⊟ **Initial14** 1 year, 8 months ago

In routed mode you can have BVI and multiple interfaces are in that BVI. BVI the uses technology IRB to switch (l2) or route (l3) traffic.

upvoted 2 times

⊟ **Initial14** 1 year, 9 months ago

Selected Answer: D

D is the right Answer. With IRB (BVI) you can switch traffic within LAN and also use BVI as Gateway.

upvoted 1 times

⊟ **Initial14** 1 year, 8 months ago

WRONG :)

upvoted 2 times

⊟ **Joe_Blue** 1 year, 9 months ago

Selected Answer: D

IRB provides Layer 2 bridging service between hosts that are within a Layer 2 domain. Also, it provides routing service for hosts that are in different subnets within a Layer 3 VPN.

https://content.cisco.com/chapter.sjs?uri=/searchable/chapter/content/en/us/td/docs/iosxr/cisco8000/l2vpn/73x/b-l2vpn-cg-cisco8000-73x/m-configure-irb.html.xml

upvoted 1 times

Question #153 *Topic 1*

An organization is configuring a new Cisco Firepower High Availability deployment. Which action must be taken to ensure that failover is as seamless as possible to end users?

A. Set the same FQDN for both chassis.

B. Set up a virtual failover MAC address between chassis.

C. Load the same software version on both chassis.

D. Use a dedicated stateful link between chassis.

Suggested Answer: *D*

Community vote distribution

D (56%) B (44%)

⊟ **Initial14** Highly Voted 👍 1 year, 9 months ago

Selected Answer: B

Only B

upvoted 5 times

⊟ **d0980cc** 3 months, 3 weeks ago

General Prerequisites for Firepower High Availability

1.Two Identical Units

For FMC HA, you need two FMCs (either hardware or virtual) with identical specifications and licensing capacity.

2.The units must run the same software version (e.g., FTD 7.1 or FMC 7.0).

Same Software Version: Both units must be on the same software version to ensure compatibility and proper synchronization.

3. Each unit requires its own Smart License entitlement. For FTD, this means two Base licenses plus any additional feature licenses (e.g., Threat, Malware

4. A dedicated high-speed link for HA communication (failover link) is required between the two units.

5. No Pending Changes: Both units must be fully deployed from the FMC with no uncommitted configuration changes before establishing HA.

Only B

upvoted 1 times

⊟ **d0980cc** 3 months, 3 weeks ago

Oops. I meant C

upvoted 1 times

⊟ **d0980cc** 2 months, 2 weeks ago

Omit previous comment. Answer is B

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense-virtual/222235-configure-virtual-mac-addresses-for-ftd.html#:~:text=Virtual%20MAC%20addresses%20allow%20the%20primary%20and%20secondary%20FTD%20to%20maintain%C2%A0consistent%2

upvoted 1 times

⊟ **Last00i** Most Recent 🕘 3 weeks ago

Selected Answer: B

to make sure a failover is as seamless as possible you have a failover link already, so the better option it has to be B with virtual mac address

upvoted 1 times

⊟ **Silexis** 4 months, 4 weeks ago

Selected Answer: B

While dedicated failover state link can be benefic if there is a lot of traffic handled by the FTD, the lack of a Virtual MAC address can create disruptions on a failover event.

"Configuring virtual MAC addresses on an FTD HA pair is beneficial to the availability of a network. Virtual MAC addresses allow the primary and secondary FTD to maintain consistent MAC addresses which prevents certain traffic disruptions."

https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense-virtual/222235-configure-virtual-mac-addresses-for-ftd.html

This is why, I will go on B

upvoted 1 times

⊟ **MB2222** 8 months, 1 week ago

It is most likely answer (D). The questions relates/emphasizes to "failover is as seamless as possible to end users", which is done via stateful links to sync the TCP session state/connection table among both firewalls.

upvoted 1 times

Silexis 4 months, 4 weeks ago

States are propagated via FOVER link in the absence of a dedicated link. A better design is to separate the datapath from the state path but while you have state without a dedicated link, you won't have MAC consistency without a Virtual MAC configured

upvoted 1 times

achille5 8 months, 2 weeks ago

Selected Answer: D

Stateful link

upvoted 3 times

gwb 9 months, 2 weeks ago

stateful link. answer D.

upvoted 2 times

pr0fectus 1 year, 2 months ago

Selected Answer: B

Answer is B.

upvoted 3 times

aalnman 1 year, 4 months ago

Selected Answer: D

To ensure that failover is as seamless as possible to end users when configuring a new Cisco Firepower High Availability deployment, the organization must D. Use a dedicated stateful link between chassis. Configuring high availability, also called failover, requires two identical Firepower Threat Defense devices connected to each other through a dedicated failover link and, optionally, a state link1. The system uses the state link to pass connection state information to the standby device, so that if a failover occurs, user connections are preserved2. Is there anything else you would like to know?

upvoted 4 times

Initial14 1 year, 9 months ago

The right answer is B. Why not D ? Because the question states "dedicated" state link. You do not need dedicated state link, you can use failover link for that, but the vMAC will help tp transition from Active FW to Passive, because MAC will stay the same, in the case where you hawe 2 mac's, the switch would have to flap, and FMC does not do graceful ARP. This is documented in Whitepaper

upvoted 3 times

gwb 9 months ago

yeah I got your point, Q did not state that there is any failover / stateful link. I assume that there is only failover link between Active/Passive at this moment, and ask what feature we need to have additionally for seamless failover. Thus stateful link (it can be used same failover link), my choice is D.

upvoted 1 times

tanri04 1 year, 9 months ago

D. Use a dedicated stateful link between chassis.

Using a dedicated stateful link between chassis ensures that the failover is as seamless as possible to end users. A dedicated stateful link allows the two Firepower chassis to synchronize connection state information in real-time, which ensures that network traffic is not interrupted during a failover event. In contrast, a virtual failover MAC address, loading the same software version, and setting the same FQDN are important for ensuring a successful failover, but they do not directly impact end-user experience.

upvoted 1 times

Mevijil 1 year, 10 months ago

Selected Answer: D

D is correct - setting up a Stateful Failover Link in addition to the Failover Link preserves the state information for existing sessions.

upvoted 3 times

Question #154 *Topic 1*

A company is in the process of deploying intrusion prevention with Cisco FTDs managed by a Cisco FMC. An engineer must configure policies to detect potential intrusions but not block the suspicious traffic. Which action accomplishes this task?

A. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

B. Configure IPS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

C. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by checking the “Drop when inline” option.

D. Configure IDS mode when creating or editing a policy rule under the Cisco FMC Intrusion tab in Access Policies section by unchecking the “Drop when inline” option.

Suggested Answer: *B*

Community vote distribution

B (67%) D (33%)

TECH3K3 1 month ago

Selected Answer: B

I use the FMC/FTD everyday at work, and there is no IDS mode, only IPS mode, with an option to uncheck "Drop When inline"

upvoted 1 times

whysohardwhy 4 months, 2 weeks ago

Selected Answer: D

Another messed up wording.

With all these fancy names let's FTD is FTD, no such a button in the menu says "Oh I'm an IPS!" or "OH Now I'm a bloody IDS!"

You make it an IDS by unchecking "drop when inline", so D.

upvoted 1 times

Silexis 4 months, 4 weeks ago

Selected Answer: B

First of all, it won't make any sense to do anything "when inline" when it comes to an IDP, because an IDS is not inline.

The B answer is that if option "Drop when inline" is Disabled, SNORT rules are evaluated for that flow and it will mark the result, without impacting traffic, as it would have taken the action on it.

https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/214609-firepower-data-path-troubleshooting-phas.html

This is why I am sticking with B

upvoted 1 times

tinyJoe 6 months, 1 week ago

Selected Answer: D

I think it is D because of the statement in the question “not block the suspicious traffic”.

upvoted 2 times

Stevens0103 10 months, 2 weeks ago

Let me rephrase each option:

A. checking the “Drop when inline” option configures the system in IPS mode

B. unchecking the “Drop when inline” option configures the system in IPS mode

C. checking the “Drop when inline” option configures the system in IDS mode

D. unchecking the “Drop when inline” option configures the system in IDS mode

upvoted 1 times

Stevens0103 10 months, 2 weeks ago

option A itself is correct but does not meet the question's requirement.

option B is wrong.

option C is wrong.

option D is correct and meets the question's requirement.

upvoted 2 times

z6st2a1jv 1 year, 1 month ago

Selected Answer: D

Curse Cisco and their semantic pitfalls.

I think you start with a neutral inspection policy. Then, the keyword is "by": By unchecking "drop when inline" in the inspection policy, you create an IDS policy, instead of an IPS policy.

So I choose D

But that could be wrong, depending on how Cisco want to interpret things...

upvoted 4 times

bassfunk 1 year, 4 months ago

Selected Answer: B

The official name of the policy is IPS. You then uncheck "drop when inline" to make it function as IDS.

upvoted 4 times

Dreng65 1 year, 5 months ago

Selected Answer: B

i think B is correct, since the cisco terminology, there's not IDS deployment, only IPS deployment for FTD.

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/getting_started_with_intrusion_policies.html?bookSearch=true#concept_D1F1CDE29BDE4ACF9F254D8E5F1D518D

Also the option of drop does exist too, have to be unchecked:

https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/getting_started_with_intrusion_policies.html?bookSearch=true#ID-2231-0000003d

upvoted 2 times

trudint 1 year, 6 months ago

IDS = Intrusion Detection System

IPS = Intrusion Prevention System

Doesn't this ^ pretty much say it all? One detects and one prevents. This is a classic example of a Cisco trip-you-up question. Its purpose is not to test whether or not you know and understand a concept. No...it's purpose is to present you with designed, indecipherable ambiguity in an effort to collect another $300.

upvoted 2 times

THEODORABLE 1 year, 7 months ago

Welcome to Cisco Trivia Game where each Game cost $300! I think its D because we are creating an IDS behaving policy by deselecting drop when inline option on the policy. Semantics are making Cisco too much money. I don't know if its technically called IDS or still IPS mode when you disable the drop when selected checkbox? I cannot find a definitive documentation that calls it out.

upvoted 4 times

Bbb78 1 year, 7 months ago

I would go for the IDS > unchecking...but then I saw the question ...it is definatley IPS > unchecking ....Cisco questions - you have to love them ...then they wonder why we are going to examtopics :)

upvoted 2 times

Question #155 Topic 1

An engineer is using the configure manager add Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?

A. DONOTRESOLVE must be added to the command

B. The IP address used should be that of the Cisco FTD, not the Cisco FMC

C. The registration key is missing from the command

D. The NAT ID is required since the Cisco FMC is behind a NAT device

Suggested Answer: *D*

Community vote distribution

C (67%) A (33%)

bf3b9bc 3 months, 3 weeks ago

Selected Answer: D

The NAT ID is required since the Cisco FMC is behind a NAT device
command line in FTD :configure manager add <FMC ip> <key> <NAT-ID>,NAT-ID is optional.

upvoted 1 times

artgen 10 months, 2 weeks ago

"If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.

If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example:

Example:
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured. "
Reference: https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/device_management_basics.html

So, according to this phrase from the cisco material, answer C seems to make more sense due to the fact that if DONTRESOLVE is missing then a NAT_ID is for sure required as well, so both of them are missing. Since we have only one option, it is more likely that the reg_key is missing, in my opinion.

upvoted 2 times

LangaMos 11 months, 2 weeks ago

Whwre did the question state that its behind the NAT device? I go with Missing Registration key

upvoted 1 times

KyPKyP 11 months, 2 weeks ago

The question is wrong , it should be "An engineer is using the configure manager add <FMC IP> Cisc404225383 command to add a new Cisco FTD device to the Cisco FMC; however, the device is not being added. Why is this occurring?"
Than "D " makes sense.

upvoted 1 times

Lula_pearl 1 year, 1 month ago

C is the correct answer. When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address] [registration key]'

upvoted 2 times

THEODORABLE 1 year, 1 month ago

I pick C. How do you know Cisc404225383 is not the hostname? the question only shows 1 item listed after the manager add base command. if that is the Nat_ID then we are missing the IP or DONTRESOLVE & reg key.

upvoted 3 times

ureis 1 year, 1 month ago

Step 5 Configure the new FMC.
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id]

{hostname | IPv4_address | IPv6_address}—Sets the FMC hostname, IPv4 address, or IPv6 address.

DONTRESOLVE — If the FMC is not directly addressable, use DONTRESOLVE instead of a hostname or IP address. If you use DONTRESOLVE , then a nat_id is required. When you add this device to the FMC, make sure that you specify both the device IP address and the nat_id ; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.

https://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61/device_management_basics.html

upvoted 1 times

Joe_Blue 1 year, 3 months ago

Selected Answer: C

configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE } regkey [nat_id]

upvoted 3 times

tinyJoe 6 months, 1 week ago

I completely agree, reg_key is required but nat_id is not.
If Cisc404225383 is the host name, then all that is missing is the reg_key.
If Cisc404225383 is the reg_key, then the hostname or IP is missing to begin with, but that is not an option.

upvoted 1 times

DID123 1 year, 4 months ago

Selected Answer: A

wrong answer, apparently the registration key and NAT ID is present and what's missing is either the FMC IP address or the DONOTRESOLVE key word before registration key, so that the FTD will actually register to any FMC provides this registration key and NAT ID regardless to the FMC IP

upvoted 1 times

Dolby58 1 year, 4 months ago

Selected Answer: C

You have to type in the registration key

upvoted 1 times

Question #156 *Topic 1*

An engineer is configuring Cisco FMC and wants to allow multiple physical interfaces to be part of the same VLAN. The managed devices must be able to perform Layer 2 switching between interfaces, including sub-interfaces. What must be configured to meet these requirements?

A. inter-chassis clustering VLAN

B. Cisco ISE Security Group Tag

C. interface-based VLAN switching

D. integrated routing and bridging

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #157 *Topic 1*

An organization does not want to use the default Cisco Firepower block page when blocking HTTP traffic. The organization wants to include information about its policies and procedures to help educate the users whenever a block occurs. Which two steps must be taken to meet these requirements? (Choose two.)

A. Edit the HTTP request handling in the access control policy to customized block

B. Modify the system-provided block page result using Python

C. Create HTML code with the information for the policies and procedures

D. Change the HTTP response in the access control policy to custom

E. Write CSS code with the information for the policies and procedures

Suggested Answer: *CD*

Community vote distribution

CD (100%)

[Removed] 9 months, 4 weeks ago

Selected Answer: CD

C and D

upvoted 2 times

kakabk 11 months, 4 weeks ago

Selected Answer: CD

https://community.cisco.com/t5/network-security/access-control-policy-block-response-page/td-p/2570606

upvoted 3 times

THEODORABLE 1 year, 1 month ago

https://www.wiresandwi.fi/blog/firepower-url-blocking-page-setup-and-management#:~:text=Configuring%20Block%20and%20Interactive%20Page&text=Log%20into%20your%20FMC%20and,the%20policy%20of%20your%20choic

upvoted 1 times

THEODORABLE 1 year, 1 month ago

C&D-- You change the response page to custom (for both types) and then you choose the edit pencil to upload your "HTML CODE"

upvoted 1 times