Question #1 *Topic 1*

Refer to the exhibit.

How does FortiGate handle the traffic with the source IP 10.0.1.130 and the destination IP 128.66.0.125?

FortiGate router policy and diagnose output

```
branch1_fgt # show router policy
config router policy
    edit 1
        set src "10.0.1.128/255.255.255.128"
        set dst "128.66.0.0/255.255.255.0"
        set action deny
    next
end

branch1_fgt # diagnose sys sdwan service4

Service(1): Address Mode(IPV4) flags=0x4200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(priority),
  link-cost-factor(latency), link-cost-threshold(10), heath-check(Corp_HC)
  Members(2):
    1: Seq_num(2 port2 underlay), alive, latency: 0.769, selected
    2: Seq_num(1 port1 underlay), alive, latency: 71.022, selected
  Application Control(3): Microsoft.Portal(41469,0) Salesforce(16920,0) Collaboration(0,28
  Src address(1):
        10.0.1.0-10.0.1.255

Service(4): Address Mode(IPV4) flags=0x24200 use-shortcut-sla use-shortcut
 Tie break: cfg
 Shortcut priority: 2
  Gen(1), TOS(0x0/0x0), Protocol(0): src(1->65535):dst(1->65535), Mode(sla hash-mode=round-rob)
  Members(2):
    1: Seq_num(1 port1 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
    2: Seq_num(2 port2 underlay), alive, sla(0x1), gid(2), num of pass(1), selected
  Src address(1):
        10.0.1.0-10.0.1.255
  Dst address(1):
   128.66.0.0-128.66.255.255
```

A. FortiGate steers the traffic flow through port2.

B. FortiGate routes the traffic flow according to the FIB.

C. FortiGate load balances the traffic flow through port1 and port2.

D. FortiGate drops the traffic flow.

Suggested Answer: *D*

Community vote distribution

D (57%) B (43%)

gowtham Most Recent 1 month, 1 week ago

Selected Answer: D

page 184 of the SD-WAN 7.6 Core Administrator Study Guide, route lookup flowchart, which states that FortiGate first checks regular (user-defined) policy routes, then ISDB routes, then SD-WAN rules, and finally the FIB if nothing else matches.

upvoted 1 times

darkstar15 2 months, 3 weeks ago

Selected Answer: D

FortiOS' order of preference regarding routing lookup is as follows: PBR -> SD-WAN rule -> FIB.

upvoted 1 times

Jordancueay 2 months, 4 weeks ago

Selected Answer: B

Fortigate will use the routing table or FIB to forward the traffic since the policy route action was deny

upvoted 3 times

BBLong 3 months, 1 week ago

Selected Answer: D

On FortiGate, policy routes take precedence over sd-wan rules. So, as traffic matches the policy route, it will be dropped.

upvoted 2 times

Question #2 *Topic 1*

Which statement is true about scheduling a FortiClient upgrade using an endpoint upgrade rule?

A. When scheduled, the installation always starts immediately if the endpoint is online.

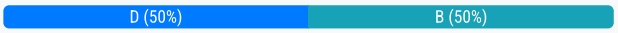
B. An endpoint upgrade rule can be assigned to a user group.

C. Scheduled upgrades automatically reboot macOS endpoints after installation.

D. If the scheduled time is already past in the local time zone of the endpoint, installation starts the next day at that time.

Suggested Answer: *B*

Community vote distribution



gowtham Most Recent 1 month ago

Selected Answer: D

Fortisase Deployment Guide stats "FortiSASE cannot apply an endpoint upgrade rule to a user group or user object" Only works on Endpoint Groups So D is correct

upvoted 1 times

Powers22 1 month, 2 weeks ago

Selected Answer: D

Although the study guide uses the wording 'user group', fortinet documentation confirms that the scoping is device based. So you cannot scope a upgrade job to user group, only device groups. D is correct as per KB "https://docs.fortinet.com/document/fortisase/7.4.0/administration-guide/132053/endpoint-upgrade"

upvoted 2 times

BBLong 3 months, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

simo94 5 months, 3 weeks ago

Selected Answer: B

page 125 of FortiSASE study guide. "only endpoints assigned to groups will be upgraded."

upvoted 2 times

Question #3 *Topic 1*

Which three factors about SLA targets and SD-WAN rules should you consider when configuring SD-WAN rules? (Choose three.)

A. When configuring an SD-WAN rule, you can select multiple SLA targets from different performance SLAs.

B. SLA targets are used only by SD-WAN rules that are configured with a Lowest Cost (SLA) strategy.

C. Member metrics are measured only if a rule uses the SLA target.

D. SD-WAN rules can use SLA targets to check whether the preferred members meet the SLA requirements.

E. When configuring an SD-WAN rule, you can select multiple SLA targets if they are from the same performance SLA.

Suggested Answer: *A, B, D*

Community vote distribution

gowtham Most Recent 1 month, 1 week ago

Selected Answer: ABD

C — False. Member metrics (latency, jitter, packet loss) are continuously measured as part of the performance SLA health-check configuration E — False. This is the inverse of the true rule:

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: ABD

ABD are correct answers.

upvoted 1 times

glbngl91 7 months, 2 weeks ago

Selected Answer: ABD

C) is not correct, member metrics are evaluated by perfomance SLA even if no SLA target is defined; instead, B) is correct, as SLA targets are only used when choosing Lowest Cost (SLA) strategy

upvoted 4 times

Question #4 *Topic 1*

Which authentication method overrides any other previously configured user authentication on FortiSASE?

A. RADIUS

B. MFA

C. Local

D. SSO

Suggested Answer: *D*

Community vote distribution

D (100%)

gowtham Most Recent 1 month, 1 week ago

Selected Answer: D

Enabling SSO Auth overrides any other Previusly created auth methods

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: D

D is correct. page 54 of SASE Core Administrator study guide.

upvoted 2 times

Question #5 *Topic 1*

Which two configurations are required for Agentless ZTNA to work? (Choose two.)

A. Proxy user single sign-on (SSO)

B. FortiClient Agent

C. FortiGate with ZTNA proxy

D. SD-WAN Private Access SPA

Suggested Answer: *A, C*

Community vote distribution

AC (100%)

gowtham Most Recent 1 month, 1 week ago

Selected Answer: AC

B- Incorrect by definition D-Broader SDWAN use case of SPA

upvoted 1 times

darkstar15 2 months, 3 weeks ago

Selected Answer: AC

B is incorrect because it is agentless. D is incorrect because SPA is a use case concept.

upvoted 1 times

Question #6 *Topic 1*

What is the purpose of the priority/failover connection feature in FortiSASE Geofencing for managing VPN connections?

A. It forces all remote users to connect only to the nearest security POP regardless of location.

B. It allows administrators to define rules to prioritize on-premises FortiGate connections for users in specific countries, with failover to a security POP if the FortiGate device is unavailable.

C. It restricts VPN access to users based on their geolocation without allowing failover options.

D. It automatically balances VPN traffic across all available security POPs without prioritizing on-premises devices.

Suggested Answer: *B*

Community vote distribution

B (100%)

BBLong Most Recent 3 months, 1 week ago

Selected Answer: B

B is correct.

Under Endpoint management -> Endpoint Profile -> Profile (select the one associated with the users) -> Advanced setting -> Failover sequence (default disabled).

upvoted 2 times

Question #7 *Topic 1*

What is the primary purpose of implementing a dedicated IP in security POPs?

A. To provide a unique identifier for logging and monitoring user activities across multiple networks

B. To ensure consistent and reliable access for specific users or devices

C. To implement geolocation rules and source IP address anchoring

D. To improve website performance by reducing load times

Suggested Answer: *C*

Community vote distribution

C (100%)

darkstar15 Most Recent 2 months, 2 weeks ago

Selected Answer: C

Source IP address anchoring. Typically, combined with geolocation rules. Administration Guide in Dedicated public IP addresses

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: C

C is correct. It helps with white listing traffic on legacy infrastructure or on SaaS applications based on the dedicated IP in PoP.

upvoted 2 times

Question #8 *Topic 1*

Refer to the exhibit.

Which two statements about the Vulnerability summary dashboard in FortiSASE are correct? (Choose two.)

A. Vulnerability scan is disabled in the endpoint profile.

B. The dashboard shows the vulnerability score for unknown applications.

C. Automatic vulnerability patching can be enabled for supported applications.

D. The dashboard allows the administrator to drill down and view CVE data and severity classifications.

Suggested Answer: *C, D*

Community vote distribution

CD (100%)

darkstar15 Most Recent 2 months, 2 weeks ago

Selected Answer: CD

Aministration Guide FortiSASE in Drilling down on vulnerabilities.

upvoted 1 times

Question #9 *Topic 1*

What is the primary function of FortiView on FortiSASE?

A. Presents raw log data in graphical format only, without sorting criteria or aggregated views.

B. Generates real-time alerts for security events and presents them in a single text-based console without metadata.

C. Displays individual logs on the GUI without aggregation, allowing administrators to sort events by time only.

D. Provides consolidated consoles to analyze security events over time using graphical or text-based log views.

Suggested Answer: *D*

Community vote distribution

D (100%)

BBLong Most Recent 3 months, 1 week ago

Selected Answer: D

D is correct. Page 120 of SASE Core Administrator 7.6.

upvoted 2 times

Question #10 *Topic 1*

Which two statements about configuring a steering bypass destination in FortiSASE are correct? (Choose two.)

A. You can select from four destination types: Infrastructure, FQDN, Local Application, or Subnet.

B. Apply condition allows split tunneling destinations to be applied to On-net, Off-net, or both types of endpoints.

C. Subnet is the only destination type that supports the Apply condition.

D. Apply condition can be set only to On-net or Off-net, but not both.

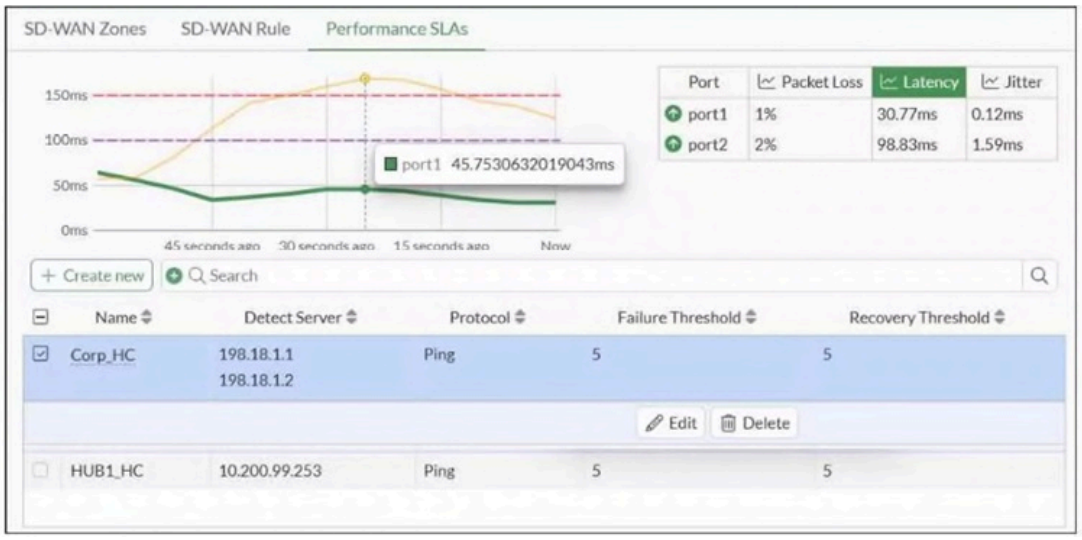
Suggested Answer: *A, B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

Refer to the exhibit.

Which conclusion can you draw from the exhibit?



A. The administrator configured the packet loss threshold for Corp_HC and HUB1_HC to 5%.

B. The administrator configured the Corp_HC performance service-level agreement (SLA) with SLA targets for the three criteria: packet loss, latency, and jitter.

C. Over the past 60 seconds, the member port2 latency was temporarily above the latency criteria defined for HUB1_HC.

D. Over the past 60 seconds, the member port1 was monitored healthy for both latency criteria of the Corp_HC definition.

Suggested Answer: *D*

Community vote distribution

D (100%)

gowtham Most Recent 1 month, 1 week ago

Selected Answer: D

A incorrect - 5 values shown is not 5%packet loss its defined as number of failed/successful probes B- Incorrect Not supported. The visible configuration table only shows Detect Server, Protocol, Failure Threshold, and Recovery Threshold C — Incorrect. The graph belongs to Corp_HC

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: D

D is correct.

upvoted 1 times

Question #12 *Topic 1*

Which statement about FortiSASE CASB capabilities is true?

A. FortiSASE provides both API-based CASB and inline CASB.

B. FortiSASE provides only API-based CASB.

C. FortiSASE provides only inline CASB.

D. FortiSASE provides CASB capabilities only through Security Fabric integration.

Suggested Answer: *A*

Community vote distribution

A (100%)

ee0808 Most Recent 6 months, 3 weeks ago

Selected Answer: A

A is right. Study guide page 74. API based CASB = Out of band CASB

upvoted 4 times

Question #13 *Topic 1*

Which three challenges in a work-from-anywhere environment does FortiSASE address? (Choose three.)

A. Lack of visibility and control

B. Poor performance

C. Inconsistent security levels

D. Lack of bandwidth

E. Remote internet connectivity

Suggested Answer: *A, B, C*

Community vote distribution

ABC (100%)

Powers22 Most Recent 1 month, 3 weeks ago

Selected Answer: ABC

Study guide page 8. Performance challenges are addressed by providing global POPs and traffic steering/bypass at the client

upvoted 2 times

Question #14 *Topic 1*

Which two methods are available for provisioning FortiClient on endpoints using FortiSASE? (Choose two.)

A. FortiClient can be provisioned only by distributing installers to end users through the FortiSASE portal without an invitation code.

B. FortiClient can be provisioned by distributing the installer to end users for manual installation.

C. FortiClient can be provisioned using installers with an invitation code from the FortiSASE portal, SCCM or GPO, or mobile device management (MDM) software.

D. FortiClient provisioning is limited to using mobile device management MDM software or manual installation without requiring an invitation code.

E. FortiClient can be provisioned using SCCM or GPO, but only through an external portal, not the FortiSASE portal.

Suggested Answer: *B, C*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

Which three reports are valid report types in FortiSASE? (Choose three.)

A. Shadow IT Report

B. Endpoint Compliance Deviation Report

C. Cyber Threat Assessment

D. Vulnerability Assessment Report

E. Web Usage Summary Report

Suggested Answer: *A, C, E*

Community vote distribution

ACE (100%)

darkstar15 Most Recent 2 months, 2 weeks ago

Selected Answer: ACE

That's correct, it's in the FortiSASE 25.3.217 Mature Administration Guide (Report types) and I also validated it in the console directly in the reports section.

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: ACE

ACE is correct.

You can find "Shadow IT report" and "Web Usage Summary Report" on pages 73 and 131 of the FortiSASE Core Administrator 7.6 Study Guide. But the other options are not clear. In FortiView you can see clients vulnerability status. Also, on page 123 Endpoint Management is explained, where you can see endpoint status. But neither clearly say anything about any reports.

If you have access to a FortiSASE dashboard however, you can see that "shadow IT Report", "Cyber Threat Assessment", and "Web Usage Summary Report" are all in the list of readily available reports that can be enabled and used. You can see them under Operations>Reports>Scheduled Reports.

upvoted 2 times

Drigga 5 months ago

Selected Answer: ACE

Pg 483 FortiSASE 25.3.212 Mature Administration Guide

upvoted 2 times

Question #16 *Topic 1*

FortiSASE allows forwarding logs to an external server.
Which two external server types are supported? (Choose two.)

A. FortiAnalyzer

B. SNMP

C. Syslog

D. API

Suggested Answer: *A, C*

Community vote distribution

AC (100%)

darkstar15 Most Recent 2 months, 2 weeks ago

Selected Answer: AC

Fortisase 26 core admin guide pg 130

upvoted 1 times

Question #17 *Topic 1*

Which statement is true about FortiSASE supported deployment?

A. FortiSASE relies on ZTNA-only mode, which replaces SWG and endpoint functions.

B. FortiSASE supports both Endpoint mode and SWG mode, depending on deployment.

C. FortiSASE supports VPN mode and Agentless mode, based on user requirements.

D. FortiSASE operates only in SWG mode, where all traffic is forced through FortiSASE POPs.

Suggested Answer: *B*

Community vote distribution

B (100%)

Powers22 Most Recent 1 month, 3 weeks ago

Selected Answer: B

I beleive this is B but appears Fortinet are dropping these terms in favour or just agent and agentless based access to SWG. Endpoint mode now commonly refered to as agent based and SWG mode commonly refered to as Agentless Mode

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: B

B is correct.

Endpoint Mode: Using Forticlient; agent-based. SWG: Secure Web Gateway; agentless (proxy)

upvoted 2 times

Question #18 *Topic 1*

What are three key routing principles of SD-WAN? (Choose three.)

A. SD-WAN members are skipped if they do not have a valid route to the destination.

B. Directly connected routes have precedence over SD-WAN rules.

C. SD-WAN rules are skipped if the best route to the destination is a static route.

D. SD-WAN rules are skipped if the best route to the destination is not an SD-WAN member.

E. Policy routes have precedence over SD-WAN rules.

Suggested Answer: *A, D, E*

Currently there are no comments in this discussion, be the first to comment!

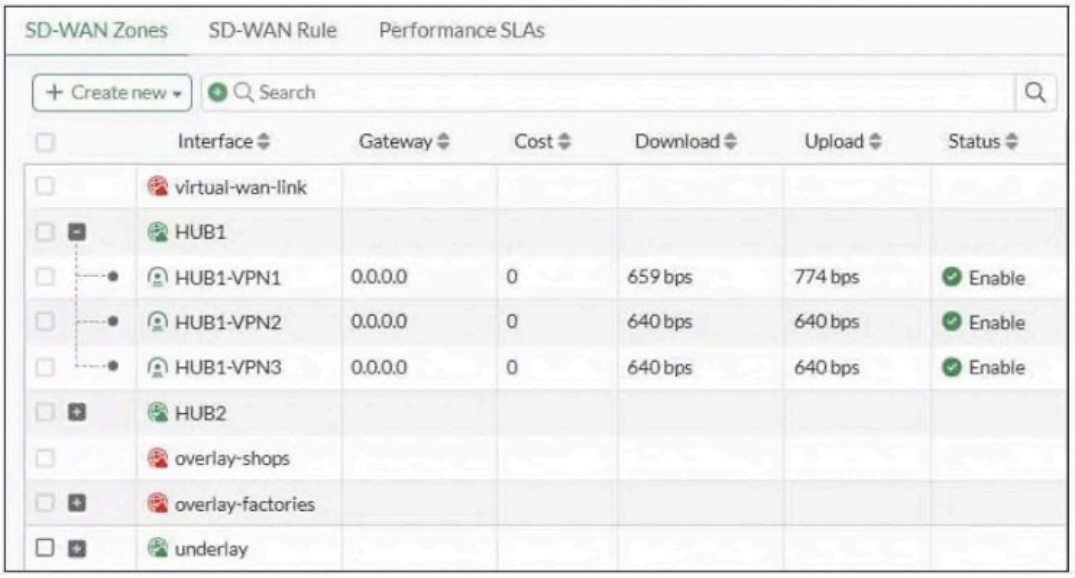
Question #19 *Topic 1*

Refer to the exhibit.

An SD-WAN zone configuration on the FortiGate GUI is shown.

What can you conclude about the zone and member configuration on this device?

SD-WAN zones



A. You can move HUB1-VPN3 from the HUB1 zone to the virtual-wan-link zone.

B. The overlay-factories zone contains no member.

C. You can delete the virtual-wan-link zones.

D. You can delete the overlay-factories zone.

Suggested Answer: *A*

Community vote distribution

A (100%)

gowtham Most Recent 1 month ago

Selected Answer: A

Page 60 of study Guide Note that once you have defined the name of a zone you cannot modify it. if you need make a change, you can simply create a new zone and move the members from one zone to the other"

upvoted 1 times

Powers22 1 month, 2 weeks ago

Selected Answer: A

It is certainly not B since there is a plus sign next to it indicating that there are sub members. You cant delete a zone that has memebers. You cannot delete the defaul zone (virtual-wan-link)

upvoted 1 times

Drigga 5 months ago

Selected Answer: A

You can assign members to different zones

upvoted 2 times

Question #20 *Topic 1*

An SD-WAN member is no longer used to steer SD-WAN traffic. You want to update the SD-WAN configuration and delete the unused member. Which action should you take first?

A. Move the SD-WAN member to the virtual-wan-link zone.

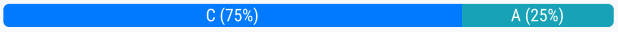
B. Disable the interface.

C. Remove the member from the performance service-level agreement (SLA) definitions.

D. Delete static route definitions for that interface.

Suggested Answer: *C*

Community vote distribution



gowtham Most Recent 1 month, 1 week ago

Selected Answer: C

you need to remove all references to it in the SD-WAN configuration

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: C

C is correct.

I was in doubt between C and D. But as the questions says the interface is not used to steer traffic, it makes sense to assume any associated static routes have also been removed.

upvoted 2 times

greeklover84 4 months, 1 week ago

Selected Answer: A

yes only A makes sense.

upvoted 1 times

BBLong 3 months, 1 week ago

you don't need to move it to the default sd-wan zone. You can remove it straight away.

upvoted 2 times

Question #21 *Topic 1*

What is a key use case for FortiSASE Secure Internet Access (SIA) in an agentless deployment?

A. It provides secure web browsing by isolating browser sessions and enforcing data loss prevention for temporary employees.

B. It acts as a secure web gateway (SWG) distributing a PAC file for explicit web proxy use, securing HTTP and HTTPS traffic with a full security stack, and is ideal for unmanaged endpoints like contractors.

C. It distributes a PAC file to secure non-web traffic protocols and applies antivirus protection only for managed endpoints.

D. It requires FortiClient endpoints and supports ZTNA tags to secure all network traffic for unmanaged endpoints.

Suggested Answer: *B*

Community vote distribution

B (100%)

greeklover84 Most Recent 4 months, 1 week ago

Selected Answer: B

yes B. confirmed.

upvoted 1 times

Question #22 *Topic 1*

SD-WAN interacts with many other FortiGate features. Some of them are required to allow SD-WAN to steer the traffic.
Which three configuration elements must you configure before FortiGate can steer traffic according to SD-WAN rules? (Choose three.)

A. Traffic shaping

B. Routing

C. Security profiles

D. Interfaces

E. Firewall policies

Suggested Answer: *B, D, E*

Community vote distribution

BDE (100%)

greeklover84 Most Recent 4 months, 1 week ago

Selected Answer: BDE

B,D,E are correct.

upvoted 2 times

Question #23 *Topic 1*

How does the FortiSASE security dashboard facilitate vulnerability management for FortiClient endpoints?

A. It automatically patches all vulnerabilities without user intervention and does not categorize vulnerabilities by severity.

B. It shows vulnerabilities only for applications and requires endpoint users to manually check for affected endpoints.

C. It displays only critical vulnerabilities, requires manual patching for all endpoints, and does not allow viewing of affected endpoints.

D. It provides a vulnerability summary, identifies affected endpoints, and supports automatic patching for eligible vulnerabilities.

Suggested Answer: *D*

Community vote distribution

greeklover84 Most Recent 4 months, 1 week ago

Selected Answer: D

Only D makes sense and I would go for D.

upvoted 2 times

Question #24 *Topic 1*

Which two statements correctly describe what happens when traffic matches the implicit SD-WAN rule? (Choose two.)

A. Traffic is load balanced using the algorithm set for the v4-ecmp-mode setting.

B. Traffic does not match any of the entries in the policy route table.

C. FortiGate flags the session with may_dirty and vwl_default.

D. The traffic is distributed, regardless of weight, through all available static routes.

E. The session information output displays no SD-WAN service id.

Suggested Answer: *B, E*

Community vote distribution

BE (100%)

darkstar15 Most Recent 2 months, 1 week ago

Selected Answer: BE

I'm only sure about option E, which is on page 202 of the SDWAN 7.6 core admin study guide.

upvoted 1 times

BBLong 3 months, 1 week ago

Selected Answer: BE

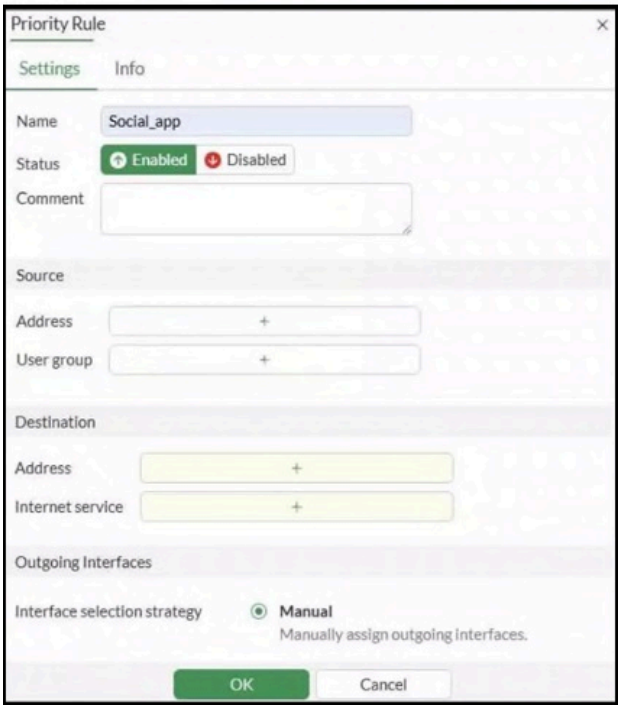
BE is correct. Policy-routes are preceded against sd-wan rules. So, if traffic has made it to the sd-wan rule table and the very last rule (implicit rule), it means that it has not matched any entries in policy route table. E is correct as well as when traffic matches the implicit sd-wan rule, in the logs no service-id is seen for the traffic logs.

upvoted 3 times

Question #25 *Topic 1*

Refer to the exhibit.
You configure SD-WAN on a standalone FortiGate device. You want to create an SD-WAN rule that steers traffic related to Facebook and LinkedIn through the less costly internet link.
What must you do to set Facebook and LinkedIn applications as destinations from the GUI?

SD-WAN rule



A. Enable the visibility of the applications field as destinations of the SD-WAN rule.

B. You cannot configure applications as destinations of an SD-WAN rule on a standalone FortiGate device.

C. Install a license to allow applications as destinations of SD-WAN rules.

D. In the Internet service field select Facebook and LinkedIn.

Suggested Answer: *D*

Community vote distribution

A (100%)

Powers22 Most Recent 1 month, 3 weeks ago

Selected Answer: A

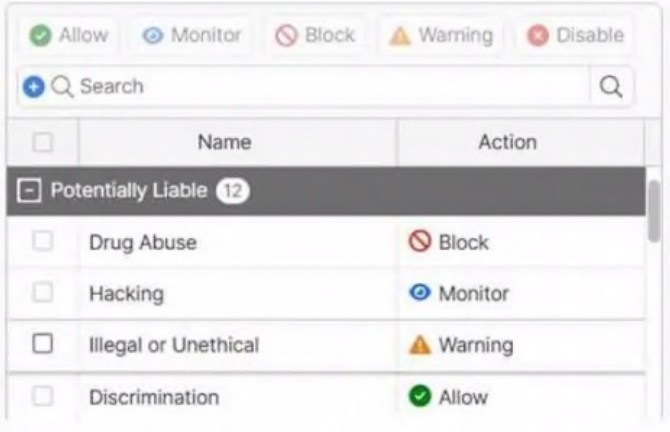
A or D will do the job. D leverages the ISDB (3-tuple IP, port and protocol) match against Fortinet maintained DB). This requires no layer-7 detection and less resource cycles. A leverages Application Aware steering where the IPS engine is used to inspect traffic and determine the application - see page 122 of the study guide. Since the questions asked what you need to do to set these in the GUI, im more inclined to answer with A.

upvoted 1 times

Question #26 *Topic 1*

Refer to the exhibit.

Which web filter category will be denied access and display a replacement message to the user?



A. Discrimination

B. Drug Abuse

C. Hacking

D. Illegal or Unethical

Suggested Answer: *B*

Community vote distribution

B (100%)

darkstar15 Most Recent 2 months, 1 week ago

Selected Answer: B

Block: Denies or blocks attempts to access any URL that belongs to the category. A replacement message displays. Fortisase Admin guide Restricting web usage using FortiGuard URL categories and URL filter

upvoted 1 times