



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

Refer to the exhibit, which shows the port1 interface configuration on FortiGate and partial session information for ICMP traffic.

```
config system interface
  edit "port1"
    set preserve-session-route enable
  next
end

# diagnose sys session list
session info: proto=1 proto_state=00 duration=4 expire=55 timeout=0 refresh_dir=both flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
state=log may_dirty npu f00 route_preserve
origin->sink: org pre->post, reply pre->post dev=7->19/19->7 gwy=100.64.1.1/10.0.1.101

# diagnose netlink interface list | grep index=19
if=port1 family=00 type=768 index=19 mtu=1420 link=0 master=0
```

What happens to the session information if a routing change occurs that affects this session?

- A. Only the interface and gateway information for dev=7 will be removed.
- B. The session information will not change unless the current route has been removed from the routing table.
- C. The session will be flagged as dirty but no route lookups will be performed.
- D. Sessions involving port7 or port19 will not have their routing information flushed.

Suggested Answer: B

Community vote distribution

B (100%)

 **d9eeb6d** 2 months ago

Selected Answer: B

Network Security Support Engineer 7.4 Study Guide p379

upvoted 2 times

 **IBB90704** 3 months ago

Selected Answer: B

FortiGate marks existing session routing information as persistent, and applies only the modified routes to new sessions.

The current route must still be present in the FIB

- Otherwise, FortiGate flags the session as dirty and reevaluates it

Pagina 380

upvoted 4 times

Refer to the exhibit, which shows the modified output of the routing kernel.

Routing information

```
# get router info routing-table database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       V - BGP VPNv4
       > - selected route, * - FIB route, p - stale info

Routing table for VRF=0
S    *> 0.0.0.0/0 [10/0] via 10.200.1.254, port1, [1/0]
S    0.0.0.0/0 [20/0] via 10.200.2.254, port2, [5/0]
S    8.8.8.8/32 [10/0] via 172.16.100.254, port8 inactive, [1/0]
O    10.0.1.0/24 [110/1] is directly connected, port3, 00:05:47, [1/0]
C    *> 10.0.1.0/24 is directly connected, port3
O    10.0.2.0/24 [110/1] is directly connected, port4, 00:05:47, [1/0]
C    *> 10.0.2.0/24 is directly connected, port4
B    *> 10.0.3.0/24 [200/10] via 10.0.1.200 {recursive is directly connected, port3}, 00:05:40, [1/0]
O    *> 10.0.4.0/24 [110/2] via 10.0.1.200, port3, 00:05:27, [1/0]
B    10.0.4.0/24 [200/10] via 10.0.1.200 {recursive is directly connected, port3}, 00:05:40, [1/0]
C    *> 10.200.1.0/24 is directly connected, port1
C    *> 10.200.2.0/24 is directly connected, port2
```

Which statement is true?

- A. The egress interface associated with static route 8.8.8.8/32 is administratively up.
- B. The default static route through 10.200.1.254 is not in the forwarding information base.
- C. The default static route through port2 is in the forwarding information base.
- D. The BGP route to 10.0.4.0/24 is not in the forwarding information base.

Suggested Answer: D

Community vote distribution

D (88%)

13%

IBB90704 Highly Voted 3 months ago

Selected Answer: D

The better routes show an asterisk beside the route source to indicate they are FIB entries, and therefore, are used for routing traffic.

Pagina 384

upvoted 5 times

rananaj Most Recent 1 month, 2 weeks ago

Selected Answer: C

Why D?

upvoted 1 times

Twefo 1 month, 2 weeks ago

C is not correct.

get router info routing-table database show all the routes, but the one that are chosen are premarked with a *

upvoted 2 times

d9eeb6d 2 months ago

Selected Answer: D

Network Security Support Engineer 7.4 Study Guide p384

* = in FIB

inactive = interface administratively down

upvoted 2 times

Refer to the exhibit.

The exhibit shows the output from using the command `diagnose debug application samld -1` to diagnose a SAML connection.

```
**** SP Login Dump ****<lasso:Login
xmlns:lasso="http://www.entrouvert.org/namespaces/lasso/0.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
LoginDumpVersion="2"><lasso:Request><samlp:AuthnRequest
ID="_EEC718A47FB37B472B205B11153ED409" Version="2.0" IssueInstant="2024-02-
21T00:58:44Z" Destination="https://10.1.10.2/saml-idp/nst/login/"
SignType="0" SignMethod="0" ForceAuthn="false" IsPassive="false"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AssertionConsumerServiceURL="https://10.1.10.254:1003/remote/saml/login/"><saml:Issuer>https://10.1.10.254:1003/remote/saml/metadata/</saml:Issuer><samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified" AllowCreate="true"/></samlp:AuthnRequest></lasso:Request><lasso:RemoteProviderID>http://10.1.10.2/samlidp/nst/metadata/</lasso:RemoteProviderID><lasso:MsgUrl>https://10.1.10.2/saml-idp/nst/login/?SAMLRequest=jZJfT8IwFMW%2FytL30W5sAZtBwhhEEtQF0AdfTN0u0GRr22%2Fnn29vGWiwUeJLk97eX%2B85p01Q1FXDJ63dqxW8tIDWe68rhw7GJHWKK4FSuRK1IDcFnw9uVnysMd4Y7TVha7IGXK2EIhgrNSKeItsRJ5ms%4</lasso:HttpRequestMethod><lasso:RequestID>_EEC718A47FB37B472B205B11153ED409</lasso:RequestID></lasso:Login>
```

Based on this output, what can you conclude?

- A. Active Directory is used for authentication.
- B. The authentication request is for an SSL VPN connection.
- C. The IdP IP address is 10.1.10.254.
- D. The IdP IP address is 10.1.10.2.

Suggested Answer: D

Community vote distribution

D (100%)

 **IBB90704** 3 months ago

Selected Answer: D

SAML serves as an open standard designed for exchanging authentication between an identity provider (IdP) and one or more service providers (SP).

IdP: A common setup is to use FortiAuthenticator as the IdP

Pagina 182,183,184,185

upvoted 3 times

Refer to the exhibit, which shows the output of the command `get router info bgp neighbors 100.64.2.254 advertised-routes`.

```
# get router info bgp neighbors 100.64.2.254 advertised-routes

VRF 0 BGP table version is 3, local router ID is 172.16.1.254
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf   Weight RouteTag Path
*> 10.20.30.40/24        100.64.2.1             xxx         0           0       100 i <-/->

Total number of prefixes 1
```

What can you conclude from the output?

- A. The BGP state of the two BGP participants is OpenConfirm.
- B. The router ID of the neighbor is 100.64.2.254.
- C. The BGP neighbor is advertising the 10.20.30.40/24 network to the local router.
- D. The local router is advertising the 10.20.30.40/24 network to its BGP neighbor.

Suggested Answer: D

Community vote distribution

D (100%)

 **IBB90704** 3 months ago

Selected Answer: D

This slide shows the command you can use to get details about the prefixes the local router is advertising.

Pagina 407

upvoted 4 times

Refer to the exhibit, which shows the partial output of a real-time OSPF debug.

Real-time OSPF debug output

```

OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114 {192.168.37.115 -> 224.0.0.5}
OSPF: -----
OSPF: Header
OSPF:   Version 2
OSPF:   Type 1 (Hello)
OSPF:   Packet Len 48
OSPF:   Router ID 0.0.0.112
OSPF:   Area ID 0.0.0.0
OSPF:   Checksum 0x2f85
OSPF:   AuType 0
OSPF: Hello
OSPF:   NetworkMask 255.255.255.0
OSPF:   HelloInterval 10
OSPF:   Options 0x2 (*| - | - | - | - | E | -)
OSPF:   RtrPriority 1
OSPF:   RtrDeadInterval 40
OSPF:   DRouter 192.168.37.114
OSPF:   BDRouter 192.168.37.115
OSPF:   # Neighbors 1
OSPF:     Neighbor 0.0.0.111
OSPF: -----
OSPF: RECV[Hello]: From 0.0.0.112 via port2:192.168.37.114: Authentication type mismatch

```

Why are the two FortiGate devices unable to form an adjacency?

- A. The Hello packet is being sent from an OSPF router with ID 0.0.0.112.
- B. The two FortiGate devices attempting adjacency are in area 0.0.0.0.
- C. One FortiGate device is configured to require authentication, while the other is not.
- D. The passwords on the FortiGate devices do not match.

Suggested Answer: C

Community vote distribution

C (100%)

 **IBB90704** Highly Voted 3 months ago

Selected Answer: C

Failed Adjacency Error Messages:

- Authentication type mismatch: One device is configured to require authentication, while the other is not (AuType1 and AuType0).
- Authentication Error: Authentication type is the same, but passwords do not match.
- HelloInterval mismatch/RouterDeadInterval mismatch: Hello/dead interval timer mismatch.
- MTU size is too large: MTU mismatch.

Pagina 449, 450.

upvoted 5 times

Refer to the exhibit, which shows one way communication of the downstream FortiGate with the upstream FortiGate within a Security Fabric.

```
# diagnose sniffer packet any "tcp port 8013 or udp port 8014" 4
Using Original Sniffing Mode
interfaces=[any]
filters=[tcp port 8013 or udp port 8014]
47.220358 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
48.215338 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
50.218552 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
54.222117 port1 in 192.168.1.112.11234 -> 192.168.1.111.8013: syn 1204417526
```

What three actions must you take to ensure successful communication? (Choose three.)

- A. You must authorize the downstream FortiGate on the root FortiGate.
- B. FortiGate must not be in NAT mode.
- C. Ensure TCP port 8013 is not blocked along the way.
- D. You must enable Security Fabric/Fortitelemetry on the receiving interface of the upstream FortiGate.
- E. Ensure the port for Neighbor Discovery has been changed.

Suggested Answer: ACD

Community vote distribution

ACD (100%)

IBB90704 3 months ago

Selected Answer: ACD

The screenshot on this slide shows a communication issue between an upstream FortiGate and a downstream FortiGate. Some common causes of this issue include:

- The Security Fabric Connection setting has not been enabled on the upstream FortiGate GUI (under Administrative Access).
- The FortiGate devices in the Security Fabric are not using the same firmware.
- The device has not been authorized on the root FortiGate yet.
- The wrong root FortiGate IP address is configured on the downstream FortiGate.
- The FortiGate is not configured in NAT mode.
- TCP port 8013 is blocked. You can use the diagnose sniffer command to verify this

Pagina 126

upvoted 4 times

Refer to the exhibit, which shows the partial output of FortiOS kernel slabs.

| | | | | | | | | | | | | | | | |
|-----------------------|---|---|------|----|---|---|----------|-----|-----|---|---|----------|---|---|---|
| packet_de_duplication | 0 | 0 | 128 | 30 | 1 | : | tunables | 252 | 126 | 0 | : | slabdata | 0 | 0 | 0 |
| ip6_nat_record | 0 | 0 | 128 | 30 | 1 | : | tunables | 252 | 126 | 0 | : | slabdata | 0 | 0 | 0 |
| tcp6_session | 0 | 0 | 1536 | 5 | 2 | : | tunables | 60 | 30 | 0 | : | slabdata | 0 | 0 | 0 |
| ip6_session | 0 | 0 | 1300 | 3 | 1 | : | tunables | 60 | 30 | 0 | : | slabdata | 0 | 0 | 0 |
| ip_nat_record | 0 | 0 | 64 | 59 | 1 | : | tunables | 252 | 126 | 0 | : | slabdata | 0 | 0 | 0 |
| sctp_session | 0 | 0 | 1600 | 5 | 2 | : | tunables | 60 | 30 | 0 | : | slabdata | 0 | 0 | 0 |
| tcp_session | 3 | 5 | 1500 | 5 | 2 | : | tunables | 60 | 30 | 0 | : | slabdata | 1 | 1 | 0 |
| ip_session | 1 | 3 | 1200 | 3 | 1 | : | tunables | 60 | 30 | 0 | : | slabdata | 1 | 1 | 0 |

Which statement is true?

- A. The total slab size of the sctp_session slab is 0 kB and is associated with the user space.
- B. The total slab size of the ip_session slab is 3600 kB and is associated with the user space.
- C. The total slab size of the ip6_session slab is 1300 kB and is associated with the kernel.
- D. The total slab size of the tcp_session slab is 7500 kB and is associated with the kernel.

Suggested Answer: D

Community vote distribution

D (100%)

IBB90704 3 months ago

Selected Answer: D

The kernel memory slabs are collections of objects with a common purpose. They are used by the kernel to store information in memory.

This slide shows an example of some slabs. There are slabs for storing information about the TCP sessions.

The entries in the route cache are also stored in memory slabs.

To check how much memory is being allocated to kernel slabs, use the command `diagnose hardware sysinfo slab`.

The first column shows the slab name. The second column shows the total amount of active objects, then the number of available objects, and then the size of each object.

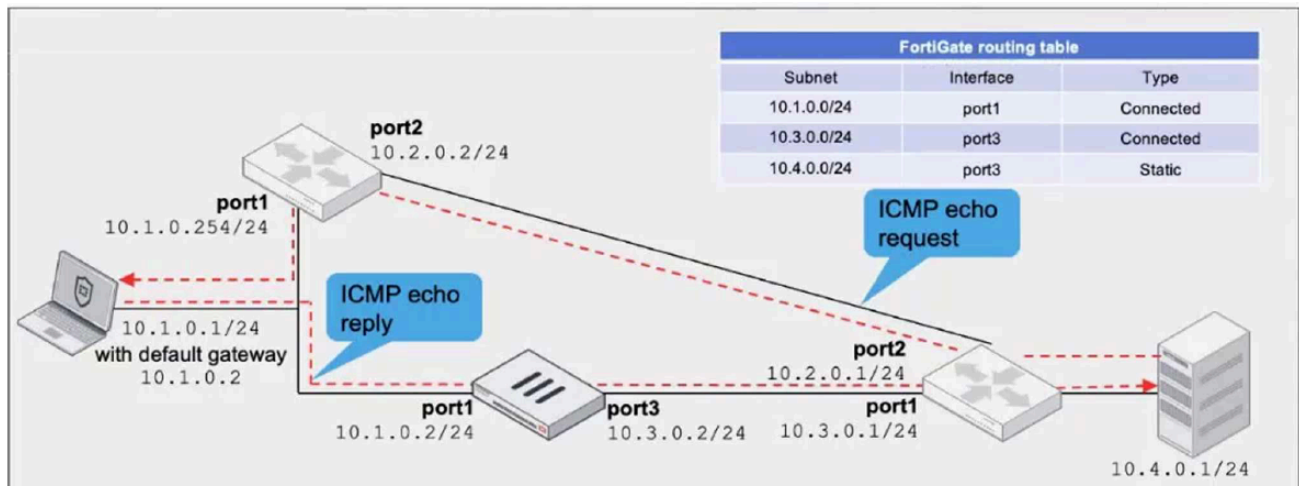
This amount changes depending on resource usage. For example, if tcp sessions increase on FortiGate, so will the available objects for that slab.

You can calculate the total amount of memory allocated to each slab type by multiplying the number of available objects by their size.

Pagina 47 y 48

upvoted 4 times

Refer to the exhibit, which a network topology and a partial routing table.



FortiGate has already been configured with a firewall policy that allows all ICMP traffic to flow from port1 to port3.

Which changes must the administrator perform to ensure the server at 10.4.0.1/24 receives the echo reply from the laptop at 10.1.0.1/24?

- A. Enable asymmetric routing under config system settings.
- B. Change the configuration from strict RPF check mode to feasible RPF check mode.
- C. A firewall policy that allows all ICMP traffic from port3 to port1.
- D. Modify the default gateway on the laptop from 10.1.0.2 to 10.2.0.2.

Suggested Answer: A

Community vote distribution

A (100%)

IBB90704 Highly Voted 3 months ago

Selected Answer: A

Allowing asymmetric routing:

```
config system settings
set asymroute enable
end
```

1. The server's ICMP request bypasses FortiGate reaching the PC.
2. The PC's echo reply passes through FortiGate. No session is matched. However, the packet is not dropped. Instead, the packet is passed to the CPU of FortiGate and is then forwarded using the FIB.
3. All subsequent echo replies are handled the same way as in step 2.
4. FortiGate essentially acts as a router. No security inspection is performed.

If you use asymmetric routing for troubleshooting purposes, remember to disable it after you resolve the issue.

Pagina 377

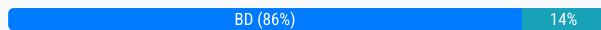
upvoted 7 times

What are two functions of automation stitches? (Choose two.)

- A. You can configure automation stitches on any FortiGate device in a Security Fabric environment.
- B. You can configure automation stitches to execute actions sequentially by taking parameters from previous actions as input for the current action.
- C. You can set an automation stitch configured to execute actions in parallel to insert a specific delay between actions.
- D. You can create automation stitches to run diagnostic commands and attach the results to an email message when CPU or memory usage exceeds specified thresholds.

Suggested Answer: BD

Community vote distribution



IBB90704 Highly Voted 3 months ago

Selected Answer: BD

- If you configure stitches in a Security Fabric, you must configure them on the root FortiGate.

- Sequential execution allows you to configure a delay

between actions to allow for tasks to be completed before proceeding to the next action. This is important because when using sequential execution, you can take action parameters from actions that have happened previously and use them as input for the action currently being executed. In the example shown on this slide, the automation stitch is going to execute actions sequentially.

- Parallel execution executes all configured actions at the same time as soon as the stitch is triggered. You cannot use action parameters with parallel execution.

Pagina 139 Network_Security_Support_Engineer_7.4_Study_Guide

Pagina 76 Enterprise_Firewall_7.2_Study

upvoted 6 times

payafs Most Recent 2 months, 2 weeks ago

Selected Answer: BC

FortiGate_7.4_Administrator_Study_Guide

Page 473

upvoted 1 times

Refer to the exhibit, which contains the partial configuration of an IPsec VPN configuration.

Partial output of IPsec VPN

```
config vpn ipsec phase1-interface
edit "IPSEC_DHCP"
set type dynamic
set interface "wan"
set mode aggressive
set peertype any
set net-device disable
set mode-cfg enable
set proposal aes128-sha256 aes256-sha256
set dhgrp 5
set xauthtype auto
set authusrgrp "IPSEC_Group"
set ipv4-start-ip 10.101.110.4
set ipv4-end-ip 10.101.110.62
set ipv4-netmask 255.255.255.192
set dns-mode auto
set ipv4-split-include "IPSEC_GRP"
set save-password enable
set client-auto-negotiate enable
set client-keep-alive enable
set dpd-retryinterval 60
end
```

After reviewing the configuration, what can you conclude about the IPsec VPN Phase 1 setup?


- A. The VPN is configured using IKEv2.
- B. Dead Peer Detection is disabled.
- C. The VPN is configured with DHCP over IPsec.
- D. The tunnel is configured as a route-based VPN.

Suggested Answer: C

Community vote distribution

C (67%)

D (33%)

  **cgallardo** 1 month, 1 week ago

Selected Answer: D

DHCP over IPSEC is achieved in phase2 with the setting:

set dhcp-ipsec enable

upvoted 2 times

  **payafs** 2 months, 3 weeks ago

Selected Answer: C

set type dynamic and set ipv4-start-ip and set ipv4-end-ip

These settings indicate that the VPN is set up to support remote dial-up clients that dynamically receive configuration information
upvoted 4 times

Refer to the exhibit, which shows the output of diagnose sys session list.

Diagnose output

```
# diagnose sys session list
session info: proto=6 proto_state=01 duration=73 expire=3597 timeout=3600
flags=00000000 sockflag=00000000 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/255
state=may_dirty synced none app_ntf
statistic {bytes/packets/allow_err}: org=822/11/1 reply=9037/15/1 tuples=2
origin->sink: org pre->post, reply pre->post dev=4->2/2->4
gwy=100.64.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:65464->54.192.15.182:80 (100.64.1.1:65464)
hook=pre dir=reply act=dnat 54.192.15.182:80->100.64.1.1:65464 (10.0.1.10:65464)
pos/ (before, after) 0/ (0,0), 0/ (0,0)
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00000098 tos=ff/ff ips view=0 app_list=0 app=0
dd_type=0 dd_mode=0
```

If the HA ID for the primary device is 0, what happens if the primary fails and the secondary becomes the primary?

- A. The secondary device has this session synchronized; however, because application control is applied, the session is marked dirty and has to be re-evaluated after failover.
- B. Traffic for this session continues to be permitted on the new primary device after failover, without requiring the client to restart the session with the server.
- C. The session will be removed from the session table of the secondary device because of the presence of allowed error packets, which will force the client to restart the session with the server.
- D. The session state is preserved but the kernel will need to re-evaluate the session because NAT was applied.

Suggested Answer: B

Community vote distribution

B (100%)

IBB90704 3 months ago

Selected Answer: B

You can check the session table of the primary device to see which sessions have been synchronized to the secondary devices. They are the ones with the synced flag. Additionally, and in the case of all sessions, the ha_id field shows the HA member ID of the device that is processing the traffic,

Pagina 297 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 3 times

Refer to the exhibit, which shows the partial output of a diagnose command.

```
# diagnose sys session list expectation
session info: proto=6 proto_state=00 duration=6 expire=23 timeout=3600 refresh_dir=both flags=00000000 sockflag=00000000
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
ha_id=0 policy_dir=1 tunnel=/
state=new npu acct-ext complex
statistic(bytes/packets/allow_err): org=0/0/0 reply=0/0/0 tuples=2
orgin->sink: org pre->post, reply pre->post dev=5->7/7->5 gwy=10.1.1.2/172.17.97.3

hook=pre dir=org act=dnat 93.157.14.94:0->10.200.1.1:60428(10.0.1.10:55402)
hook=pre dir=org act=noop 0.0.0.0:0->0.0.0.0:0(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=25 id_policy_id=0 auth_info=0 chk_client_info=0 vd=0
serial=008423f4 tos=ff/ff ips_view=0 app_list=0 app=0
```

Which two conclusions can you draw from the output shown in the exhibit? (Choose two.)

- A. FortiGate will drop the expected traffic if it does not arrive within 23 seconds.
- B. Clearing the master session has no impact on the expectation session.
- C. This is a pinhole session to allow traffic for a TCP protocol that dynamically assigns TCP ports.
- D. The session is checked against firewall policy ID 25.

Suggested Answer: AC

Community vote distribution

AC (100%)

 **IBB90704** 3 months ago

Selected Answer: AC

You can also see that FortiGate created an expectation session and opened the pin-hole port for the expected return traffic from the server with the IP address 93.157.14.94.

Pagina 115

duration: duration of the session (value in seconds).

expire: a countdown from the 'timeout' since the last packet passing via session (value in seconds).

timeout: an indicator of how long the session can stay open in the current state (value in seconds).

*shaper: the traffic shaper profile info (if traffic shaping is utilized).

policy_dir: 0 original direction | 1 reply direction.

tunnel: VPN tunnel name.

helper: name of the utilized session helper.

vlan_cos: Ingress COS values are displayed in the session output in the range 0-7/255, but admin COS values are displayed in the range 8-15/255 even though the value on the wire will be in the range 0-7. When no COS is utilized the value is 255/255.

state: See the table below for a list of states and what is the meaning.

upvoted 4 times

Consider the scenario where the server name indication (SNI) does not match either the common name (CN) or any of the subject alternative names (SAN) in the server certificate.

Which action will FortiGate take when using the default settings for SSL certificate inspection?

- A. FortiGate uses the CN information from the Subject field in the server certificate.
- B. FortiGate uses the SNI from the user's web browser.
- C. FortiGate will establish a connection without SSL/TLS inspection.
- D. The web filter will automatically bypass SSL inspection for this connection.

Suggested Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **payafs** 2 months, 2 weeks ago

Selected Answer: A

FortiGate 7.6 Administrator Study Guide 263

upvoted 2 times

🗲️ 👤 **IBB90704** 3 months ago

Selected Answer: A

When doing certificate-based inspection, by default, FortiGate validates the information in the SNI field of the client's request against the information in CN and SAN fields of the server's certificate. If the domain in the SNI field does not match any of the domains listed in the CN and SAN fields, FortiGate uses the domain in the CN field instead of the domain in the SNI field

Pagina 238 Enterprise_Firewall_7.2_Study

upvoted 4 times

Refer to the exhibits.

Exhibit 1

```
FGT-A # get router info bgp summary
***
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.37.202 4      65110   2500   2552     5    0  0 1d11h33m      0
```

Exhibit 2

```
FGT-B # show router bgp

config network
edit 1
set prefix 172.16.0.0 255.255.0.0
next
end
```

Exhibit 3

```
FGT-B # diagnose ip address list | grep port3
IP=172.16.54.115->172.16.54.202/255.255.255.0 index=5 devname=port3
```

An administrator is attempting to advertise the network configured on port3. However, FGT-A is not receiving the prefix.

Which two actions can the administrator take to fix this problem? (Choose two.)

- A. Modify the prefix using the network command from 172.16.0.0/16 to 172.16.54.0/24.
- B. Manually add the BGP route on FGT-A.
- C. Restart BGP using a soft reset to force both peers to exchange their complete BGP routing tables.
- D. Use the set network-import-check disable command.

Suggested Answer: AD

Community vote distribution

AD (100%)

IBB90704 3 months ago

Selected Answer: AD

You can also use the network command to configure FortiGate BGP to advertise prefixes. However, an exact match of the prefix in the network command must be active in the routing table. If the routing table doesn't contain an active route with a destination subnet that matches the prefix, FortiGate doesn't advertise the prefix. Pagina 388 Enterprise_Firewall_7.2_Study

There are two ways to fix the issue in troubleshooting scenario 2. The first way is to change the prefix manually to represent the network assigned.

The other option is to disable the set network-import-check. This is the safety mechanism that prevented FortiOS from advertising the falsely configured route. Disabling this mechanism is generally not recommended because this mechanism ensures that only the correct networks are advertised, which avoids routing issues. Pagina 420 - 421 Network_Security_Support_Engineer_7.4_Study_Guid
upvoted 4 times

Refer to the exhibit, which shows a partial output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -1
# diagnose debug enable
fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

- A. The user was found in the LDAP tree, whose root is TAC.ottawa.fortinet.com.
- B. FortiOS performs a bind to the LDAP server using the user's credentials.
- C. FortiOS collects the user group information.
- D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Suggested Answer: AD

Community vote distribution

AD (100%)

IBB90704 3 months ago

Selected Answer: AD

There are four steps to LDAP authentication using regular bin:

- The second step, FortiGate does a search query in the LDAP database to find the user's location—in other words, the user's DN.

A start_search_dn message indicates that FortiGate is performing step two: searching for the user in the LDAP tree.

Pagina 157 y 164 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 3 times

During which phase of IKEv2 does the Diffie-Helman key exchange take place?

- A. IKE_Req_INIT
- B. Create_CHILD_SA
- C. IKE_Auth
- D. IKE_SA_INIT

Suggested Answer: D

Community vote distribution

D (100%)

 **IBB90704** 3 months ago

Selected Answer: D

Page 348 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 3 times

In the SAML negotiation process, which section does the Identity Provider (IdP) provide the SAML attributes utilized in the authentication process to the Service Provider (SP)?

- A. SP Login dump
- B. Authentication Response
- C. Authentication Request
- D. Assertion dump

Suggested Answer: D

Community vote distribution

D (100%)

🗨️ 👤 **IBB90704** 3 months ago

Selected Answer: D

SAML attributes are pieces of information about a user that are exchanged between IdPs and SPs during the SAML authentication process. These attributes are included in the SAML assertion, which is built by the IdP as part of the authentication process. The SAML assertion contains information about the user, such as their identity, attributes, and authentication method.

Pagina 181 Network_Security_Support_Engineer_7.4_Study_Guide
upvoted 2 times

Refer to the exhibit, which shows the partial output of diagnose sys session stat.

```
# diagnose sys session stat
misc info: session_count=1523 setup_rate=0 exp_count=0 reflect_count=0 clash=113
memory_tension_drop=0 ephemeral=0/131072 removeable=0 extreme_low_mem=0
npu_session_count=0
delete=0, flush=1, dev_down=0/0
session walkers: active=0, vf-42, dev-0, saddr-0, npu-0
TCP sessions:
  562 in ESTABLISHED state
  15 in SYN_RECV state
  27 in CLOSE state
```

Which statement about the output shown in the exhibit is correct?

- A. 27 sessions have expired but are still in the session table in case any out-of-order packets arrive.
- B. 15 sessions have been categorized as ephemeral.
- C. 113 sessions have been dropped because of memory page exhaustion.
- D. 562 TCP sessions have their proto_state set to 01 if there is no inspection.

Suggested Answer: A

Community vote distribution

A (100%)

🗉 👤 **payafs** 2 months, 2 weeks ago

Selected Answer: A

When a session is closed by both the sender and receiver, FortiGate keeps that session in the session table for a few seconds, to allow for any out-of-order packets that might arrive after the FICK packet.

Network Security Support Engineer 7.4 Study Guide 84

upvoted 2 times

🗉 👤 **payafs** 2 months, 2 weeks ago

Selected Answer: A

Sessions in the CLOSE state are kept in the table for a short time after closure to handle any late or out-of-order packets related to the connection. This is standard TCP behavior.

upvoted 2 times

Refer to the exhibit, which shows the partial output of command diagnose debug rating.

```
-- Server List (Mon May 6 03:47:52 2024) --
IP          Weight  RTT  Flags  TZ  FortiGuard-requests  Curr Lost  Total Lost  Updated Time
64.26.151.37 10      45   -5     -5  262432              0          846 Mon May 6 03:47:43 2024
64.26.151.35 10      46   -5     -5  329072              0          6806 Mon May 6 03:47:43 2024
66.117.56.37 10      75   -5     -5  71638               0          275 Mon May 6 03:47:43 2024
65.210.95.240 20      71   -8     -8  36875               0          92 Mon May 6 03:47:43 2024
209.22.147.36 20      103 DI -8     -8  34784               0          1070 Mon May 6 03:47:43 2024
208.91.112.194 20      107 D  -8     -8  35170               0          1533 Mon May 6 03:47:43 2024
96.45.33.65 60      144  0      0  33728               0          120 Mon May 6 03:47:43 2024
80.85.69.41 71      226  1      1  33797               0          192 Mon May 6 03:47:43 2024
62.209.40.74 150     97   9      9  33754               0          145 Mon May 6 03:47:43 2024
121.111.236.179 45      44  P    -5  26410              26226     26227 Mon May 6 03:47:43 2024
```

In this exhibit, which FDS server will the FortiGate algorithm choose?

- A. 66.117.56.37
- B. 208.91.112.194
- C. 209.22.147.36
- D. 64.26.151.37

Suggested Answer: D

Community vote distribution

D (100%)

 **IBB90704** 3 months ago

Selected Answer: D

FortiGate uses the server with the lowest weight as the one for the rating queries. If two or more servers have the same weight, FortiGate uses the server with the lowest round-trip time (RTT)

Pagina 233 Network_Security_Support_Engineer_7.4_Study

upvoted 3 times

Refer to the exhibit, which shows the output of the command `get router info ospf neighbor`.

```
# get router info ospf neighbor
```

OSPF process 0, VRF 0:

| Neighbor ID | Pri | State | Dead Time | Address | Interface |
|-------------|-----|--------------|-----------|------------|-----------|
| 0.0.0.12 | 1 | Full/DROther | 02:14:39 | 10.10.2.1 | wan1 |
| 0.0.0.15 | 1 | Full/BDR | 04:26:37 | 10.10.3.2 | wan2 |
| 0.0.0.18 | c1 | Full/ - | 05:04:36 | 172.16.1.2 | ToHub |

To what extent does FortiGate operate when looking at its OSPF neighbors? (Choose two.)

- A. The local FortiGate has at least one interface that participates in a broadcast network.
- B. The local FortiGate has at least one interface that participates in a point-to-point network.
- C. The local FortiGate is the DR.
- D. Neighbor 0.0.0.18 is the designated router (DR).

Suggested Answer: AB

Community vote distribution


AB (100%)

 **payafs** 2 months, 2 weeks ago

Selected Answer: AB

Answer > A,B

upvoted 2 times

 **IBB90704** 3 months ago

Selected Answer: AB

Pagina 181 Enterprise_Firewall_7.2_Study

The command on this slide shows a summary of the statuses of all the OSPF neighbors. For each neighbor, it displays the adjacency state and if it is a DR, a BDR, or neither (DROther)

Pagina 362 Enterprise_Firewall_7.2_Study.

- Point-to-point networks contain only two peers, one at each end of a point-to-point link
- Broadcast networks (multi-access) support more than two attached routers. They also support sending messages to multiple recipients (broadcasting).

Pagina 365 Enterprise_Firewall_7.2_Study.

In any multi-access network there is one DR and one BDR.

Pagina 439 Network_Security_Support_Engineer_7.4_Study

FULL/- This represents a point-to-point network

upvoted 4 times

FortiGate performs different actions when in conserve mode depending on the configured memory thresholds.

Which actions correlates to which thresholds? (Choose two.)

- A. FortiGate exits conserve mode when the system memory goes below the configured green threshold.
- B. FortiGate starts dropping all new sessions when the system memory reaches the configured red threshold.
- C. FortiGate enters conserve mode when the system memory reaches the configured extreme threshold.
- D. FortiGate starts taking the configured action for new sessions requiring content inspection when the system memory reaches the configured red threshold.

Suggested Answer: AD

Community vote distribution

AD (100%)

🗉 👤 **IBB90704** 2 months, 4 weeks ago

Selected Answer: AD

Extreme: The threshold at which FortiGate starts dropping new sessions.

- Red: The threshold at which FortiGate enters conserve mode.
- Green: The threshold at which FortiGate exits conserve mode

Pagina 57 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 4 times

Refer to the exhibits, which contain the partial configurations of two VPNs on FortiGate.

Exhibit 1

```
config vpn ipsec phase1-interface
edit "user-1"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-1"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

Exhibit 2

```
config vpn ipsec phase1-interface
edit "user-2"
    set type dynamic
    set interface "port1"
    set mode main
    set xauthtype auto
    set authusrgrp "Users-2"
    set peertype any
    set dhgrp 14 15 19
    set proposal aes128-sha256 aes256-sha384
    set psksecret <encrypted_password>
next
```

An administrator has configured two VPNs for two different user groups. Users who are in the Users-2 group are not able to connect to the VPN. After running a diagnostics command, the administrator discovers that FortiGate is not matching the user-2 VPN for members of the Users-2 group.

Which two changes must the administrator make to fix the issue? (Choose two.)

- A. Change to aggressive mode on both VPNs.
- B. Enable XAuth on both VPNs.
- C. Use different pre-shared keys on both VPNs.
- D. Set up specific peer IDs on both VPNs.

Suggested Answer: AD

Community vote distribution

AD (100%)

 **IBB90704** Highly Voted 3 months ago

Selected Answer: AD

When you configure multiple dial-up IPsec VPNs, IKEv2 makes it simpler to match the intended gateway by peer ID. With IKEv2, you can either use the standard peer ID attribute or the Fortinet proprietary network ID attribute to indicate the phase 1 gateway to match on the dial-up server, regardless of the authentication mode in use. However, with IKEv1, you can use the peer ID only, and then combine it with aggressive mode and pre-shared key authentication, or with main mode and certificate signature authentication.

  **d9eeb6d** Most Recent 1 month, 3 weeks ago

Selected Answer: AD

FCSS - Network Security Support Engineer 7.4 Sample Questions

same question and response A & D correct

upvoted 2 times

Refer to the exhibit.

Debug output

```
FGT # diagnose debug application ike -1
FGT # diagnose debug enable

FGT # ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0...
ike 0: IKEv1 exchange=Informational id=61bba3725bd738d3/265a0b7a271799b7:9e253b8b len=108 vrf=0
ike 0: in
61BBA3725BD738D3265A0B7A271799B7081005019E253B8B0000000CE306FFBD5AD97F5AD027B12CAE19C5EFA091209F6D184E10DF2548B9B1FF6BF6A13167A172
26398E 851BE86CDACD29234B58E5F48024711F4EA1F216E791CB1B13650F1E4698CFA5A653CE9E627C92E9
ike 0:VPN_0:24266: dec 977A47FB000000200000000101108D2861BBA3725BD738D3265A0B7A271799B70000014D85DB9684B6CFE9C681AE840B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 0F45C660000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000000
ike 0:VPN_0:24319: out AD893C189C22FA2E8D3B17E7FB9574BA4BF1D49AD47DE62294ECA98B204D890A367DBDDDB20E5812CB470F87CB15504E
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0...
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:blidd9b5f len=108 vrf=0
ike 0: in 82A79C36BC7F9ECDE1062B00FEBCE8239F55E1F3E38196550041FDAAF20304B253855D2A3E253A6480D90
ike 0:VPN_0:24319: dec 8CC06CBD000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000001E186A982E6B2A3E9FBF8F30B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc 11AEC31B000000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000001
ike 0:VPN_0:24319: out E83C93D51EF44D937E260373CC9A86A09398EA3EDDD78FAEC8DE4E1F650DDC2E9E5626F34EF2346DF1807983C12E80D2
ike shrank heap by 335872 bytes
ike 0: comes 73.25.189.174:4500->96.71.182.225:4500,ifindex=18,vrf=0...
ike 0: IKEv1 exchange=Informational id=30db9994e7e8547d/50f9d18113b6ca99:a9040efb len=108 vrf=0
ike 0: in 0710D9A5184A392DC8DB96B354FF46B84E6A79622FC1D44BC7F964986AD95D49AC93BEDE376CB31EA2BD57
ike 0:VPN_0:24319: dec 03A44559000000200000000101108D2830DB9994E7E8547D50F9D18113B6CA9900000002C0D9F8CEB8B2B7CDD5CACA0B
ike 0:VPN_0:24319: notify msg received: R-U-THERE
ike 0:VPN_0:24319: enc E18A8338C00000200000000101108D2930DB9994E7E8547D50F9D18113B6CA9900000002
ike 0:VPN_0:24319: out C4906BDD8812D02AE1672BD0E893431344D7BC31E9323A2C56E27DB43B747870885D7954558993B25BC43118695BEA47
ike 0:VPN_0:24266: recv IPsec SA delete, spi count 1
ike 0:VPN_0: deleting IPsec SA with SPI 6161297a
ike 0:VPN_0:vpn2-1: deleted IPsec SA with SPI 6161297a, SA count: 0
ike 0:VPN_0:7220167: del route 172.21.27.56/255.255.255 tunnel 73.25.189.174 oif VPN_0(12922) metric 15 priority 1
ike 0:VPN_0: sending SNMP tunnel DOWN trap for vpn2-1
ike 0:VPN_0:vpn2-1: delete
```

An IPsec VPN tunnel is dropping, as shown by the debug output.

Analyzing the debug output, what could be causing the tunnel to go down?

- A. Phase 2 drops but Phase 1 is up.
- B. Dead Peer Detection is not receiving its acknowledge packet.
- C. The tunnel drops during rekey negotiation.
- D. The tunnel drops after the timer expires.

Suggested Answer: B

Community vote distribution

B (100%)

 **IBB90704** 2 months, 4 weeks ago

Selected Answer: B

notify msg received: R-U-THERE:

These messages are part of the DPD (dead peer detection)

upvoted 4 times

Refer to the exhibit, which shows two entries that were generated in the FSSO collector agent logs.

```
name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
failed to connect to registry: WORKSTATION02 (192.168.12.232)
```


What three conclusions can you draw from these log entries? (Choose three.)

- A. The user's status shows as "not verified" in the collector agent.
- B. The FortiGate firmware version is not compatible with that of the collector agent.
- C. Remote registry is not running on the workstation.
- D. DNS resolution is unable to resolve the workstation name.
- E. A firewall is blocking traffic to port 139 and 445.

Suggested Answer: ACE

Community vote distribution

ACE (100%)

 **IBB90704** 2 months, 4 weeks ago

Selected Answer: ACE

- Active users with a status of "not verified" are also a common problem.
- A firewall is blocking traffic to port 139 and 445
- The workstation remote registry service is not running

Pagina 222 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 3 times

Refer to the exhibit, which shows a partial web filter profile configuration.

Web filter profile

Edit Web Filter Profile

☒ **Bandwidth Consuming** 6

| | |
|---------------------------------|---|
| Freeware and Software Downloads | <input checked="" type="checkbox"/> Allow |
| File Sharing and Storage | <input checked="" type="checkbox"/> Block |
| 30% 93 | |

☐ Allow users to override blocked categories

☒ **Static URL Filter**

Block invalid URLs ☐

URL Filter ☒

+ Create New
Edit
Delete

Q

| URL | Type | Action | Status |
|--------------|----------|---|--|
| *dropbox.com | Wildcard | <input checked="" type="checkbox"/> Allow | <input checked="" type="checkbox"/> Enable |

1

Block malicious URLs discovered by FortiSandbox ☐

Content Filter ☒

+ Create New
Edit
Delete

| Pattern Type | Pattern | Language | Action | Status |
|--------------|-----------|----------|--|--|
| Wildcard | *dropbox* | Western | <input checked="" type="checkbox"/> Exempt | <input checked="" type="checkbox"/> Enable |

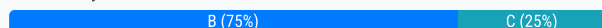
The URL www.dropbox.com is categorized as File Sharing and Storage.

Which action does FortiGate take if a user attempts to access www.dropbox.com?

- A. FortiGate blocks the connection as an invalid URL.
- B. Based on the URL Filter configuration, FortiGate allows the connection.
- C. FortiGate blocks the connection, based on the FortiGuard category-based filter configuration.
- D. Based on the Web Content filter configuration, access to www.dropbox.com would be exempted.

Suggested Answer: B

Community vote distribution



cgallardo 1 month, 1 week ago



Selected Answer: C

FortiGate follows a specific order when evaluating web traffic:

1. Static URL Filter: First, it checks the static URL filter for a match.
2. FortiGuard Category Filter: If the URL isn't found in the static URL filter or the action is "Allow", FortiGate then checks the FortiGuard category filter. (in this example category is blocking)

3.Advanced Filters: Finally, it may apply advanced filters like content filtering or script filtering.

upvoted 1 times

  **IBB90704** 3 months ago

Selected Answer: B

During web filtering inspection, FortiGate first checks the static URL filter list, then the FortiGuard categories, and then the content filtering list.

Pagina 235 Enterprise_Firewall_7.2_Study.

upvoted 3 times

The local OSPF router is unable to establish adjacency with a peer.

Which two things should the administrator do to troubleshoot the issue? (Choose two.)

- A. Check whether TCP port 179 is blocked.
- B. Check if there is an active static route to the peer.
- C. Check whether both peers have an IP address within the same subnet.
- D. Check if IP protocol 89 is blocked.

Suggested Answer: CD

Community vote distribution

CD (100%)

🗲️ 👤 **joeytrib** 1 month, 4 weeks ago

Selected Answer: CD

Correct answer C&D (P.445)

upvoted 2 times

🗲️ 👤 **IBB90704** 2 months, 4 weeks ago

Selected Answer: CD

Check that the local router can reach the remote peer. IP addresses must be in the same subnet and have the same subnet mask.

- Ensure that IP protocol 89 is not blocked

Pagina 445 Network_Security_Support_Engineer_7.4_Study_Guide-

upvoted 4 times

Refer to the exhibit.

```
# diagnose sys top
Run Time: 0 days, 0 hours and 18 minutes
OU, ON, 1S, 95I, OWA, OHI, OSI, OST; 16063, 12523F
    pyfcgid      248      S      2.9      3.8  9
    newcli       251      R      0.1      1.0  5
merged_daemons 185      S      0.1      0.7  6
    miglogd      177      S      0.0      6.8  0
    pyfcgid      249      S      0.0      3.0  2
    pyfcgid      246      S      0.0      2.8  5
    reportd      197      S      0.0      2.7  2
    cmdbsvr      113      S      0.0      2.4  7
```

Which three pieces of information does the diagnose sys top command provide? (Choose three.)

- A. The miglogd daemon is running on CPU core ID 0.
- B. The diagnose sys top command has been running for 18 minutes.
- C. The cmdbsvr process is occupying 2.4% of the total user memory space.
- D. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.
- E. If the newcli daemon continues to be in the R state, it will need to be manually restarted.

Suggested Answer: ACD

Community vote distribution

ACD (100%)

🗨️ 👤 **joeytrib** 1 month, 4 weeks ago

Selected Answer: ACD

Correct answer : ACD (P49)

upvoted 2 times

🗨️ 👤 **IBB90704** 2 months, 4 weeks ago

Selected Answer: ACD

Pagina 49 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 4 times

Refer to the exhibit, which shows a partial output from the get router info routing-table database command.

```
# get router info routing-table database
---omitted---

Routing table for VRF=0
S          0.0.0.0/0 [20/0] via 100.64.2.254, port2, [10/0]
S          0.0.0.0/0 [10/0] via 100.64.1.254, port1 inactive, [50/0]
---omitted---
```

The administrator wants to configure a default static route for port3 and assign a distance of 50 and a priority of 0. What will happen to the port1 and port2 default static routes after the port3 default static route is created?

- A. The port2 default static route will be injected into the forwarding information base (FIB).
- B. The port1 default static route will be injected into the FIB.
- C. Neither of the routes shown in the output will be injected into the FIB.
- D. Both default static routes shown in the output will be injected into the FIB.

Suggested Answer: A

Community vote distribution

A (100%)

🗳️ 👤 **joeytrib** 1 month, 4 weeks ago

Selected Answer: A

Correct Answer : A

upvoted 1 times

🗳️ 👤 **d9eeb6d** 1 month, 4 weeks ago

Selected Answer: A

port1 inactive = interface administratively down -> not in FIB

Network Security Support Engineer Study Guide p384

upvoted 1 times

🗳️ 👤 **IBB90704** 2 months, 4 weeks ago

Selected Answer: A

First, FortiGate uses the most specific route, which is the one with the longest netmask (smallest subnet). If there are two or more routes with the same longest netmask, the device selects the one with the shortest distance. After that, FortiGate uses the lowest metric as the tiebreaker for dynamic routes. In the case of static routes, FortiGate uses the lowest priority instead. If there are multiple routes with the same netmask, distance, metric, and priority, FortiGate shares the traffic among all of them. This is called equal-cost multi-path (ECMP). ECMP is supported for static, BGP, and OSPF routes.

Pagina 363 Network_Security_Support_Engineer_7.4_Study_Guide

upvoted 3 times


Which three common FortiGate-to-collector-agent connectivity issues can you identify using the FSSO real-time debug? (Choose three.)

- A. Log is full on the collector agent.
- B. Inability to reach IP address of the collector agent.
- C. Refused connection. Potential mismatch of TCP port.
- D. Mismatched pre-shared password.
- E. Incompatible collector agent software version.

Suggested Answer: BCD

Community vote distribution

BCD (100%)

 **IBB90704** 2 months, 4 weeks ago

Selected Answer: BCD

The error server authentication failed, aborting in the FortiGate real-time debug might indicate a mismatch in the password shared between the collector agent and FortiGate.

The error connection refused might indicate that the TCP communication between FortiGate and the collector agent is blocked by a firewall or another device.

The error no route to host might indicate that the IP address of the collector agent is not routable from FortiGate.

Pagina 206 Network_Security_Support_Engineer_7.4_Study_Guide
upvoted 3 times

Refer to the exhibit, which shows a FortiGate configuration.

FortiGate configuration

```
config system fortiguard
  set protocol udp
  set port 8888
  set load-balance-servers1
  set auto-join-forticloud enable
  set update-server-location any
  set sandbox-region ''
  set fortiguard-anycast disable
  set antispam-force-off disable
  set antispam-cache enable
  set antispam-cache-ttl 1800
  set antispam-cache-mpercent2
  set antispam-timeout 7
  set webfilter-force-off enable
  set webfilter-cache enable
  set webfilter-cache-ttl 3600
  set webfilter-timeout 15
  set sdns-server-ip "208.91.112.220"
  set sdns-server-port 53
  unset sdns-options
  set source-ip 0.0.0.0
  set source-id6 ::
  set proxy-server-ip 0.0.0.0
  set proxy-server-port 0
  set proxy-username
  set ddns-server-ip 0.0.0.0
  set dns-server-port 443
end
```

An administrator is troubleshooting a web filter issue on FortiGate.

The administrator has configured a web filter profile and applied it to a policy; however, the web filter is not inspecting any traffic that is passing through the policy.

What must the administrator do to fix the issue?

- A. Disable webfilter-force-off at the VDOM level.
- B. Set sdns-server-ip to service.fortiguard.net.
- C. Disable webfilter-force-off.
- D. Change protocol to TCP and port to 53.

Suggested Answer: C

Community vote distribution

C (100%)

IBB90704 2 months, 4 weeks ago

Selected Answer: C

webfilter-force-off

disable (default) : enable web filter globally

enable: disable web filter globally

Pagina 252 Network_Security_Support_Engineer_7.4_Study_Guide
upvoted 2 times

Refer to the exhibit, which contains partial output from an IKE real-time debug.

Debug output

```
ike 0:624000:98: responder: main mode get 1st message...
ike 0:624000:98: VID DPD AFCAD71368A1F1C96B8696FC77570100
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3
ike 0:624000:98: VID FRAGMENTATION 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000
ike 0:624000:98: VID FORTIGATE 8299031757A36082C6A621DE00000000
ike 0:624000:98: incoming proposal:
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 0:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=256
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA2_256.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: my proposal, gw Remotesite:
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP2048.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: proposal id = 1:
ike 0:624000:98:   protocol id = ISAKMP:
ike 0:624000:98:   trans_id = KEY_IKE.
ike 0:624000:98:   encapsulation = IKE/none
ike 0:624000:98:   type=OAKLEY_ENCRYPT_ALG, val=AES_CBC, key-len=128
ike 0:624000:98:   type=OAKLEY_HASH_ALG, val=SHA.
ike 0:624000:98:   type=AUTH_METHOD, val=PRESHARED_KEY.
ike 0:624000:98:   type=OAKLEY_GROUP, val=MODP1536.
ike 0:624000:98: ISAKMP SA lifetime=86400
ike 0:624000:98: negotiation failure
ike Negot:: 624ea7b1bba276fb/0000000000000000:98: no SA proposal chosen
```

The administrator does not have access to the remote gateway.

Based on the debug output, which configuration change the administrator make to the local gateway to resolve the phase 1 negotiation error?

- A. In the phase 1 proposal configuration, add AES256-SHA256 to the list of encryption algorithms.
- B. In the phase 1 proposal configuration, add AESCBC-SHA2 to the list of encryption algorithms.
- C. In the phase 1 network configuration, set the IKE version to 2.
- D. In the phase 1 proposal configuration, add AES128-SHA128 to the list of encryption algorithms.

Suggested Answer: A

Community vote distribution

A (100%)

Incoming proposal

AES-256

SHA-256

My proposal

AES-128

SHA-1

No SA proposal chose

upvoted 3 times

Refer to the exhibit.

Antivirus profile configuration

```
config antivirus profile
  edit "Block"
    config http
      set av-scan block
    end
    config ftp
      set av-scan block
    end
    config imap
      set av-scan block
    end
    config pop3
      set av-scan block
    end
    config smtp
      set av-scan block
    end
  next
end
```

Firewall policy configuration

```
config firewall ssl-ssh-profile
edit "certificate-inspection"
  set comment "SSL handshake inspection."
  config https
    set ports 443
    set status certificate-inspection
    set quic inspect
  end
  config ftps
    set status disable
  end
  config imaps
    set status disable
  end
  config pop3s
    set status disable
  end
  config smtps
    set status disable
  end
  config ssh
    set ports 22
    set status disable
  end
  config dot
    set status disable
    set quic inspect
    set unsupported-ssl-version allow
  end
next
end
```

Antivirus is unable to detect an infected file downloaded through HTTPS. Part of the configuration used for antivirus inspection is shown in the