



Fortinet

Exam Questions FCP_FGT_AD-7.4

FCP - FortiGate 7.4 Administrator

NEW QUESTION 1

Refer to the exhibit, which shows the IPS sensor configuration.

Edit IPS Sensor

Name

WINDOWS_SERVERS

Comments

Write a comment... 0/255

Block malicious URLs

☐

IPS Signatures and Filters

+ Create New

Edit

Delete

| Details | Exempt IPs | Action | Packet Logging |
|------------------------------------|------------|---------|----------------|
| Microsoft.Windows.iSCSI.Target.DoS | 0 | Monitor | Enabled |
| Windows | | Block | Disabled |

2

If traffic matches this IPS sensor, which two actions is the sensor expected to take? (Choose two.)

- A. The sensor will gather a packet log for all matched traffic.
- B. The sensor will reset all connections that match these signatures.
- C. The sensor will allow attackers matching the Microsoft.Windows.iSCSI.Target.DoS signature.
- D. The sensor will block all attacks aimed at Windows servers.

Answer: AC

Explanation:

The IPS sensor configuration shows that:

➤ The Microsoft.Windows.iSCSI.Target.DoS signature is set to "Monitor" with packet logging enabled, meaning that while traffic matching this signature will be allowed, it will also be logged for further analysis.

➤ The generic Windows filter is set to "Block," meaning that all other attacks matching this filter will be blocked. However, the sensor will not reset connections or log packets unless specified.

Therefore, the sensor will allow attackers matching the specific DoS signature while blocking other attacks against Windows.

References:

➤ FortiOS 7.4.1 Administration Guide: IPS Configuration

NEW QUESTION 2

When FortiGate performs SSL/SSH full inspection, you can decide how it should react when it detects an invalid certificate. Which three actions are valid actions that FortiGate can perform when it detects an invalid certificate? (Choose three.)

- A. Allow & Warning
- B. Trust & Allow
- C. Allow
- D. Block & Warning
- E. Block

Answer: ADE

Explanation:

When FortiGate performs SSL/SSH full inspection and detects an invalid certificate, there are three valid actions it can take:

➤ Allow & Warning: This action allows the session but generates a warning.

➤ Block & Warning: This action blocks the session and generates a warning.

➤ Block: This action blocks the session without generating a warning.
Actions such as "Trust & Allow" or just "Allow" without additional configurations are not applicable in the context of handling invalid certificates.
References:
➤ FortiOS 7.4.1 Administration Guide: Configuring SSL/SSH inspection profile

NEW QUESTION 3

Which two statements describe how the RPF check is used? (Choose two.)

A. The RPF check is run on the first sent packet of any new session.
B. The RPF check is run on the first reply packet of any new session.
C. The RPF check is run on the first sent and reply packet of any new session.
D. The RPF check is a mechanism that protects FortiGate and the network from IP spoofing attacks.

Answer: AD

Explanation:
The Reverse Path Forwarding (RPF) check is run on the first sent packet of any new session to ensure that the packet arrives on a legitimate interface. This check protects the network from IP spoofing attacks by verifying that a return route exists from the receiving interface back to the source IP address. If the route is invalid or not found, the packet is discarded. Options B and C are incorrect because RPF checks are performed on the first sent packet, not the reply packet.
References:
➤ FortiOS 7.4.1 Administration Guide: Reverse Path Forwarding (RPF) Check

NEW QUESTION 4

Which three methods are used by the collector agent for AD polling? (Choose three.)

A. WinSecLog
B. WMI
C. NetAPI
D. FSSO REST API
E. FortiGate polling

Answer: ABC

Explanation:
The Fortinet Single Sign-On (FSSO) Collector Agent supports three primary methods for Active Directory (AD) polling to collect user information:
➤ WinSecLog: Monitors Windows Security Event Logs for login events.
➤ WMI: Uses Windows Management Instrumentation to poll user login sessions.
➤ NetAPI: Utilizes the Netlogon API to query domain controllers for user session data.
These methods allow the FortiGate to gather user logon information and enforce user-based policies effectively.
References:
➤ FortiOS 7.4.1 Administration Guide: FSSO Configuration

NEW QUESTION 5

What are two features of collector agent advanced mode? (Choose two.)

A. In advanced mode, FortiGate can be configured as an LDAP client and group filters can be configured on FortiGate.
B. Advanced mode supports nested or inherited groups.
C. In advanced mode, security profiles can be applied only to user groups, not individual users.
D. Advanced mode uses the Windows convention —NetBios: Domain\Username.

Answer: AD

Explanation:
Advanced mode allows for configuration as an LDAP client and supports group filtering directly on the FortiGate, as well as nested or inherited groups.

NEW QUESTION 6

Refer to the exhibit, which shows a partial configuration from the remote authentication server.

| Attribute | Value | Vendor | Actions |
|---------------------|----------|----------|---|
| Fortinet-Group-Name | Training | Fortinet |   |

Why does the FortiGate administrator need this configuration?

A. To authenticate only the Training user group.
B. To set up a RADIUS server Secret
C. To authenticate and match the Training OU on the RADIUS server.
D. To authenticate Any FortiGate user groups.

Answer: A

NEW QUESTION 7

An administrator manages a FortiGate model that supports NTurbo. How does NTurbo enhance performance for flow-based inspection?

- A. NTurbo offloads traffic to the content processor.
- B. NTurbo creates two inspection sessions on the FortiGate device.
- C. NTurbo buffers the whole file and then sends it to the antivirus engine.
- D. NTurbo creates a special data path to redirect traffic between the IPS engine its ingress and egress interfaces.

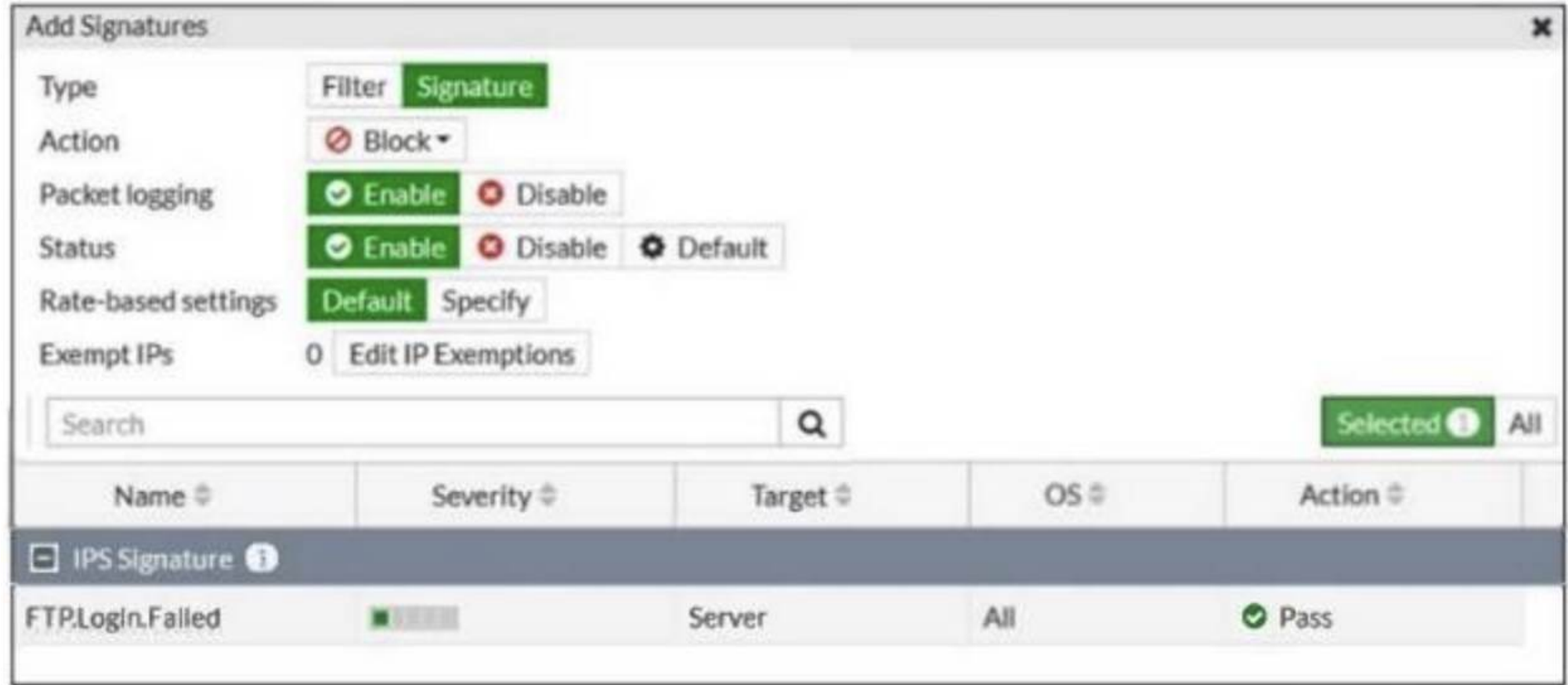
Answer: A

Explanation:

NTurbo enhances performance for flow-based inspection by offloading traffic to the content processor.

NEW QUESTION 8

Refer to the exhibit.



| Name | Severity | Target | OS | Action |
|------------------|----------|--------|----|--------|
| IPS Signature | | | | |
| FTP.Login.Failed | Server | All | | Pass |

Review the intrusion prevention system (IPS) profile signature settings shown in the exhibit. What do you conclude when adding the FTP.Login.Failed signature to the IPS sensor profile?

- A. Traffic matching the signature will be allowed and logged.
- B. The signature setting uses a custom rating threshold.
- C. The signature setting includes a group of other signatures.
- D. Traffic matching the signature will be silently dropped and logged.

Answer: A

Explanation:

The exhibit shows that the "FTP.Login.Failed" IPS signature is set with the action "Pass" and packet logging enabled. This means that any traffic matching this signature will be allowed through the FortiGate, and the traffic details will be logged for monitoring and analysis purposes.

References:

> FortiOS 7.4.1 Administration Guide: IPS Signature Actions

NEW QUESTION 9

Which two settings are required for SSL VPN to function between two FortiGate devices? (Choose two.)

- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN.
- B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate.
- C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate.
- D. The client FortiGate requires a manually added route to remote subnets.

Answer: BC

Explanation:

For SSL VPN to function correctly between two FortiGate devices, the following settings are required:

- > B. The server FortiGate requires a CA certificate to verify the client FortiGate certificate: The server FortiGate must have a Certificate Authority (CA) certificate installed to authenticate and verify the certificate presented by the client FortiGate device.
 - > C. The client FortiGate requires a client certificate signed by the CA on the server FortiGate: The client FortiGate must have a client certificate that is signed by the same CA that the server FortiGate uses for verification. This ensures a secure SSL VPN connection between the two devices.
- The other options are not directly necessary for establishing SSL VPN:

- A. The client FortiGate requires the SSL VPN tunnel interface type to connect SSL VPN: This is incorrect as SSL VPN does not require a specific tunnel interface type; it typically uses an SSL VPN client profile.
- D. The client FortiGate requires a manually added route to remote subnets: While routing may be necessary, it is not specifically required for the SSL VPN functionality between two FortiGates.

References

- FortiOS 7.4.1 Administration Guide - Configuring SSL VPN, page 1203.
- FortiOS 7.4.1 Administration Guide - SSL VPN Authentication, page 1210.

NEW QUESTION 10

Refer to the exhibits, which show the system performance output and the default configuration of high memory usage thresholds in a FortiGate.

System Performance output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2061108k total, 1854997k used (90%), 106111k free (5.1%), 100000k freeable (4.8%)
Average network usage: 83 / 0 kbps in 1 minute, 81 / 0 kbps in 10 minutes, 81 / 0 kbps in 30 minutes
Average sessions: 5 sessions in 1 minute, 3 sessions in 10 minutes, 3 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes, 0 sessions per second in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 3 hours, 28 minutes
```

Memory usage threshold settings

```
config system global
    set memory-use-threshold-red 88
    set memory-use-threshold-extreme 95
    set memory-use-threshold-green 82
end
```

Based on the system performance output, what can be the two possible outcomes? (Choose two.)

- A. FortiGate will start sending all files to FortiSandbox for inspection.
- B. FortiGate has entered conserve mode.
- C. Administrators cannot change the configuration.
- D. Administrators can access FortiGate only through the console port.

Answer: BC

Explanation:

Based on the system performance output provided, the memory usage on the FortiGate device is at 90%, which is above the green threshold (82%) but below the red threshold (88%). Given this high memory usage, the FortiGate device will enter "conserve mode" to prevent further resource exhaustion. In conserve mode:

- B. FortiGate has entered conserve mode: When the memory usage reaches or exceeds certain thresholds (in this case, the green and red thresholds), the FortiGate enters conserve mode to protect itself from running out of memory entirely. This mode limits some functionalities to reduce memory usage and avoid a potential system crash.
- D. Administrators can access FortiGate only through the console port: During conserve mode, administrative access might be restricted, and administrators may only be able to connect to the device via the console port. This restriction is in place to ensure that the FortiGate can be managed directly, even under low resource conditions.

The other options are not correct:

- A. FortiGate will start sending all files to FortiSandbox for inspection: This is unrelated to memory usage and conserve mode.
- C. Administrators cannot change the configuration: While access may be limited, configuration changes can still be made via the console port.

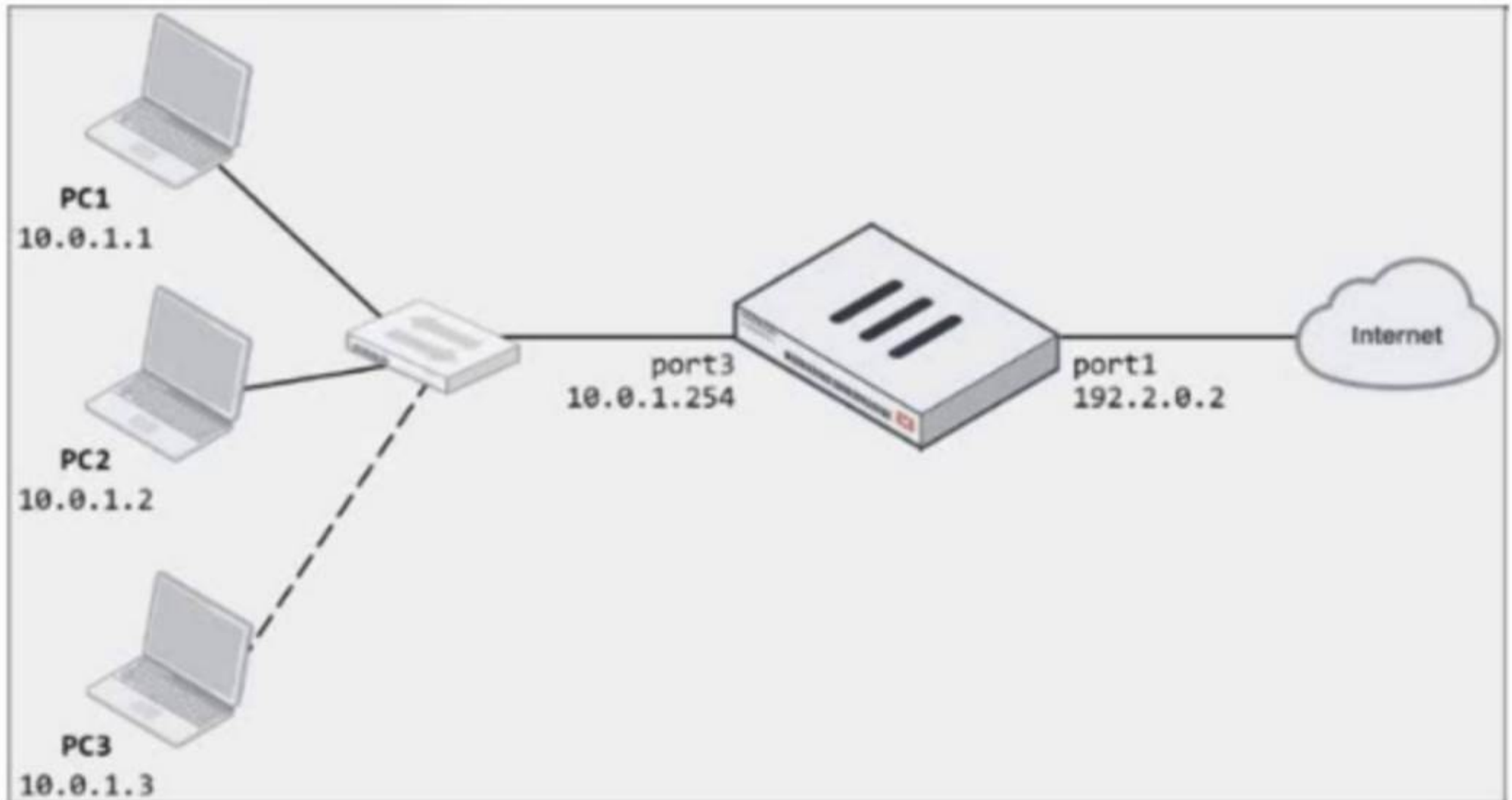
References

- FortiOS 7.4.1 Administration Guide - Monitoring System Resources and Performance, page 325.
- FortiOS 7.4.1 Administration Guide - Conserve Mode, page 330.

NEW QUESTION 10

Refer to the exhibits.

Network diagram



Dynamic IP pool

Edit Dynamic IP Pool

| | |
|---------------------------------|-------------------------------------|
| Name | internet-pool |
| Comments | Write a comment... 0/255 |
| Type | One-to-One |
| External IP Range | 192.2.0.10-192.2.0.11 |
| ARP Reply | <input checked="" type="checkbox"/> |

Firewall policy

Edit Policy

Name

LAN-to-Internet

Incoming Interface

LAN (port3)

×

Outgoing Interface

WAN (port1)

×

Source

all

×

Destination

all

×

Schedule

always

▼

Service

ALL

×

Action

✓ ACCEPT

⊘ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall/Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

internet-pool

×

Preserve Source Port

Protocol Options

PROT

default

The exhibits show a diagram of a FortiGate device connected to the network, as well as the firewall policy and IP pool configuration on the FortiGate device. Two PCs, PC1 and PC2, are connected behind FortiGate and can access the internet successfully. However, when the administrator adds a third PC to the network (PC3), the PC cannot connect to the internet. Based on the information shown in the exhibit, which two configuration options can the administrator use to fix the connectivity issue for PC3? (Choose two.)

- A. In the firewall policy configuration, add 10.
- B. 3 as an address object in the source field.
- C. In the IP pool configuration, set endip to 192.2.0.12.
- D. Configure another firewall policy that matches only the address of PC3 as source, and then place the policy on top of the list.
- E. In the IP pool configuration, set cype to overload.

Answer: BD

Explanation:

To resolve the issue of PC3 not being able to access the internet, the administrator needs to adjust the IP pool configuration or the firewall policy. The following two options will fix the connectivity issue:

- B. In the IP pool configuration, set the ending IP to 192.2.0.12: The current IP pool range is 192.2.0.10-192.2.0.11, which only provides two IP addresses for network address translation (NAT). To allow PC3 to access the internet, the IP pool should be expanded to include an additional IP address by changing the end of the range to 192.2.0.12.

Guaranteed success with Our exam guides

visit - <https://www.certshared.com>



D. In the IP pool configuration, set type to overload: Instead of using a one-to-one NAT, changing the type to overload will allow multiple internal addresses (such as PC1, PC2, and PC3) to share a single external IP address. This will solve the issue without needing additional public IP addresses. The other options are not suitable:



A. In the firewall policy configuration, add 10.0.1.3 as an address object in the source field: This option is unnecessary since the firewall policy already allows all addresses from the source (LAN port3).



C. Configure another firewall policy that matches only the address of PC3 as the source, and then place the policy on top of the list: This option is redundant and would not resolve the underlying issue with the IP pool configuration.

References



FortiOS 7.4.1 Administration Guide - Configuring Firewall Policies, page 512.



FortiOS 7.4.1 Administration Guide - Configuring NAT with IP Pools, page 518.

NEW QUESTION 12

An administrator configured a FortiGate to act as a collector for agentless polling mode.

What must the administrator add to the FortiGate device to retrieve AD user group information?

- A. LDAP server
- B. RADIUS server
- C. DHCP server
- D. Windows server

Answer: A

Explanation:

To retrieve AD user group information in agentless polling mode, the administrator must add an LDAP server to the FortiGate device.

NEW QUESTION 17

Refer to the exhibit to view the firewall policy.

Firewall policy configuration

Edit Policy

| | | | |
|--------------------|---|---|---|
| Name | Internet_Access | | |
| Incoming Interface | port2 | + | ✕ |
| Outgoing Interface | port1 | + | ✕ |
| Source | all | + | ✕ |
| Destination | all | + | ✕ |
| Schedule | always | | |
| Service | <div> DNS ✕ </div> <div> FTP ✕ </div> <div> HTTP ✕ </div> <div> HTTPS ✕ </div> <div>+</div> | | |
| Action | <div> <input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY </div> | | |
| Inspection Mode | <div> Flow-based Proxy-based </div> | | |

Firewall/Network Options

NAT
☒

IP Pool Configuration

Use Outgoing Interface Address
Use Dynamic IP Pool

Preserve Source Port
☐

Protocol Options

PROT default

Security Profiles

AntiVirus
☒

AV default

Web Filter
☐

DNS Filter
☐

Application Control
☐

IPS
☐

File Filter
☐

SSL Inspection

SSL certificate-inspection

Why would the firewall policy not block a well-known virus, for example eicar?

- A. The action on the firewall policy is not set to deny.
- B. The firewall policy is not configured in proxy-based inspection mode.
- C. Web filter is not enabled on the firewall policy to complement the antivirus profile.
- D. The firewall policy does not apply deep content inspection.

Answer: B

Explanation:

The firewall policy shown in the exhibit is configured in flow-based inspection mode. In flow-based inspection, certain security features, such as deep content inspection, might not be as effective as in proxy-based mode. Proxy-based inspection is necessary for thorough content inspection, which includes identifying and blocking well-known viruses like EICAR.

References:



FortiOS 7.4.1 Administration Guide: Inspection Modes

NEW QUESTION 20

A network administrator wants to set up redundant IPsec VPN tunnels on FortiGate by using two IPsec VPN tunnels and static routes. All traffic must be routed through the primary tunnel when both tunnels are up. The secondary tunnel must be used only if the primary tunnel goes down. In addition, FortiGate should be able to detect a dead tunnel to speed up tunnel failover. Which two key configuration changes must the administrator make on FortiGate to meet the requirements? (Choose two.)

- A. Enable Dead Peer Detection
- B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels.
- C. Configure a lower distance on the static route for the primary tunnel, and a higher distance on the static route for the secondary tunnel.
- D. Configure a higher distance on the static route for the primary tunnel, and a lower distance on the static route for the secondary tunnel.

Answer: AC

Explanation:

To configure redundant IPsec VPN tunnels on FortiGate with failover capability, the following two key configuration changes are required:



A. Enable Dead Peer Detection (DPD): Dead Peer Detection is crucial for detecting if the remote peer is unreachable. By enabling DPD, FortiGate can quickly detect a dead tunnel, ensuring a faster failover to the secondary tunnel when the primary tunnel goes down.



C. Configure a lower distance on the static route for the primary tunnel and a higher distance on the static route for the secondary tunnel: The static route with the lower distance (higher priority) will be used when both tunnels are operational. If the primary tunnel fails, the higher distance (lower priority) route for the secondary tunnel will take over, ensuring traffic is routed correctly.

The other options are not suitable:



B. Enable Auto-negotiate and Autokey Keep Alive on the phase 2 configuration of both tunnels: This option is not directly related to the requirements of failover between two IPsec VPN tunnels.



D. Configure a higher distance on the static route for the primary tunnel and a lower distance on the static route for the secondary tunnel: This would prioritize the secondary tunnel over the primary tunnel, which is opposite to the desired configuration.

References



FortiOS 7.4.1 Administration Guide - Configuring IPsec VPN, page 1320.



FortiOS 7.4.1 Administration Guide - Redundant VPN Configuration, page 1335.

NEW QUESTION 23

Refer to the exhibit.

| ID | Name | Source | Destination | Schedule | Service | Action | NAT | Type | Security Profiles |
|----|-------------|------------------------------|-------------|----------|---------------------------|--------|-----|----------|--|
| 1 | Full_Access | Remote-users LOCAL_SUB... | all | always | HTTP HTTPS ALL_ICMP | ACCEPT | NAT | Standard | Category_Monitor certificate-inspection |

FortiGate is configured for firewall authentication. When attempting to access an external website, the user is not presented with a login prompt. What is the most likely reason for this situation?

- A. The Service DNS is required in the firewall policy.
- B. The user is using an incorrect user name.
- C. The Remote-users group is not added to the Destination.
- D. No matching user account exists for this user.

Answer: A

Explanation:

Firewall authentication generally requires the DNS service to be enabled in the firewall policy to correctly resolve hostnames during the authentication process. If DNS is not allowed in the firewall policy, the FortiGate cannot resolve external domains, and as a result, the user may not be presented with the login prompt when attempting to access an external website.

References:



FortiOS 7.4.1 Administration Guide: Firewall Authentication Configuration

NEW QUESTION 26

The HTTP inspection process in web filtering follows a specific order when multiple features are enabled in the web filter profile. Which order must FortiGate use when the web filter profile has features such as safe search enabled?

- A. FortiGuard category filter and rating filter
- B. Static domain filter, SSL inspection filter, and external connectors filters
- C. DNS-based web filter and proxy-based web filter
- D. Static URL filter, FortiGuard category filter, and advanced filters

Answer: D

Explanation:

FortiGate applies web filters in the following order: Static URL filter, FortiGuard category filter, Web content filter, Web script filter, and Antivirus scanning.

NEW QUESTION 28

Refer to the exhibit, which shows an SD-WAN zone configuration on the FortiGate GUI.

FortiGate SD-WAN zone configuration



Based on the exhibit, which statement is true?

- A. The underlay zone contains port1 and
- B. The d-wan zone contains no member.
- C. The d-wan zone cannot be deleted.
- D. The virtual-wan-link zone contains no member.

Answer: C

Explanation:

In FortiGate's SD-WAN configuration, the d-wan zone is a system default SD-WAN zone that is automatically created and cannot be deleted. This zone is used to manage dynamic WAN links for SD-WAN traffic balancing and routing. It ensures that multiple WAN interfaces can be grouped and managed effectively for WAN link optimization.

Why the other options are less appropriate:

- A. The underlay zone contains port1 and: There is no mention in the exhibit about an "underlay zone" containing port1.
- B. The d-wan zone contains no member: This statement is irrelevant since the focus is on the zone's deletion, not its members.
- D. The virtual-wan-link zone contains no member: This is unrelated to the core fact that the d-wan zone cannot be deleted.

Reference:

FortiOS 7.4.1 Administration Guide: SD-WAN Zone Configuration

NEW QUESTION 33

Examine the IPS sensor and DoS policy configuration shown in the exhibit, then answer the question below.

IPS Sensor

Edit IPS Sensor

WINDOWS_SERVER

Name

EMAIL-SERVER-IPS

[View IPS Signatures]

Comments

IPS Signatures

Add Signatures
Delete
Edit IP Exemptions

| Name | Exempt IPs | Severity | Target | Service | OS | Action | Packet Logging |
|---------------------|------------|----------|--------|---------|-----|--------|----------------|
| SMTPLoginBruteForce | | | Server | TCP_SMT | All | Block | |

IPS Filters

Add Filter
Edit Filter
Delete

| Filter Details | Action | Packet Logging |
|------------------------------------|--------|----------------|
| Location: server Protocol: SMTP | Block | |

Rate Based Signatures

| Enable | Signature | Threshold | Duration (seconds) | Track By | Action | Block Duration (minutes) |
|-------------------------------------|--|-----------|--------------------|-----------|--------|--------------------------|
| <input checked="" type="checkbox"/> | IMAPLoginBruteForce | 60 | 10 | Source IP | Block | None |
| <input type="checkbox"/> | Digipen Asterisk INWIT TCP Connection Class DDoS | 1 | 1 | Any | Block | None |

Apply

DoS Policy

Incoming Interface

port1

Source Address

all

+

X

Destination Address

all

+

X

Services

ALL

+

X

L3 Anomalies

| Name | Status | Logging | Pass | Block | Action |
|----------------|--------------------------|--------------------------|------|-------|--------|
| ip_src_session | <input type="checkbox"/> | <input type="checkbox"/> | Pass | Block | |
| ip_dst_session | <input type="checkbox"/> | <input type="checkbox"/> | Pass | Block | |

When detecting attacks, which anomaly, signature, or filter will FortiGate evaluate first?

- A. SMTP.Login.Brute.Force
- B. IMAP.Login.brute.Force
- C. ip_src_session
- D. Location: server Protocol: SMTP

Answer: B

Explanation:

When FortiGate evaluates potential attacks, the IPS sensor follows a specific processing order based on the configuration of filters, signatures, and anomaly thresholds. In this case:

- The IPS sensor is configured with IMAP.Login.brute.Force, which comes first in the order of evaluation.
- FortiGate prioritizes based on signature definitions in the sensor, and since IMAP.Login.brute.Force appears higher in the configuration, it will be evaluated before the other signatures and anomalies.

Why the other options are less appropriate:

- A. SMTP.Login.Brute.Force: This would be evaluated after IMAP.Login.brute.Force, based on the sensor configuration hierarchy.
- C. ip_src_session: This is part of the DoS policy and does not come into play until after IPS signatures are evaluated.
- D. Location: server Protocol: SMTP: This appears to be part of the broader IPS sensor rule, but it is not the first item in the evaluation chain.

NEW QUESTION 34

Consider the topology:

Application on a Windows machine <--(SSL VPN)-->FGT--> Telnet to Linux server.

An administrator is investigating a problem where an application establishes a Telnet session to a Linux

server over the SSL VPN through FortiGate and the idle session times out after about 90 minutes. The administrator would like to increase or disable this timeout.

The administrator has already verified that the issue is not caused by the application or Linux server.

This issue does not happen when the application establishes a Telnet connection to the Linux server directly on the LAN.

What two changes can the administrator make to resolve the issue without affecting services running through FortiGate? (Choose two.)

A. Set the maximum session TTL value for the TELNET service object.

B. Set the session TTL on the SSLVPN policy to maximum, so the idle session timeout will not happen after 90 minutes.

C. Create a new service object for TELNET and set the maximum session TTL.

D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy.

Answer: CD

Explanation:

The issue with the idle session timing out after 90 minutes can be resolved by adjusting the session Time-To-Live (TTL) for the TELNET service used over the SSL VPN connection. Here's how the administrator can address the problem:

- C. Create a new service object for TELNET and set the maximum session TTL:

By creating a new service object specifically for TELNET and setting a custom maximum session TTL, the administrator can ensure that the TELNET session does not time out prematurely. This way, the session will last longer or indefinitely, depending on the configured TTL.

- D. Create a new firewall policy and place it above the existing SSLVPN policy for the SSL VPN traffic, and set the new TELNET service object in the policy:

Creating a dedicated firewall policy for SSL VPN traffic and placing it above the existing one allows the administrator to apply the new TELNET service object with a longer session TTL. This will ensure the new policy with the adjusted settings takes precedence for TELNET traffic.

Why the other options are less appropriate:

- A. Set the maximum session TTL value for the TELNET service object:

This would work if you were adjusting an existing TELNET service object. However, creating a new service object for TELNET and applying it in the firewall policy (as described in options C and D) is more granular and won't affect other services using the same TELNET object.

- B. Set the session TTL on the SSLVPN policy to maximum:

While this would extend the session timeout for the entire SSL VPN traffic, it could affect other services running through the SSL VPN, which may not be desirable. This option would lack the necessary specificity for only the TELNET traffic.

NEW QUESTION 37

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

FCP_FGT_AD-7.4 Practice Exam Features:

- * FCP_FGT_AD-7.4 Questions and Answers Updated Frequently
- * FCP_FGT_AD-7.4 Practice Questions Verified by Expert Senior Certified Staff
- * FCP_FGT_AD-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * FCP_FGT_AD-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The FCP_FGT_AD-7.4 Practice Test Here](#)