



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



## **CERTIFICATION TEST**

- [CertificationTest.net](https://CertificationTest.net) - Cheap & Quality Resources With Best Support

To maintain security efficacy of its public cloud resources by using native tools, a company purchases Cloud NGFW credits to replicate the Panorama, PA-Series, and VM-Series devices used in physical data centers. Resources exist on AWS and Azure:

The AWS deployment is architected with AWS Transit Gateway, to which all resources connect

The Azure deployment is architected with each application independently routing traffic

The engineer deploying Cloud NGFW in these two cloud environments must account for the following:

Minimize changes to the two cloud environments

Scale to the demands of the applications while using the least amount of compute resources

Allow the company to unify the Security policies across all protected areas

Which two implementations will meet these requirements? (Choose two.)

- A. Deploy a VM-Series firewall in AWS in each VPC, create an IPSec tunnel between AWS and Azure, and manage the policy with Panorama.
- B. Deploy Cloud NGFW for Azure in vNET/s, update the vNET/s routing to path traffic through the deployed NGFWs, and manage the policy with Panorama.
- C. Deploy Cloud NGFW for Azure in vWAN, create a vWAN to route all appropriate traffic to the Cloud NGFW attached to the vWAN, and manage the policy with local rules.
- D. Deploy Cloud NGFW for AWS in a centralized Security VPC, update the Transit Gateway to route all appropriate traffic through the Security VPC, and manage the policy with Panorama.

**Suggested Answer: BD**

Community vote distribution

BD (100%)


 **emily\_098** 2 weeks, 4 days ago

**Selected Answer: BD**

B,D are the Correct Option

I've tried a few mock test platforms, but SkillCertExams stood out. Their content is top-notch and very similar to what you see on the actual exam.

upvoted 4 times

 **fosi130** 1 month, 2 weeks ago

**Selected Answer: BD**

it is BD

upvoted 1 times

During an upgrade to the routing infrastructure in a customer environment, the network administrator wants to implement Advanced Routing Engine (ARE) on a Palo Alto Networks firewall.  
Which firewall models support this configuration?

- A. PA-5280, PA-7080, PA-3250, VM-Series
- B. PA-455, VM-Series, PA-1410, PA-5450
- C. PA-3260, PA-5410, PA-850, PA-460
- D. PA-7050, PA-1420, VM-Series, CN-Series

**Suggested Answer: A**

*Community vote distribution*

A (100%)

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

**Selected Answer: A**

Higher series supports ARE  
upvoted 1 times

🗳️ 👤 **Mohamed\_Waly** 3 months ago

**Selected Answer: A**

The following models support the Advanced Routing Engine:

PA-7000 Series  
PA-5400 Series  
PA-5200 Series  
PA-3400 Series  
PA-3200 Series  
PA-400 Series  
VM-Series  
M-700 appliance  
M-600 appliance  
M-300 appliance  
M-200 appliance

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-networking-admin/advanced-routing>

upvoted 4 times

Which two statements apply to configuring required security rules when setting up an IPSec tunnel between a Palo Alto Networks firewall and a third-party gateway? (Choose two.)

- A. For incoming and outgoing traffic through the tunnel, creating separate rules for each direction is optional.
- B. The IKE negotiation and IPSec/ESP packets are allowed by default via the intrazone default allow policy.
- C. For incoming and outgoing traffic through the tunnel, separate rules must be created for each direction.
- D. The IKE negotiation and IPSec/ESP packets are denied by default via the interzone default deny policy.

**Suggested Answer:** CD

Community vote distribution



6ed627d 6 days, 10 hours ago

**Selected Answer:** AC

Set up a simple lab with two PA-VMs connected directly.

Configured a VPN with only the essential settings.

The Tunnel Info and IKE Info came up successfully without requiring any security policy.

So, IPSec/ESP packets are allowed by default through the intrazone-default allow policy, making it optional to create separate rules for each direction.

upvoted 2 times

jose\_traga\_japis 1 week, 5 days ago

**Selected Answer:** CD

it's CD

upvoted 1 times

bloodybeaver 2 weeks, 4 days ago

**Selected Answer:** BD

B & D is 100% correct. but would also say A is correct as you dont need to have 2 rules you could have any source & any destination. Thinking the question or answers are wrong or missing something

upvoted 1 times

fosi130 1 month, 2 weeks ago

**Selected Answer:** CD

it is CD

upvoted 2 times

1318f4b 1 month, 2 weeks ago

**Selected Answer:** AB

A: You don't have to have a separate rule for each direction of traffic, you could put all the zones in both sides of the rule, it is a best practice to separate the rules by direction but it is not required.

B: IKE and IPSEC will happen Untrust to Untrust so they will be allowed by the intrazone rule.

upvoted 3 times

mirko1976 2 months, 1 week ago

**Selected Answer:** CD



Separate Rules Must Be Created

On Palo Alto Networks firewalls, security policies are unidirectional. This means that for bi-directional communication through an IPSec VPN, you need to create two separate security rules: one for traffic entering the tunnel and another for traffic exiting the tunnel. This ensures traffic in both directions is explicitly permitted.

D. IKE and IPSec Packets Are Denied by Default

IKE negotiation (UDP 500/4500) and IPSec ESP (protocol 50) traffic does not match existing policies by default. If the tunnel interface connects different zones (e.g., "untrust" to "vpn"), and there are no explicit rules, the traffic will hit the interzone-default-deny policy and be blocked. Therefore, you must create a rule to explicitly allow IKE and IPSec traffic if needed..



upvoted 2 times

  **Kick86** 2 months, 1 week ago

**Selected Answer: BD**

B and D Correct

upvoted 1 times

  **lildevil** 1 month, 1 week ago

Your answers directly conflict one another.

upvoted 1 times

  **bloodybeaver** 2 weeks, 4 days ago

no.. im looking at my palo policies now

B: intrazone is allow by default

D: interzone is deny by default

upvoted 1 times

Which statement describes the role of Terraform in deploying Palo Alto Networks NGFWs?

- A. It acts as a logging service for NGFW performance metrics.
- B. It orchestrates real-time traffic inspection for network segments.
- C. It provides Infrastructure-as-Code (IaC) to automate NGFW deployment.
- D. It manages threat intelligence data synchronization with NGFWs.

**Suggested Answer:** C

*Community vote distribution*

C (100%)

 **Mohamed\_Waly** 3 months ago

**Selected Answer: C**

Cloud NGFW can be deployed and configured with Terraform, allowing configuration to be defined and managed as code, facilitating automated operations.

Cloud NGFW for AWS is using a dedicated Terraform provider

Cloud NGFW for Azure is leveraging the existing AzureRM provider

<https://pan.dev/terraform/docs/cloudngfw/#:~:text=Cloud%20NGFW%20can%20be%20deployed%20and%20configured%20with,Cloud%20NGFW%20Terraform>  
upvoted 1 times

By default, which type of traffic is configured by service route configuration to use the management interface?

- A. Security zone
- B. IPSec tunnel
- C. Virtual system (VSYS)
- D. Autonomous Digital Experience Manager (ADEM)

**Suggested Answer:** D

*Community vote distribution*

D (100%)

 **465c6d1** 2 months ago

**Selected Answer: D**

By default, management traffic on a Palo Alto Networks firewall is routed through the management interface. However, some specific types of traffic can be configured to use different service routes.

The service route configuration allows certain types of traffic (such as updates, logging, or management protocols) to be routed via specific interfaces.

Among the options provided:

Security zone is a logical grouping for traffic filtering, not related to service route configuration.

IPSec tunnel is a VPN mechanism, not a traffic type configured by default to use the management interface.

Virtual system (VSYS) is a logical firewall partition, not a traffic type.

Autonomous Digital Experience Manager (ADEM) is a Palo Alto Networks service that by default uses the management interface for its traffic.

Therefore, the traffic type configured by service route configuration to use the management interface by default is ADEM.

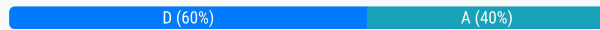
upvoted 1 times

In regard to the Advanced Routing Engine (ARE), what must be enabled first when configuring a logical router on a PAN-OS firewall?

- A. License
- B. Plugin
- C. Content update
- D. General setting

**Suggested Answer: A**

*Community vote distribution*



**wjj1982** 1 month, 2 weeks ago

**Selected Answer: A**

depends i guess if it's a brand new firewall which have no license yet. Then it required license to be implemented to support advanced routing. ./ this kind of questioning is so shit because depending on what the state of the firewall. The answer can be A or D.

upvoted 2 times

**FandleFloX** 2 months ago

**Selected Answer: D**

<https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-networking-admin/advanced-routing/enable-advanced-routing#:~:text=Select%20DeviceSetup,Advanced%20Routing.>

Select DeviceSetupManagement and edit the General Settings.

Enable Advanced Routing.

upvoted 2 times

**fepz** 2 months, 3 weeks ago

**Selected Answer: D**

Its not necessary license to use ARE

upvoted 1 times



Which two zone types are valid when configuring a new security zone? (Choose two.)

- A. Tunnel
- B. Intrazone
- C. Internal
- D. Virtual Wire

**Suggested Answer:** *AD*

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

An organization has configured GlobalProtect in a hybrid authentication model using both certificate-based authentication for the pre-logon stage and SAML-based multi-factor authentication (MFA) for user logon.

How does the GlobalProtect agent process the authentication flow on Windows endpoints?

- A. The GlobalProtect agent uses the machine certificate to establish a pre-logon tunnel; upon user sign-in, it prompts for SAML-based MFA credentials, ensuring both device and user identities are validated before granting full access.
- B. The GlobalProtect agent uses the machine certificate during pre-logon for initial tunnel establishment, and then seamlessly reuses the same machine certificate for user-based authentication without requiring MFA.
- C. Once the machine certificate is validated at pre-logon, the Windows endpoint completes MFA on behalf of the user by passing existing Windows Credential Provider details to the GlobalProtect gateway without prompting the user.
- D. GlobalProtect requires the user to log in first for SAML-based MFA before establishing the pre-logon tunnel, rendering the pre-logon certificate authentication (CA) flow redundant.

**Suggested Answer: A**

*Community vote distribution*

A (100%)

🗨️ 👤 **lildevil** 1 month, 1 week ago

**Selected Answer: A**

A is the only correct answer.

upvoted 1 times

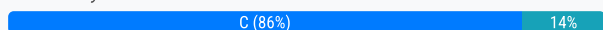
An NGFW engineer is configuring multiple Panorama-managed firewalls to start sending all logs to Strata Logging Service. The Strata Logging Service instance has been provisioned, the required device certificates have been installed, and Panorama and the firewalls have been successfully onboarded to Strata Logging Service.

Which configuration task must be performed to start sending the logs to Strata Logging Service and continue forwarding them to the Panorama log collectors as well?

- A. Modify all active Log Forwarding profiles to select the "Cloud Logging" option in each profile match list in the appropriate device groups.
- B. Enable the "Panorama/Cloud Logging" option in the Logging and Reporting Settings section under Device --> Setup --> Management in the appropriate templates.
- C. Select the "Enable Duplicate Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.
- D. Select the "Enable Cloud Logging" option in the Cloud Logging section under Device --> Setup --> Management in the appropriate templates.

**Suggested Answer: D**

*Community vote distribution*



**mirko1976** 2 months, 1 week ago

**Selected Answer: C**

When configuring Panorama-managed firewalls to send logs to both the Strata Logging Service (formerly Cortex Data Lake) and Panorama log collectors, you need to enable duplicate logging. This ensures that logs are sent to both destinations simultaneously. Strata Logging Service becomes the primary log storage once onboarded. However, if you still want logs to be available on Panorama log collectors, you must explicitly enable duplicate logging.

upvoted 2 times

**Kick86** 2 months, 1 week ago

**Selected Answer: A**

Add the log forwarding profile match list for each log type - click Add > Log Forwarding profile Match List and select the log type you want to forward. Select Panorama/Cloud Logging as the Forward Method to enable the firewalls in the device group to send logs so you can monitor the logs and generate reports from Panorama.

upvoted 1 times

**0d6e481** 2 months, 2 weeks ago

**Selected Answer: C**

For firewalls running PAN-OS 8.1 or later releases, you can opt to send logs to both the Strata Logging Service and to your Panorama and on premise log collection setup when you select Enable Duplicate Logging (Cloud and On-Premise). When enabled, the firewalls that belong to the selected Template will save a copy of the logs to both locations. You may select either Enable Duplicate Logging (Cloud and On-Premise) or Enable Strata Logging Service, but not both.

<https://docs.paloaltonetworks.com/panorama/10-2/panorama-admin/manage-log-collection/forward-logs-to-strata-logging-service>

upvoted 2 times

**ThelioNN** 2 months, 2 weeks ago

**Selected Answer: C**

C as they want to continue sending also to Panorama

upvoted 2 times

An NGFW engineer is configuring multiple Layer 2 interfaces on a Palo Alto Networks firewall, and all interfaces must be assigned to the same VLAN. During initial testing, it is reported that clients located behind the various interfaces cannot communicate with each other. Which action taken by the engineer will resolve this issue?

- A. Configure each interface to belong to the same Layer 2 zone and enable IP routing between them.
- B. Assign each interface to the appropriate Layer 2 zone and configure a policy that allows traffic within the VLAN.
- C. Assign each interface to the appropriate Layer 2 zone and configure Security policies for interfaces not assigned to the same zone.
- D. Enable IP routing between the interfaces and configure a Security policy to allow traffic between interfaces within the VLAN.

**Suggested Answer:** B

*Community vote distribution*

C (100%)

🗨️ 👤 **fepz** 2 months, 3 weeks ago

**Selected Answer: C**

the correct answer is C!

upvoted 2 times

In a Palo Alto Networks environment, GlobalProtect has been enabled using certificate-based authentication for both users and devices. To ensure proper validation of certificates, one or more certificate profiles are configured.

What function do certificate profiles serve in this context?

- A. They store private keys for users and devices, effectively allowing the firewall to issue or reissue certificates if the primary Certificate Authority (CA) becomes unavailable, providing a built-in fallback CA to maintain continuous certificate issuance and authentication.
- B. They define trust anchors (root / intermediate Certificate Authorities (CAs)), specify revocation checks (CRL/OCSP), and map certificate attributes (e.g., CN) for user or device authentication.
- C. They allow the firewall to bypass certificate validation entirely, focusing only on username / password-based authentication.
- D. They provide a one-click mechanism to distribute certificates to all endpoints without relying on external enrollment methods.

**Suggested Answer:** *B*

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

How does a Palo Alto Networks NGFW respond when the preemptive hold time is set to 0 minutes during configuration of route monitoring?

- A. It does not accept the configuration.
- B. It accepts the configuration but throws a warning message.
- C. It removes the static route because 0 is a NULL value.
- D. It reinstalls the route into the routing information base (RIB) as soon as the path comes up.

**Suggested Answer:** *D*

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

After an engineer configures an IPSec tunnel with a Cisco ASA, the Palo Alto Networks firewall generates system messages reporting the tunnel is failing to establish.

Which of the following actions will resolve this issue?

- A. Ensure that an active static or dynamic route exists for the VPN peer with next hop as the tunnel interface.
- B. Configure the Proxy IDs to match the Cisco ASA configuration.
- C. Check that IPSec is enabled in the management profile on the external interface.
- D. Validate the tunnel interface VLAN against the peer's configuration.

**Suggested Answer:** *B*

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

Which configuration in the LACP tab will enable pre-negotiation for an Aggregate Ethernet (AE) interface on a Palo Alto Networks high availability (HA) active/passive pair?

- A. Set Transmission Rate to "fast."
- B. Set passive link state to "Auto."
- C. Set "Enable in HA Passive State."
- D. Set LACP mode to "Active."

**Suggested Answer: C**

*Community vote distribution*

C (100%)

🗨️ 👤 **Mohamed\_Waly** 3 months ago

**Selected Answer: C**

[https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmleCAC&lang=en_US%E2%80%A9#:~:text=Devices%20such%20as%20PA-3000%20Series,%20PA-5000%20Series,%20and,allow%20passive%20device%20to%20engage%20in%20LACP%20pre-negotiation.)

[id=kA10g000000CmleCAC&lang=en\\_US%E2%80%A9#:~:text=Devices%20such%20as%20PA-3000%20Series,%20PA-5000%20Series,%20and,allow%20passive%20device%20to%20engage%20in%20LACP%20pre-negotiation.](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmleCAC&lang=en_US%E2%80%A9#:~:text=Devices%20such%20as%20PA-3000%20Series,%20PA-5000%20Series,%20and,allow%20passive%20device%20to%20engage%20in%20LACP%20pre-negotiation.)

upvoted 1 times



When integrating Kubernetes with Palo Alto Networks NGFWs, what is used to secure traffic between microservices?

- A. Service graph
- B. Ansible automation modules
- C. Panorama role-based access control (RBAC)
- D. CN-Series firewalls

**Suggested Answer:** D

Community vote distribution

D (100%)

🗨️ 👤 **Mohamed\_Waly** 3 months ago

**Selected Answer: D**

The CN-Series firewall is the containerized next-generation firewall that provides visibility and security for your containerized application workloads on Kubernetes clusters. The CN-Series firewall uses native Kubernetes (K8s) constructs and Palo Alto Networks components to make this possible.

<https://docs.paloaltonetworks.com/cn-series/getting-started/cn-series-firewall-for-kubernetes/cn-series-core-building-blocks#:~:text=The%20CN-Series%20firewall%20is%20the%20containerized%20next-generation%20firewall,Palo%20Alto%20Networks%20components%20to%20make%20this%20possible.>

upvoted 1 times

When configuring a Zone Protection profile, in which section (protection type) would an NGFW engineer configure options to protect against activities such as spoofed IP addresses and split handshake session establishment attempts?

- A. Flood Protection
- B. Protocol Protection
- C. Packet-Based Attack Protection
- D. Reconnaissance Protection

**Suggested Answer: B**

Community vote distribution

C (100%)

  **mirko1976** 2 months, 3 weeks ago

**Selected Answer: C**

In a Zone Protection profile, the Packet-Based Attack Protection section is specifically designed to defend against threats such as spoofed IP addresses and split handshake session establishment attempts. This section allows you to configure the firewall to drop or strip packets with undesirable characteristics across various protocols, including IP, TCP, ICMP, IPv6, and ICMPv6.

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-packet-based-attack-protection>

upvoted 3 times

  **Mohamed\_Waly** 3 months ago

**Selected Answer: C**

The firewall can drop IP packets that contain specific header options or are malformed.

Some packet-based attack protection recommendations apply somewhat equally to all organizations. For example, prevent IP address spoofing in security zones by selecting Spoofed IP address from the Packet based protection tab

upvoted 2 times

For which two purposes is an IP address configured on a tunnel interface? (Choose two.)

- A. Use of dynamic routing protocols
- B. Tunnel monitoring
- C. Use of peer IP
- D. Redistribution of User-ID

**Suggested Answer:** AB

*Community vote distribution*

AB (100%)

 **Mohamed\_Waly** 3 months ago

**Selected Answer:** AB

So the only time you actually need an IP on the tunnel interface is if you've setup tunnel monitoring, or you are using a dynamic routing protocol to route the traffic.

[https://live.paloaltonetworks.com/t5/general-topics/what-is-the-role-of-an-ip-address-on-a-tunnel-interface/td-](https://live.paloaltonetworks.com/t5/general-topics/what-is-the-role-of-an-ip-address-on-a-tunnel-interface/td-p/255523#:~:text=So%20the%20only%20time%20you%20actually%20need%20an,a%20dynamic%20routing%20protocol%20to%20route%20the%20traffic.)

[p/255523#:~:text=So%20the%20only%20time%20you%20actually%20need%20an,a%20dynamic%20routing%20protocol%20to%20route%20the%20traffic.](https://live.paloaltonetworks.com/t5/general-topics/what-is-the-role-of-an-ip-address-on-a-tunnel-interface/td-p/255523#:~:text=So%20the%20only%20time%20you%20actually%20need%20an,a%20dynamic%20routing%20protocol%20to%20route%20the%20traffic.)  
upvoted 1 times

Which PAN-OS method of mapping users to IP addresses is the most reliable?

- A. Port mapping
- B. GlobalProtect
- C. Syslog
- D. Server monitoring

**Suggested Answer: B**

*Community vote distribution*

B (100%)

🗨️ 👤 **b6940ee** 2 months, 2 weeks ago

**Selected Answer: B**

GlobalProtect authenticates the user and assigns an IP making it the most accurate method  
upvoted 1 times

🗨️ 👤 **ThelioNN** 2 months, 2 weeks ago

**Selected Answer: B**

Should be B  
upvoted 1 times

🗨️ 👤 **mirko1976** 2 months, 3 weeks ago

**Selected Answer: B**

GlobalProtect is the most reliable method for mapping users to IP addresses in PAN-OS because:

- It directly establishes a secure connection between the user's device and the firewall, allowing accurate and real-time user identification.
- It provides built-in user authentication, capturing both the IP address and the username upon connection.
- It remains consistent even if users move between networks or change IPs, making it ideal for mobile or remote users.

D. Server monitoring: Polls domain controllers for login events, but may miss logouts or fail with stale sessions.  
upvoted 1 times

In an active/active high availability (HA) configuration with two PA-Series firewalls, how do the firewalls use the HA3 interface?


- A. To forward packets to the HA peer during session setup and asymmetric traffic flow
- B. To exchange hellos, heartbeats, HA state information, and management plane synchronization for routing and User-ID information
- C. To synchronize sessions, forwarding tables, IPSec security associations, and ARP tables between firewalls in an HA pair
- D. To perform session cache synchronization among all HA peers having the same cluster ID

**Suggested Answer: A**

Community vote distribution

A (83%)

C (17%)

  **1318f4b** 1 month, 2 weeks ago

**Selected Answer: A**

A is the correct answer.

upvoted 2 times

  **FandleFlox** 2 months ago



**Selected Answer: A**

I dunno what they're thinking

[https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-](https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links#:~:text=The%20firewalls%20use%20this%20link%20for%20forwarding%20packets%20to%20the%20peer%20during%20session%20setup%20and%20asy)

[links#:~:text=The%20firewalls%20use%20this%20link%20for%20forwarding%20packets%20to%20the%20peer%20during%20session%20setup%20and%20asy](https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-links-and-backup-links#:~:text=The%20firewalls%20use%20this%20link%20for%20forwarding%20packets%20to%20the%20peer%20during%20session%20setup%20and%20asy)


upvoted 2 times

  **Kick86** 2 months, 1 week ago

**Selected Answer: C**

the HA3 interface is used for packet forwarding between the two firewalls. It's crucial for the firewalls to synchronize session tables and routing information to ensure consistent traffic processing.

upvoted 1 times

  **mirko1976** 2 months, 3 weeks ago

**Selected Answer: A**

A. To forward packets to the HA peer during session setup and asymmetric traffic flow

The HA3 interface in an Active/Active High Availability (HA) configuration is primarily used to forward packets between firewalls during session setup and asymmetric traffic flows.

Specifically, the HA3 link facilitates: Packet forwarding between Active/Active HA peers during session setup and asymmetric traffic flow.

<https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability/set-up-activeactive-ha/configure-activeactive-ha>

upvoted 2 times

A PA-Series firewall with all licensable features is being installed. The customer's Security policy requires that users do not directly access websites. Instead, a security device must create the connection, and there must be authentication back to the Active Directory servers for all sessions.

Which action meets the requirements in this scenario?

- A. Deploy the transparent proxy with Web Cache Communications Protocol (WCCP).
- B. Deploy the Next-Generation Firewalls as normal and install the User-ID agent.
- C. Deploy the Advanced URL Filtering license and captive portal.
- D. Deploy the explicit proxy with Kerberos authentication scheme.

**Suggested Answer:** *D*

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

What must be configured before a firewall administrator can define policy rules based on users and groups?

- A. User Mapping profile
- B. Authentication profile
- C. Group mapping settings
- D. LDAP Server profile

**Suggested Answer:** *C*

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

Which statement applies to the relationship between Panorama-pushed Security policy and local firewall Security policy?

- A. When a policy match is found in a local firewall policy, if any Panorama shared post-rule is configured, it will still be evaluated.
- B. Local firewall rules are evaluated after Panorama pre-rules and before Panorama post-rules.
- C. Panorama post-rules can be configured to be evaluated before local firewall policy for the purpose of troubleshooting.
- D. The order of policy evaluation can be configured differently in different device groups.

**Suggested Answer:** *B*

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



- A. DDNS
- B. Link Duplex
- C. NetFlow
- D. LLDP

### Community vote distribution



**Selected Answer: A**

Dynamic DNS (DDNS) allows a Palo Alto Networks firewall to automatically update its public IP address with a DDNS service provider.

**Selected Answer: A**

**Selected Answer: A**

Dunno what they're talking about. Just configure a layer 2 interface. There is an option for netflow profile but there is no DDNS tab under the advanced tab.  
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/monitoring/netflow-monitoring#:~:text=You%20can%20export%20NetFlow%20records%20for%20Layer%203%2C%20Layer%202%2C%20virtual%20wire%2C%20tap%2C%20VLAN>  
 upvoted 1 times

What is a result of enabling split tunneling in the GlobalProtect portal configuration with the "Both Network Traffic and DNS" option?

- A. It specifies when the secondary DNS server is used for resolution to allow access to specific domains that are not managed by the VPN.
- B. It allows users to access internal resources when connected locally and external resources when connected remotely using the same FQDN.
- C. It allows devices on a local network to access blocked websites by changing which DNS server resolves certain domain names.
- D. It specifies which domains are resolved by the VPN-assigned DNS servers and which domains are resolved by the local DNS servers.

**Suggested Answer:** *D*

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