PaloAltoNetworks.PCNSA.v2024-06-29.q230

試験コード:	PCNSA
試験名称:	Palo Alto Networks Certified Network Security Administrator
認定資格:	Palo Alto Networks
無料問題数:	230
バージョン:	v2024-06-29
アクセス数:	1151
ページビュー数:	2300
https://www.jpnpdf.com/PaloAltoNetworks.PCNSA.v2024-06-29.q230-mondaishu.html	

最新問題: **1**
An administrator creates a new Security policy rule to allow DNS traffic from the LAN to the DMZ zones.
The administrator does not change the rule type from its default value.
What type of Security policy rule is created?
A. Universal
B. Intrazone
C. Tagged
D. Interzone
Answer: A (メーッセージを残す**)**

最新問題: **2**
Which statement is true regarding a Prevention Posture Assessment?
A. The Security Policy Adoption Heatmap component filters the information by device groups, serial numbers, zones, areas of architecture, and other categories
B. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture
C. It provides a percentage of adoption for each assessment area
D. It performs over 200 security checks on Panorama/firewall for the assessment
Answer: B (メーッセージを残す**)**
Explanation
References:

最新問題: **3**
管理者は、危険なメディア コンテンツ Web サイトへのアクセスを防止したいと考えています。この目標を達成するには、どの 2 つの URL カテゴリをカスタム URL カテゴリに組み合わせる必要がありますか? (2つお選びください)

A. 娯楽と趣味
B. 既知のリスク
C. ストリーミングメディア
D. 高リスク
Answer: A,C (メーッセージを残す)

最新問題**: 4**
Why should a company have a File Blocking profile that is attached to a Security policy?
A. To block uploading and downloading of any type of files
B. To detonate files in a sandbox environment
C. To analyze file types
D. To block uploading and downloading of specific types of files
Answer: (解答を表示する)

最新問題**: 5**
An administrator would like to protect against inbound threats such as buffer overflows and illegal code execution.
Which Security profile should be used?
A. URL filtering
B. Vulnerability protection
C. Antivirus
D. Anti-spyware
Answer: (解答を表示する)

最新問題**: 6**
Which license must an Administrator acquire prior to downloading Antivirus Updates for use with the firewall?
A. Threat Prevention License
B. Threat Environment License
C. Threat Protection License
D. Threat Implementation License
Answer: A (メーッセージを残す)

最新問題**: 7**
Panorama の設定と Panorama が管理するファイアウォールを安全にバックアップするという企業要件を満たすには、新しいスケジュールされた設定エクスポートを追加するときにどのプロトコルを選択する必要がありますか?
A. SMB v3
B. FTP
C. HTTPS
D. SCP

Answer: D (メーッセージを残す)

最新問題**: 8**
パロアルトネットワーク ファイアウォールを通過するトラフィックをブロックするために使用できるインターフェイス展開方法を 3 つ選択してください。3つお選びください。）
A. 仮想ワイヤー
B. レイヤ 2
C. タップ
D. レイヤ 3
E. は
Answer: A,D,E (メーッセージを残す)

最新問題**: 9**
Which protocol is used to map usernames to user groups when User-ID is configured?
A. TACACS+
B. SAML
C. LDAP
D. RADIUS
Answer: C (メーッセージを残す)
Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

最新問題**: 10**
Which license is required to use the Palo Alto Networks built-in IP address EDLs?
A. DNS Security
B. Threat Prevention
C. WildFire
D. SD-Wan
Answer: B (メーッセージを残す)
Explanation/Reference:
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in- policy/builtin-edls.html#:~:text=With%20an%

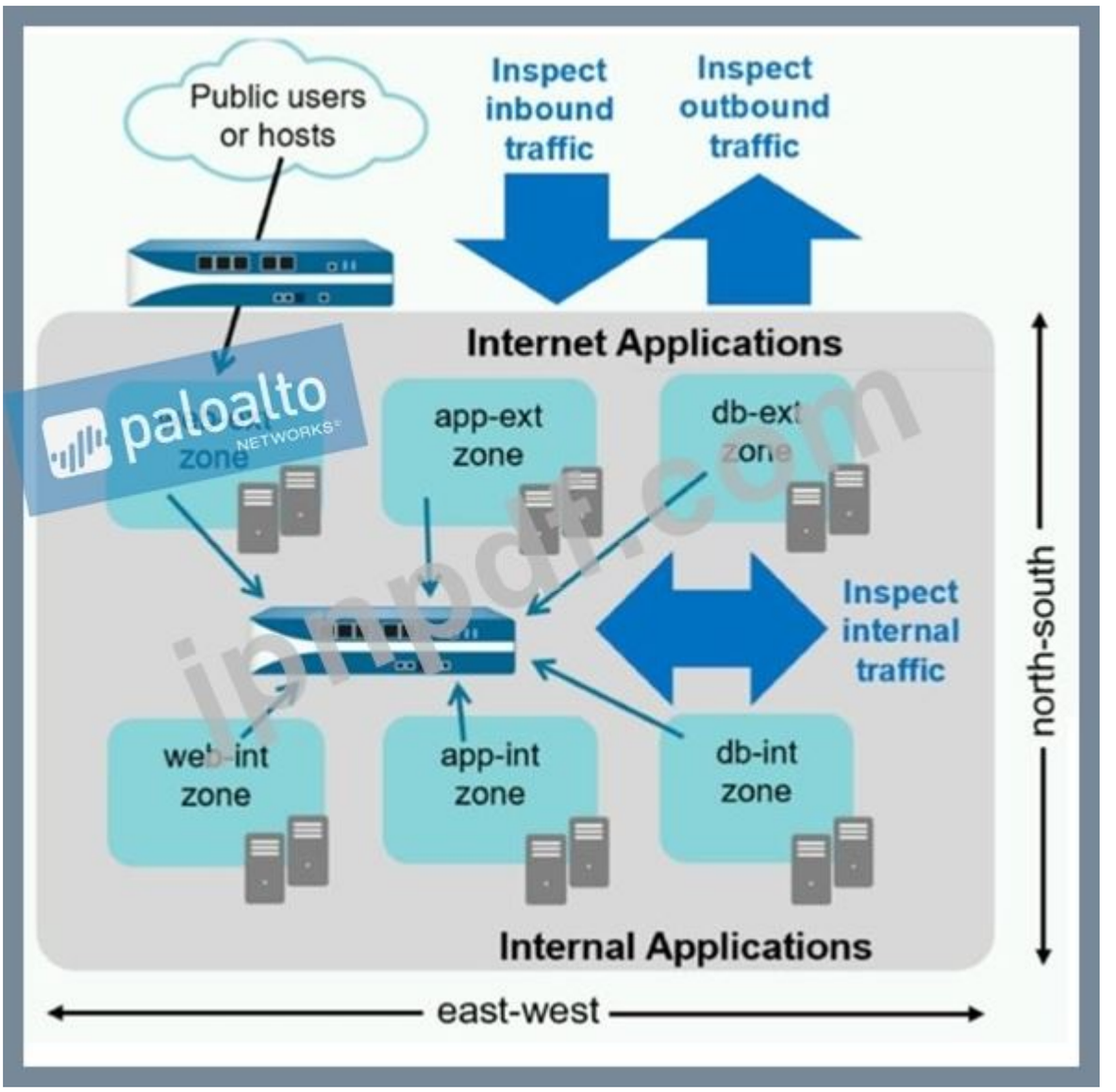
最新問題**: 11**
セキュリティ ポリシーを構成する場合、User-ID のベスト プラクティスは何ですか?
A. Limit User-ID to users registered in an Active Directory server.
B. Use only one method for mapping IP addresses to usernames.
C. エージェントがサービスを監視していないゾーンで User-ID エージェントを許可します。
D. Deny WMI traffic from the User-ID agent to any external zone.

Answer: (解答を表示する**)**

最新問題**: 12**
Which type of security rule will match traffic between the Inside zone and Outside zone, within the Inside zone, and within the Outside zone?
A. global
B. intrazone
C. interzone
D. universal
Answer: D (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

最新問題**: 13**
Facebook チャットの使用を許可する必要がある 2 つの App-ID アプリケーションはどれですか? (2つお選びください。)
A. フェイスブック
B. Facebook ベース
C. フェイスブックチャット
D. フェイスブックメール
Answer: B,C (メーッセージを残す**)**

最新問題**: 14**
管理者は、悪意のある横方向の移動アクティビティにより、ネットワーク内のトラフィックを保護する必要があることに気づきました。表示された画像に基づいて、管理者は悪意のあるアクティビティを軽減するためにどのトラフィックを監視し、ブロックする必要があるでしょうか?



A. 境界トラフィック
B. ブランチ オフィスのトラフィック
C. 南北交通
D. 東西トラフィック
Answer: D (メーッセージを残す**)**

最新問題**: 15**
An administrator is updating Security policy to align with best practices.

Which Policy Optimizer feature is shown in the screenshot below?

A. Rules without App Controls

B. New App Viewer

C. Rule Usage - Unused

D. Unused Apps

Answer: (解答を表示する**)**

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules

最新問題**: 16**

スクリーンショットによると、ĩt」というラベルが付いたユーザーのグループの目的は何ですか?

A. グループ ĩt」内のユーザーに IT アプリケーションへのアクセスを許可します

B. ĩすべての」ユーザーが DMZ ゾーン内のサーバーにアクセスできるようにします

C. グループ DMZ」内のユーザーが IT アプリケーションにアクセスできるようにします

D. ユーザーがすべてのポートで IT アプリケーションにアクセスできるようにします

Answer: A (メーッセージを残す**)**

最新問題: **17**
トラフィックがセキュリティ ポリシー ルールに一致するが、添付されたセキュリティ プロファイルが一致するトラフィックをブロックするように構成されているとします。
ファイアウォールが一致するトラフィックにアクションを適用する方法を正確に説明しているのはどれですか?
A. ブロック ルールの場合、セキュリティ プロファイル アクションは最後に適用されます
B. ブロック ルールの場合、セキュリティ ポリシー ルール アクションは最後に適用されます。
C. 許可されたルールの場合、セキュリティ プロファイル アクションは最後に適用されます。
D. 許可ルールの場合、セキュリティ ポリシー ルールが最後に適用されます。
Answer: (解答を表示する**)**

最新問題: **18**
Where in the PAN-OS GUI can an administrator monitor the rule usage for a specified period of time?
A. Objects > Schedules
B. Policies > Policy Optimizer
C. Monitor > Packet Capture
D. Monitor > Reports
Answer: B (メーッセージを残す**)**
The Policy Optimizer is a feature in the PAN-OS GUI that allows an administrator to monitor the rule usage for a specified period of time, as well as optimize the security policies based on the traffic logs and recommendations. The Policy Optimizer can help the administrator to improve the security posture, reduce the attack surface, and simplify the policy management. The Policy Optimizer can be accessed from Policies > Policy Optimizer in the PAN-OS GUI. Reference: Policy Optimizer, View Policy Rule Usage, Updated Certifications for PAN-OS 10.1

最新問題: **19**
Based on the Security policy rules shown, SSH will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. same port as ssl and snmpv3
B. any port
C. only ephemeral ports

D. the default port
Answer: D (メーッセージを残す**)**

最新問題**: 20**
パケット フロー プロセス中に、アプリケーション識別で実行される 2 つのプロセスはどれですか? (2つお選びください。)
A. パターンベースのアプリケーション識別
B. アプリケーション オーバーライド ポリシーの一致
C. セッション アプリケーションが識別されました
D. アプリケーションがコンテンツ検査から変更されました
Answer: (解答を表示する**)**
http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

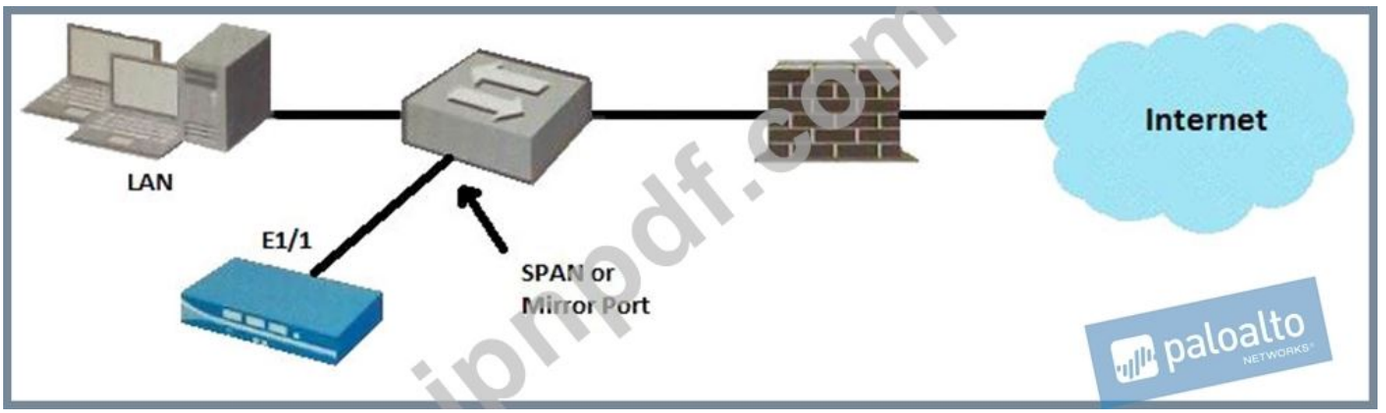
最新問題**: 21**
画像を考慮して、セキュリティ ポリシー ルールに関して正しい 2 つのオプションはどれですか。(2つお選びください。)

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	any	ftp-service...	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	facebook	Application-d...	Allow	None

A. Office プログラムを許可するルールはアプリケーション フィルターを使用しています
B. Web サーバーへの FTP を許可するルールでは、App-ID を使用した FTP が許可されています
C. Office プログラムを許可するルールはアプリケーション グループを使用しています
D. ソーシャル ネットワーキングを許可するルールで、Facebook のすべての機能を許可します。
Answer: A,D (メーッセージを残す**)**
Web サーバーへの FTP を許可するルールでは、APP-ID ではなくポートベースのルールを使用して FTP が許可されます。

最新問題**: 22**
Which object would an administrator create to enable access to all applications in the office-programs subcategory?
A. HIP profile
B. URL category
C. application filter
D. application group
Answer: C (メーッセージを残す**)**

最新問題**: 23**



Given the topology, which zone type should interface E1/1 be configured with?

A. Virtual Wire

B. Tunnel

C. Tap

D. Layer3

Answer: C (メーッセージを残す)

最新問題: **24**

The Palo Alto Networks NGFW was configured with a single virtual router named VR-1.

What changes are required on VR-1 to route traffic between two interfaces on the NGFW>

A. Add interfaces to the virtual router

B. Add zones attached to interfaces to the virtual router

C. Add a static routes to route between the two interfaces

D. Enable the redistribution profile to redistribute connected routes

Answer: (解答を表示する)

最新問題: **25**

スクリーンショットによると、ﾎ」というラベルが付いたユーザーのグループの目的は何ですか?

	Name	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application
1	allow-it	universal	inside	any	it	dmz	any	it-tools

A. グループ DMZ」内のユーザーが IT アプリケーションにアクセスできるようにします

B. ﾘすべての」ユーザーが DMZ ゾーン内のサーバーにアクセスできるようにします

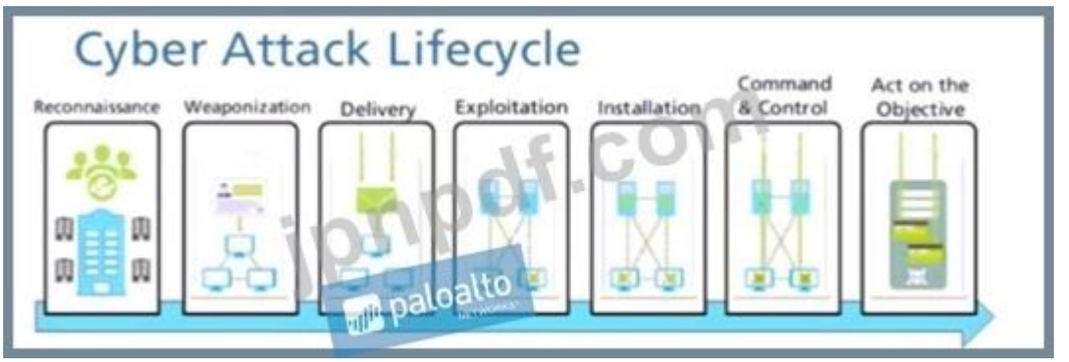
C. ユーザーがすべてのポートで IT アプリケーションにアクセスできるようにします

D. グループ ﾎ」内のユーザーに IT アプリケーションへのアクセスを許可します

Answer: D (メーッセージを残す)

最新問題: **26**

サイバー攻撃のライフサイクル図を考慮して、攻撃者が標的のマシンの脆弱性に対して悪意のあるコードを実行できる段階を特定します。

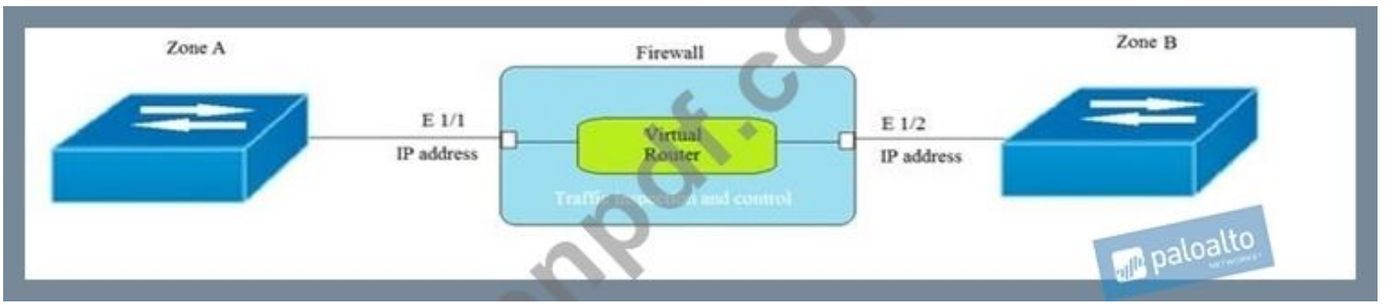


A. 偵察
B. インストール
C. エクスプロイト
D. 目標に基づいて行動する
Answer: C (メーッセージを残す**)**

最新問題**: 27**
Which table for NAT and NPTv6 (IPv6-to-IPv6 Network Prefix Translation) settings is available only on Panorama?
A. NAT Target Tab
B. NAT Active/Active HA Binding Tab
C. NAT Translated Packet Tab
D. NAT Policies General Tab
Answer: A (メーッセージを残す**)**
The NAT Target tab is a table that allows you to specify the target firewalls or device groups for each NAT policy rule on Panorama. This tab is available only on Panorama and not on individual firewalls. The NAT Target tab enables you to create a single NAT policy rulebase on Panorama and then selectively push the rules to the firewalls or device groups that require them. This reduces the complexity and duplication of managing NAT policies across multiple firewalls1. Reference: NAT Target Tab, NAT Policy Overview, NPTv6 Overview, Updated Certifications for PAN-OS 10.1.

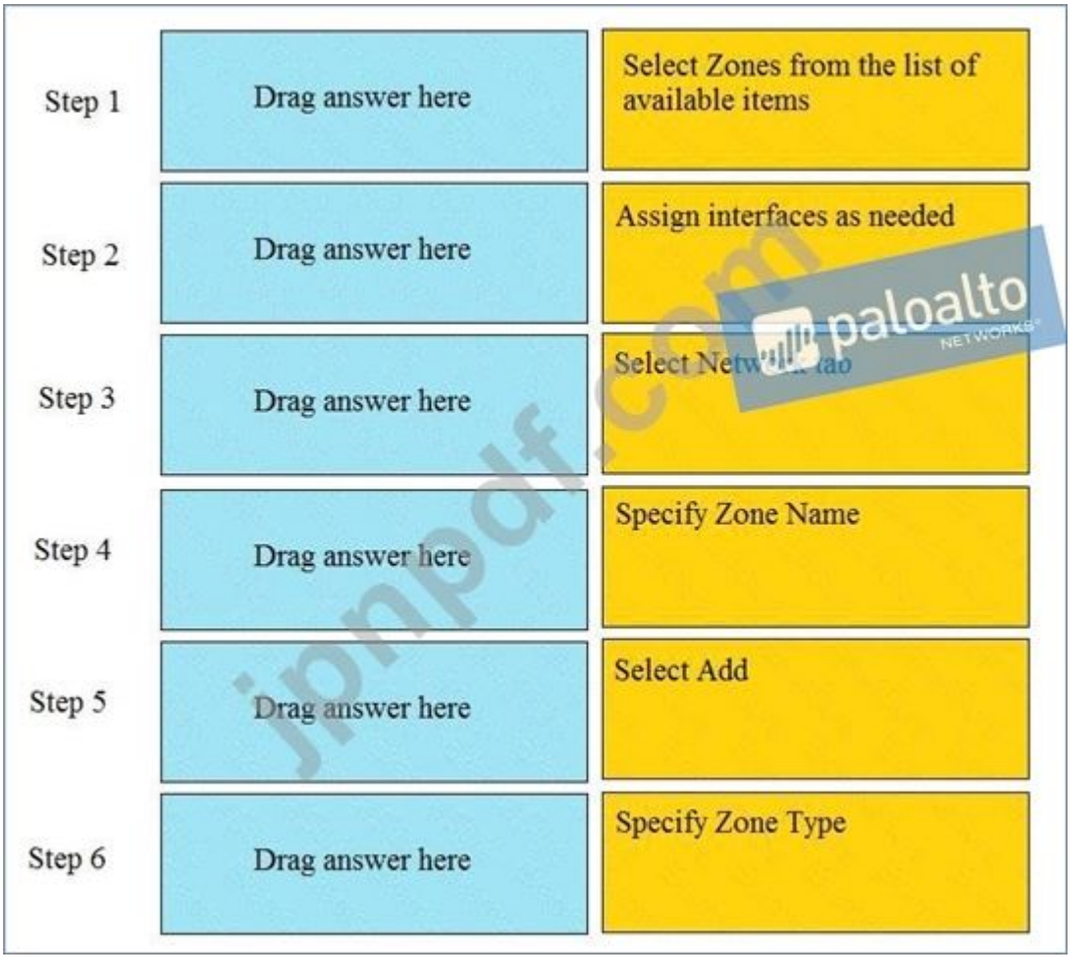
最新問題**: 28**
What is the correct process tor creating a custom URL category?
A. Objects > Custom Objects > URL Category > Add
B. Objects > Security Profiles > URL Category > Add
C. Objects > Security Profiles > URL Filtering > Add
D. Objects > Custom Objects > URL Filtering > Add
Answer: A (メーッセージを残す**)**

最新問題**: 29**
Given the topology, which zone type should zone A and zone B to be configured with?

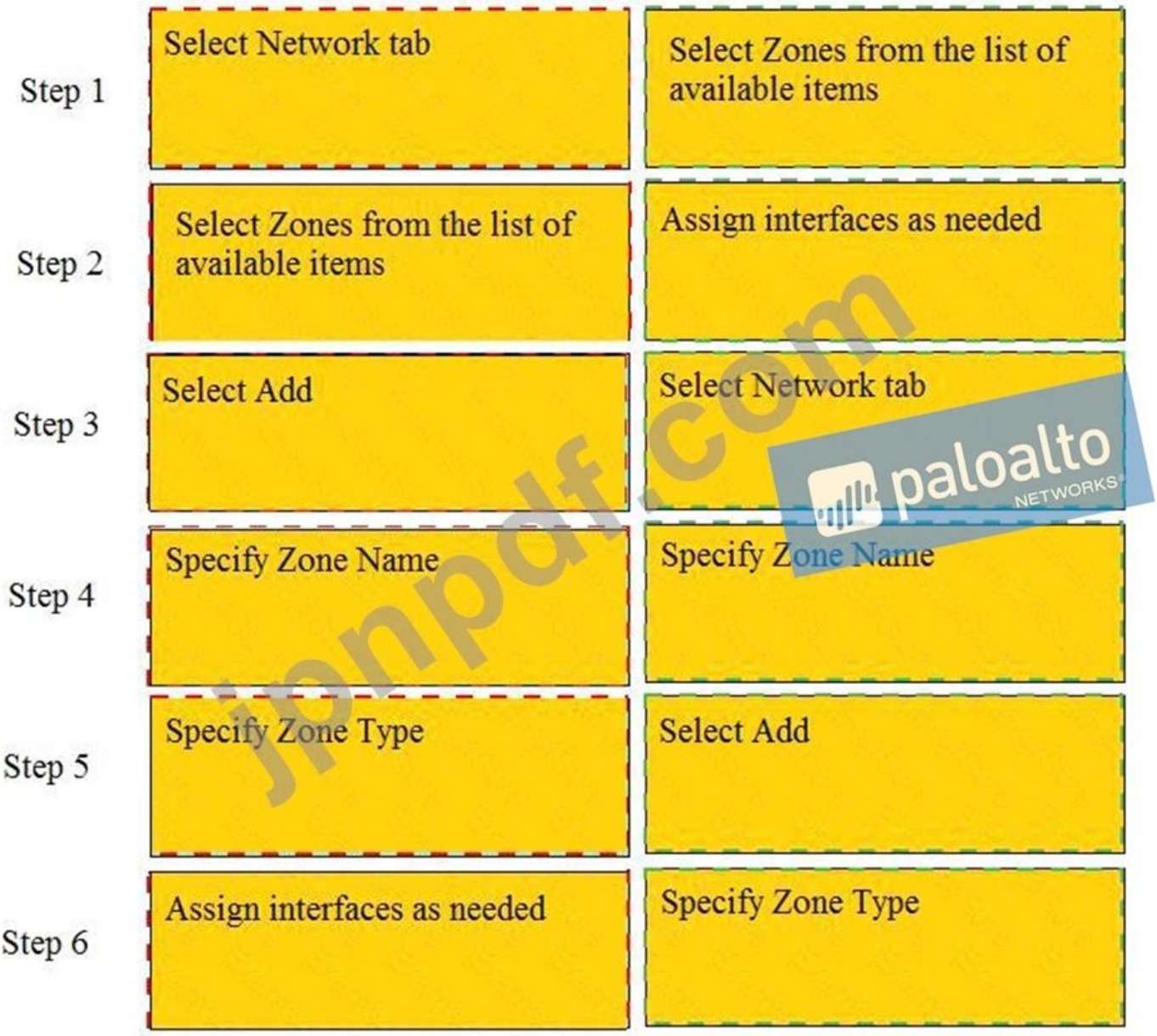


A. Virtual Wire
B. Tap
C. Layer2
D. Layer3
Answer: D (メーッセージを残す)

最新問題**: 30**
パロアルトネットワーク ファイアウォールを使用して新しいセキュリティ ゾーンを作成するために必要な手順を指示します。



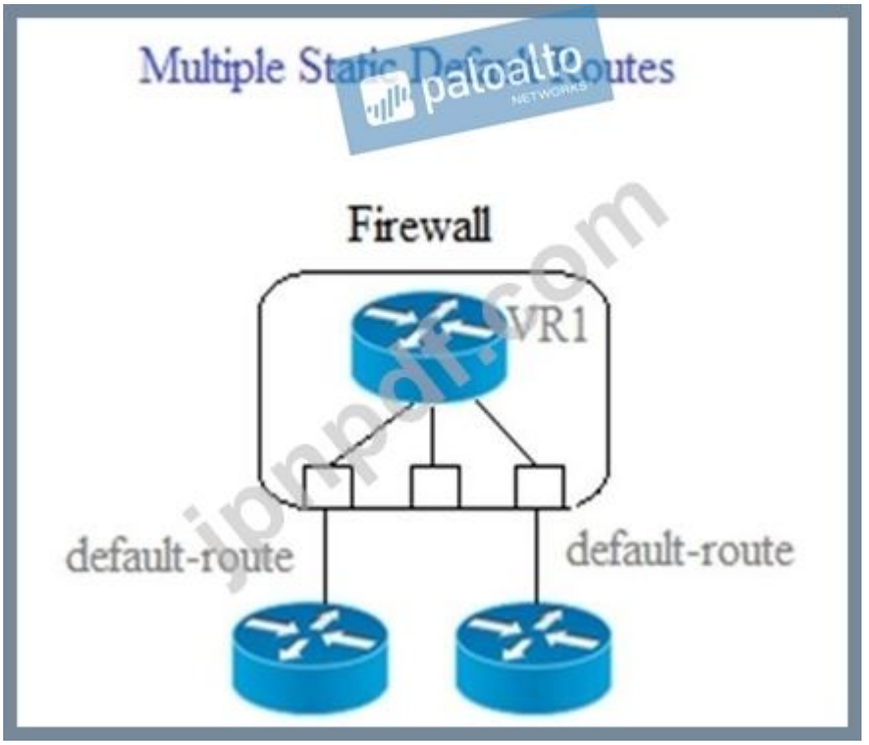
Answer:



説明
ステップ 1 - [ネットワーク] タブを選択します
ステップ 2 - 使用可能なアイテムのリストからゾーンを選択します
ステップ 3 - [追加] を選択します
ステップ 4 - ゾーン名の指定
ステップ 5 - ゾーンのタイプを指定する
ステップ 6 - 必要に応じてインターフェイスを割り当てる

最新問題: **31**
Which administrator type utilizes predefined roles for a local administrator account?
A. Device administrator
B. Role-based
C. Superuser
D. Dynamic
Answer: D (メーッセージを残す**)**

最新問題: **32**
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)



A. Path monitoring determines if route is useable
B. Route with lowest metric is actively used
C. Path monitoring does not determine if route is useable
D. Route with highest metric is actively used
Answer: A,B (メーッセージを残す**)**

最新問題: **33**
Assume a custom URL Category Object of "NO-FILES" has been created to identify a specific website.
How can file uploading/downloading be restricted for the website while permitting general browsing access to that website?
A. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate Data Filtering profile

B. Create a Security policy with a URL Filtering profile that references the site access setting of block to NO-FILES
C. Create a Security policy that references NO-FILES as a URL Category qualifier, with an appropriate File Blocking profile
D. Create a Security policy with a URL Filtering profile that references the site access setting of continue to NO-FILES
Answer: B (メーッセージを残す)

最新問題**: 34**
Based on the screenshot what is the purpose of the included groups?

			Source			Destination				
	Name	Type	Zone	Address	User	Zone	Address	Application	Service	Action
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.
B. They are used to map usernames to group names.
C. They contain only the users you allow to manage the firewall.
D. They are groups that are imported from RADIUS authentication servers.
Answer: B (メーッセージを残す)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

最新問題**: 35**
カスタム URL カテゴリ オブジェクトを作成する場合、有効なタイプはどれですか?
A. カテゴリー致
B. ドメイン一致
C. ホスト名
D. ワイルドカード
Answer: (解答を表示する)

最新問題**: 36**
ステートメントを完成させます。セキュリティ プロファイルはトラフィックをブロックまたは許可できます。
A. 不明な tcp または不明な udp トラフィック上
B. トラフィックを許可するセキュリティ ポリシーによって評価された後
C. セキュリティ ポリシーによって評価される前
D. トラフィックを許可またはブロックするセキュリティ ポリシーによって評価された後
Answer: (解答を表示する)
説明

セキュリティ プロファイルは、トラフィック フローの一致基準には使用されません。セキュリティ プロファイルは、アプリケーションまたはカテゴリがセキュリティ ポリシーによって許可された後、トラフィックのスキャンに適用されます。

最新問題: **37**
You receive notification about new malware that infects hosts through malicious files transferred by FTP.
Which Security profile detects and protects your internal networks from this threat after you update your firewall's threat signature database?
A. Antivirus profile applied to inbound Security policy rules.
B. Data Filtering profile applied to outbound Security policy rules.
C. Vulnerability Protection profile applied to outbound Security policy rules.
D. URL Filtering profile applied to inbound Security policy rules.
Answer: A (メーッセージを残す**)**

最新問題: **38**
The firewall sends employees an application block page when they try to access Youtube.
Which Security policy rule is blocking the youtube application?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. allowed-security services
B. Deny Google
C. intrazone-default
D. interzone-default
Answer: (解答を表示する**)**

最新問題: **39**
Which interface type is part of a Layer 3 zone with a Palo Alto Networks firewall?
A. Aggregation
B. High Availability
C. Aggregate
D. Management
Answer: C (メーッセージを残す**)**

最新問題: **40**

ユーザー名を IP アドレスにマッピングする 3 つの方法は何ですか？ 3つお選びください。）

A. サーバー監視

B. マインメルド

C. トラップ

D. オートフォーカス

E. ポートマッピング

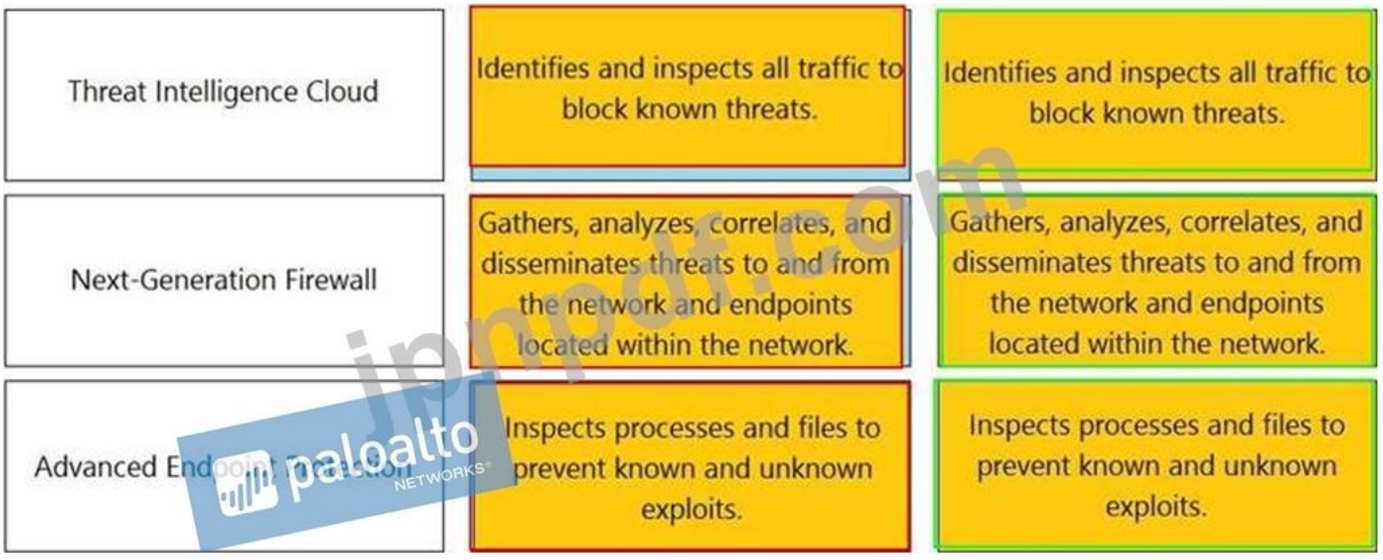
F. syslog

Answer: A,E,F (メーッセージを残す**)**

最新問題: **41**

Match each feature to the DoS Protection Policy or the DoS Protection Profile.

Answer:



最新問題: **42**

最近、ポリシーを最適化するためにファイアウォールに変更が加えられ、セキュリティ チームはそれらの変更が効果があるかどうかを確認したいと考えています。すべてのセキュリティ ポリシー ルールでヒット カウンタをゼロにリセットする最も簡単な方法は何ですか?

A. CLI でコマンド 「reset rules」を入力し、Enter キーを押します。

B. ルールを強調表示し、ルールごとに [ルール ヒット カウンターのリセット] > [選択されたルール] を使用します。

C. ファイアウォールを再起動します

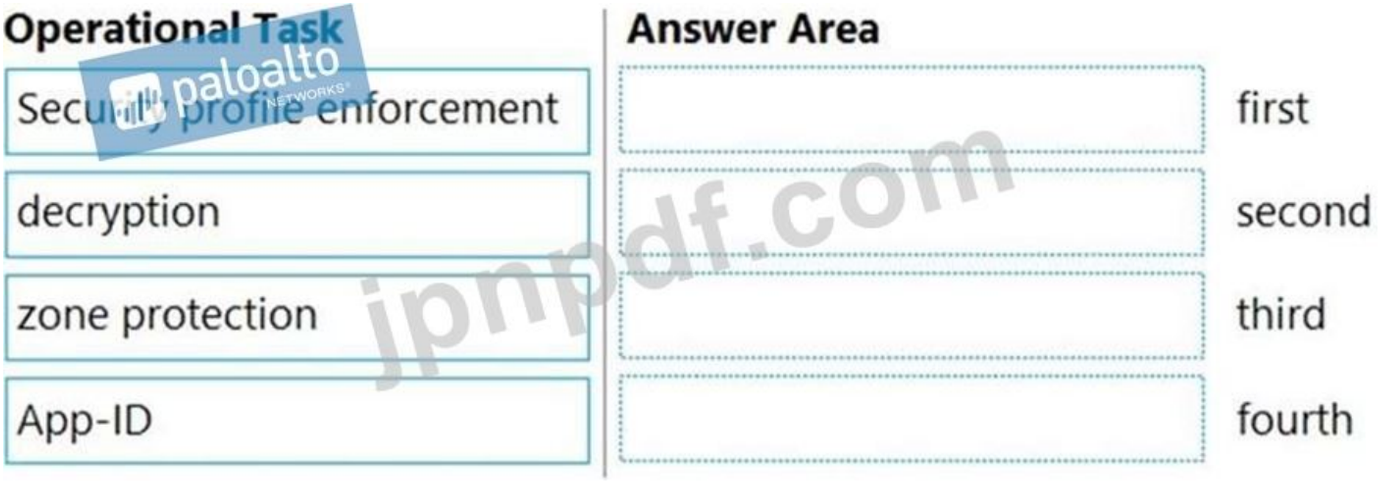
D. [ルール ヒット カウンターのリセット] > [すべてのルール] オプションを使用します。

Answer: D (メーッセージを残す)

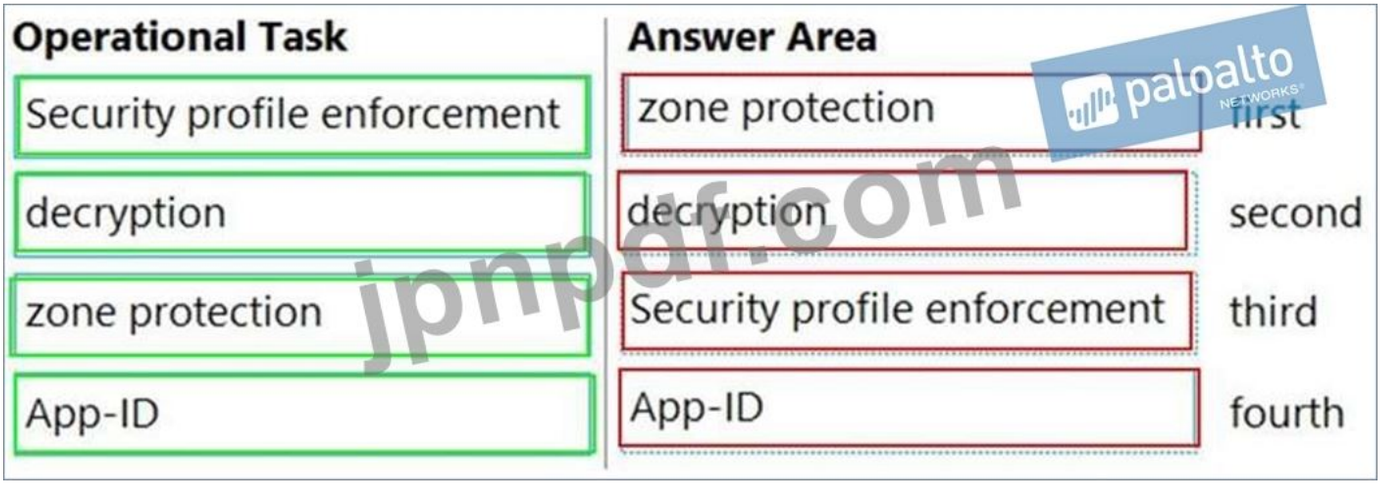
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/policies/policies-security/creating-and-managing-policies

最新問題: **43**

Place the steps in the correct packet-processing order of operations.



Answer:



最新問題: **44**

App-ID コンテンツの更新に関して正しい 2 つの記述はどれですか? (2つお選びください。)

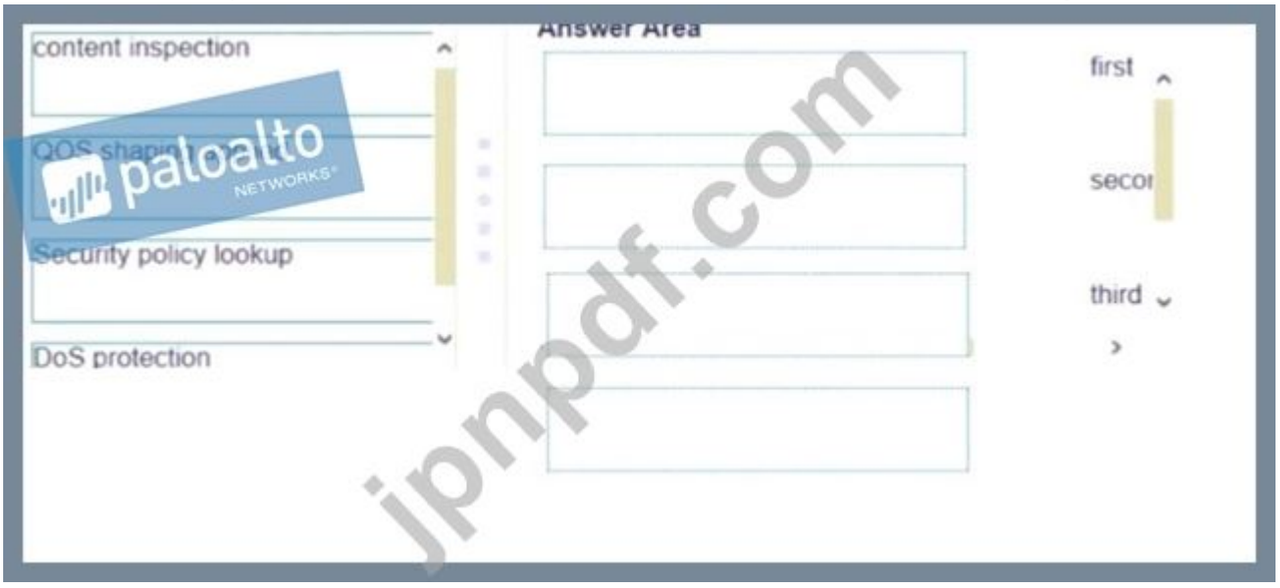
A. 更新されたアプリケーション コンテンツにより、セキュリティ ポリシー ルールの適用方法が変更される可能性があります

B. アプリケーション コンテンツの更新後、新しいアプリケーションは使用前に手動で分類する必要があります
C. 既存のセキュリティ ポリシー ルールは、アプリケーション コンテンツの更新の影響を受けません。
D. アプリケーション コンテンツの更新後、新しいアプリケーションが自動的に識別され、分類されます。
Answer: (解答を表示する**)**
新しい App-ID が導入され、毎週の更新によってファイアウォールに配信されると、フィルター基準を満たすアプリケーションの動的フィルターが自動的に更新されます。これにより、セキュリティ ポリシー管理に関連する管理労力を最小限に抑えることができます。
https://www.paloaltonetworks.com/resources/techbriefs/app-id-tech-brief.html

最新問題**: 45**
Which statement best describes the use of Policy Optimizer?
A. Policy Optimizer can display which Security policies have not been used in the last 90 days
B. Policy Optimizer can add or change a Log Forwarding profile for each Secunty policy selected
C. Policy Optimizer on a VM-50 firewall can display which Layer 7 App-ID Security policies have unused applications
D. Policy Optimizer can be used on a schedule to automatically create a disabled Layer 7 App-ID Security policy for every Layer 4 policy that exists Admins can then manually enable policies they want to keep and delete ones they want to remove
Answer: C (メーッセージを残す**)**

最新問題**: 46**
Panorama のどこにゾーン保護プロファイルを設定しますか?
A. 共有
B. テンプレート
C. デバイスグループ
D. パノラマタブ
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/use-case-configure-firewall

最新問題: 47
次のステップを、パケット処理操作の最初から最後までの順序で配置します。



Answer:

最新問題: 48
How many zones can an interface be assigned with a Palo Alto Networks firewall?
A. two
B. three
C. one
D. four
Answer: C (メーッセージを残す)

最新問題: **49**

If the firewall interface E1/1 is connected to a SPAN or mirror port, which interface type should E1/1 be configured as?

A. Layer 2

B. Tap

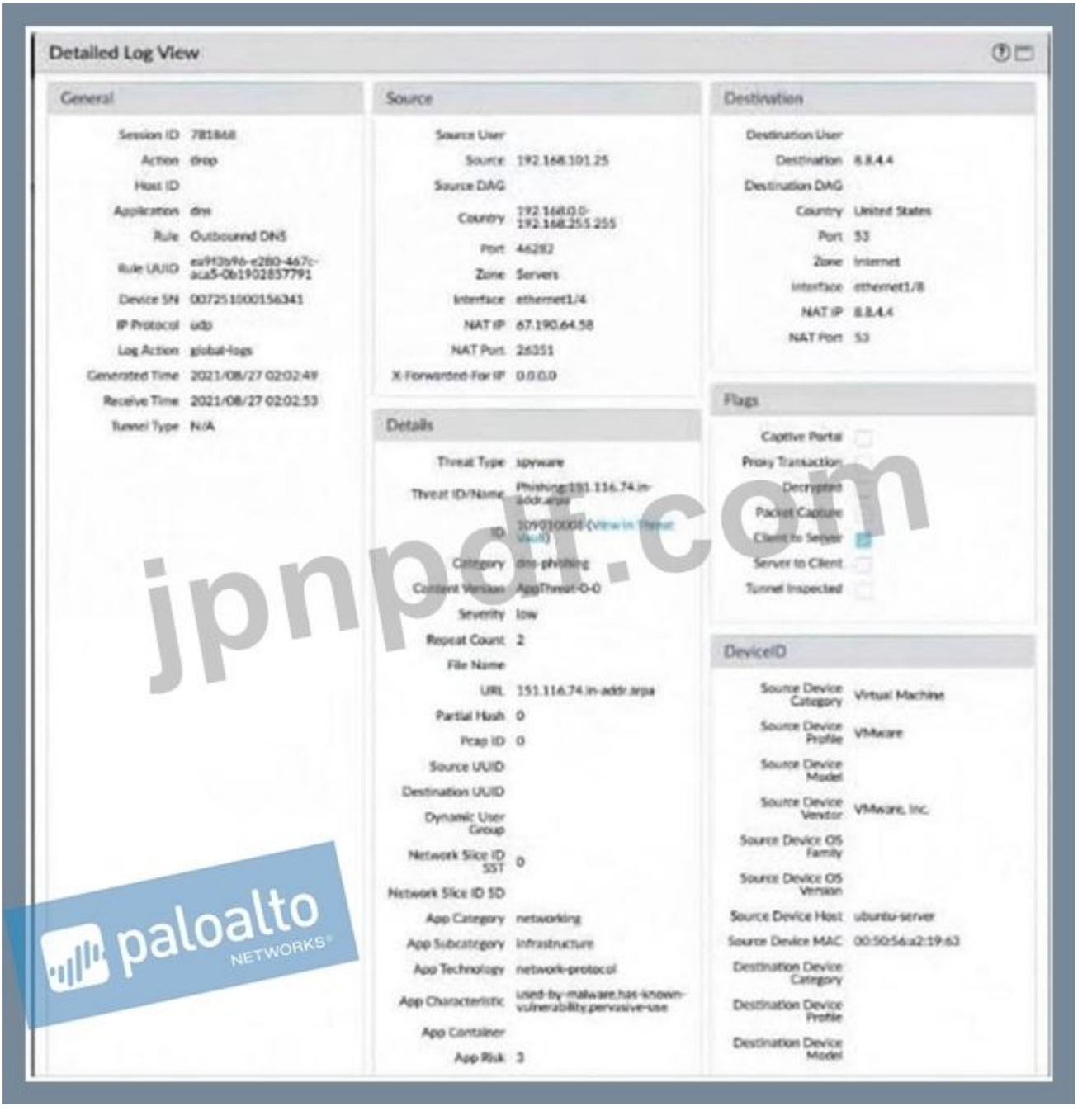
C. Virtual Wire

D. Layer 3

Answer: B (メーッセージを残す**)**

最新問題: **50**

Given the detailed log information above, what was the result of the firewall traffic inspection?



A. It was blocked by the Anti-Virus Security profile action.

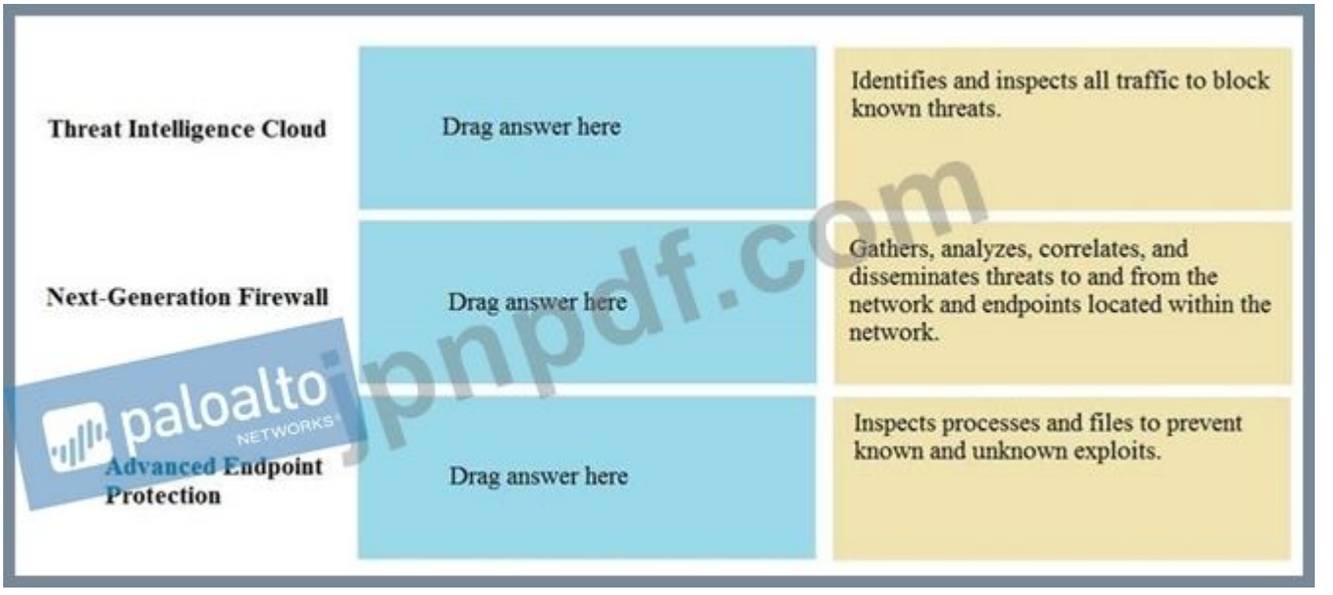
B. It was blocked by the Vulnerability Protection profile action.
C. It was blocked by the Anti-Spyware Profile action.
D. It was blocked by the Security policy action.
Answer: C (メーッセージを残す)

最新問題: **51**
In the example security policy shown, which two websites would be blocked? (Choose two.)

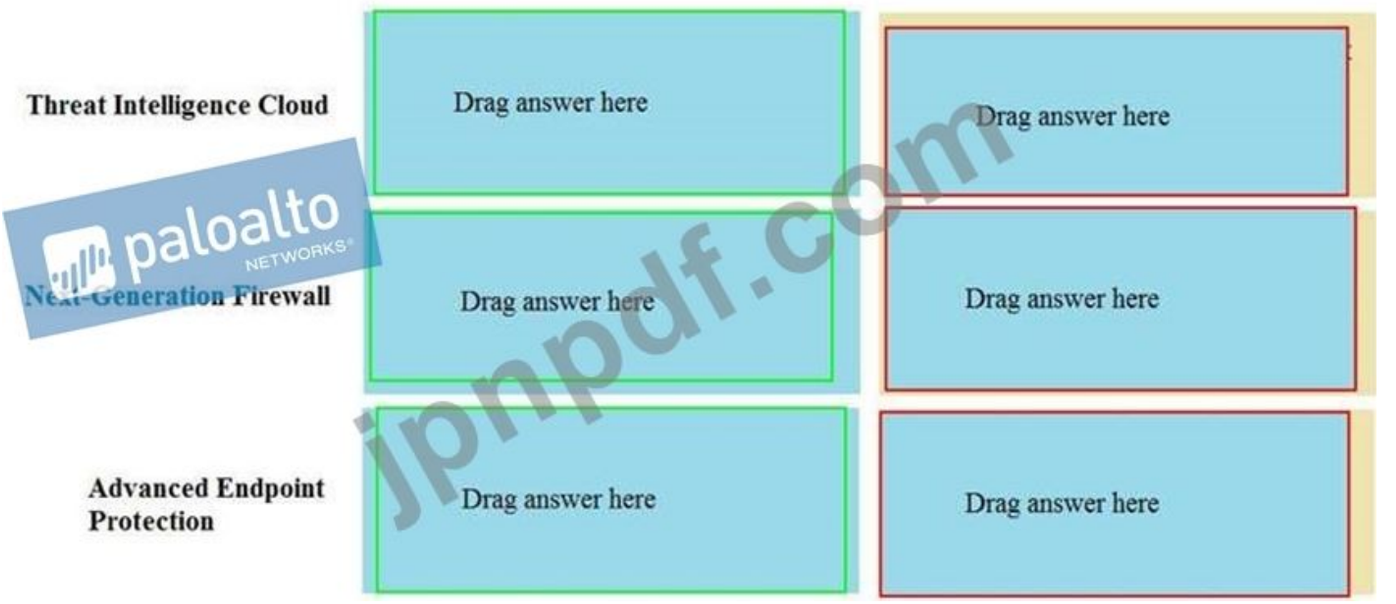
			Source		Destination						
	Name	Tags	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Block-sites	outbound	inside	any	outside	any	any	any	social-networking	Deny	none

A. Facebook
B. Amazon
C. YouTube
D. LinkedIn
Answer: (解答を表示する)

最新問題: **52**
Match the Palo Alto Networks Security Operating Platform architecture to its description.



Answer:



最新問題: **53**
アプリケーション グループ オブジェクトの機能は何ですか?
A. ポリシーで同様に扱いたいアプリケーションが含まれています
B. 定義したアプリケーション属性に基づいてアプリケーションを動的にグループ化します。
C. アプリケーションの特定のポートとプロトコルを表します。
D. ルールまたは構成オブジェクトの目的を特定し、ルールベースをより適切に整理するのに役立ちます。
Answer: A (メーッセージを残す**)**
アプリケーション グループは、ポリシー内で同様に扱う必要があるアプリケーションを含むオブジェクトです。アプリケーション グループは、組織内での使用を明示的に許可したアプリケーションへのアクセスを有効にするのに役立ちます。認可されたアプリケーションをグループ化すると、ルールベースの管理が簡素化されます。サポートするアプリケーションに変更があった場合に個々のポリシー ルールを更新する代わりに、影響を受けるアプリケーション グループのみを更新できます。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-group

最新問題: **54**
What must be configured before setting up Credential Phishing Prevention?
A. Anti Phishing Block Page
B. Threat Prevention
C. Anti Phishing profiles
D. User-ID
Answer: D (メーッセージを残す**)**
To enable credential phishing prevention, you must configure both User-ID to detect when users submit valid corporate credentials to a site (as opposed to personal credentials) and URL Filtering

to specify the URL categories in which you want to prevent users from entering their corporate credentials.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/prevent-credential-phishing

最新問題: **55**
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?

A. It defines the SSUTLS encryption strength used to protect the management interface.
B. It defines the CA certificate used to verify the client's browser.
C. It defines the certificate to send to the client's browser from the management interface.
D. It defines the firewall's global SSL/TLS timeout values.
Answer: C (メーッセージを残す**)**

最新問題: **56**

Which three Ethernet interface types are configurable on the Palo Alto Networks firewall? (Choose three.)

A. Virtual Wire

B. Tap

C. Dynamic

D. Layer 3

E. Static

Answer: (解答を表示する**)**

Palo Alto Networks firewalls support three types of Ethernet interfaces that can be configured on the firewall: virtual wire, tap, and layer 31. These interface types determine how the firewall processes traffic and applies security policies. Some of the characteristics of these interface types are:

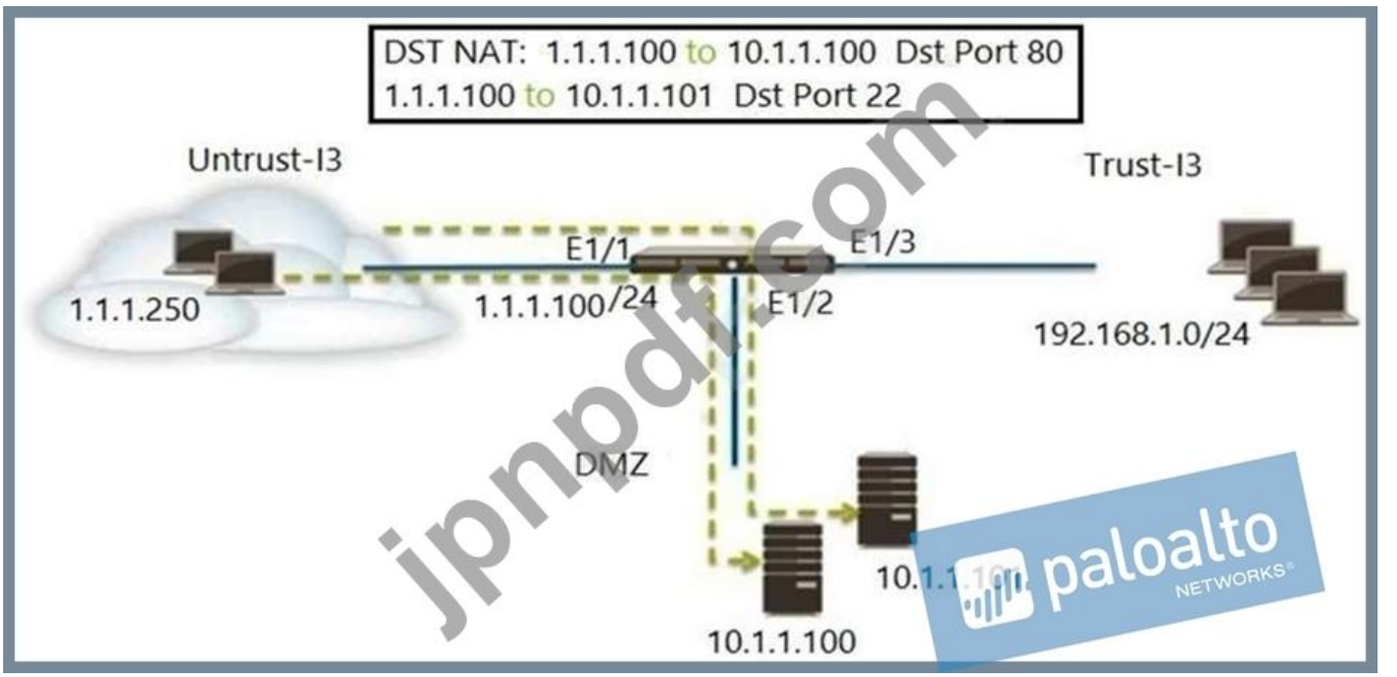
Virtual Wire: A virtual wire interface allows the firewall to transparently pass traffic between two network segments without modifying the packets or affecting the routing. The firewall can still apply security policies and inspect the traffic based on the source and destination zones of the virtual wire2.

Tap: A tap interface allows the firewall to passively monitor traffic from a network switch or router without affecting the traffic flow. The firewall can only receive traffic from a tap interface and cannot send traffic out of it. The firewall can apply security policies and inspect the traffic based on the source and destination zones of the tap interface3.

Layer 3: A layer 3 interface allows the firewall to act as a router and participate in the network routing. The firewall can send and receive traffic from a layer 3 interface and apply security policies and inspect the traffic based on the source and destination IP addresses and zones of the interface4.

最新問題**: 57**

Refer to the exhibit. An administrator is using DNAT to map two servers to a single public IP address. Traffic will be steered to the specific server based on the application, where Host A (10.1.1.100) receives HTTP traffic and Host B (10.1.1.101) receives SSH traffic.



Which two Security policy rules will accomplish this configuration? (Choose two.)

A. Untrust (Any) to DMZ (1.1.1.100), ssh - Allow

B. Untrust (Any) to DMZ (10.1.1.100, 10.1.1.101), ssh, web-browsing - Allow

C. Untrust (Any) to Untrust (10.1.1.1), ssh - Allow

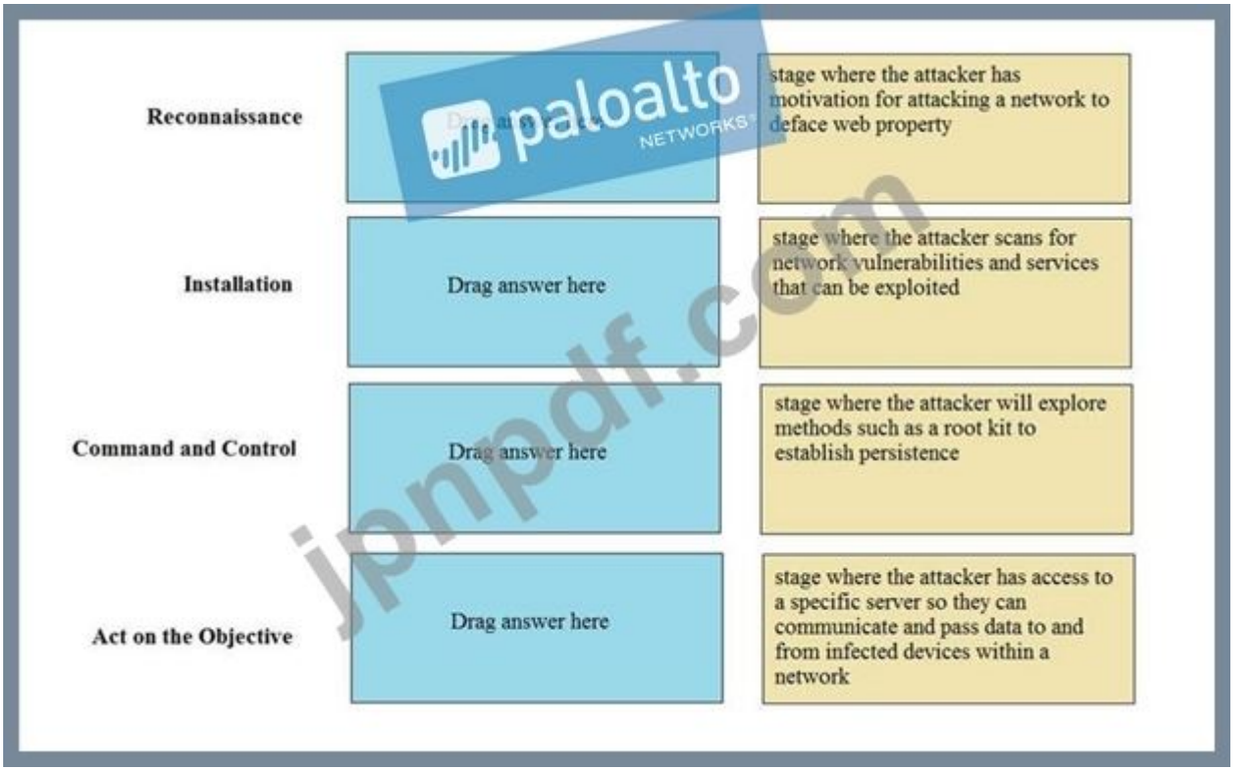
D. Untrust (Any) to DMZ (1.1.1.100), web-browsing - Allow

E. Untrust (Any) to Untrust (10.1.1.1), web-browsing - Allow

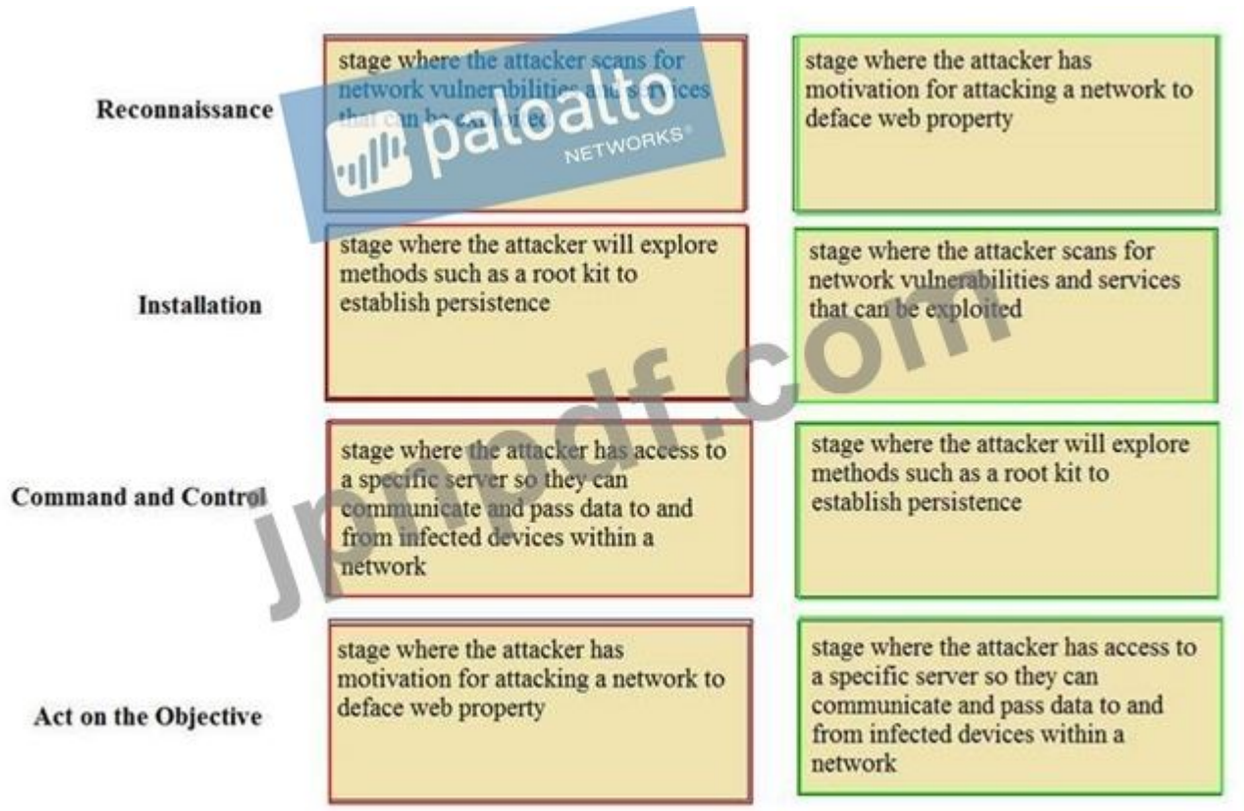
Answer: A,D (メーッセージを残す**)**

最新問題**: 58**

Match the Cyber-Attack Lifecycle stage to its correct description.

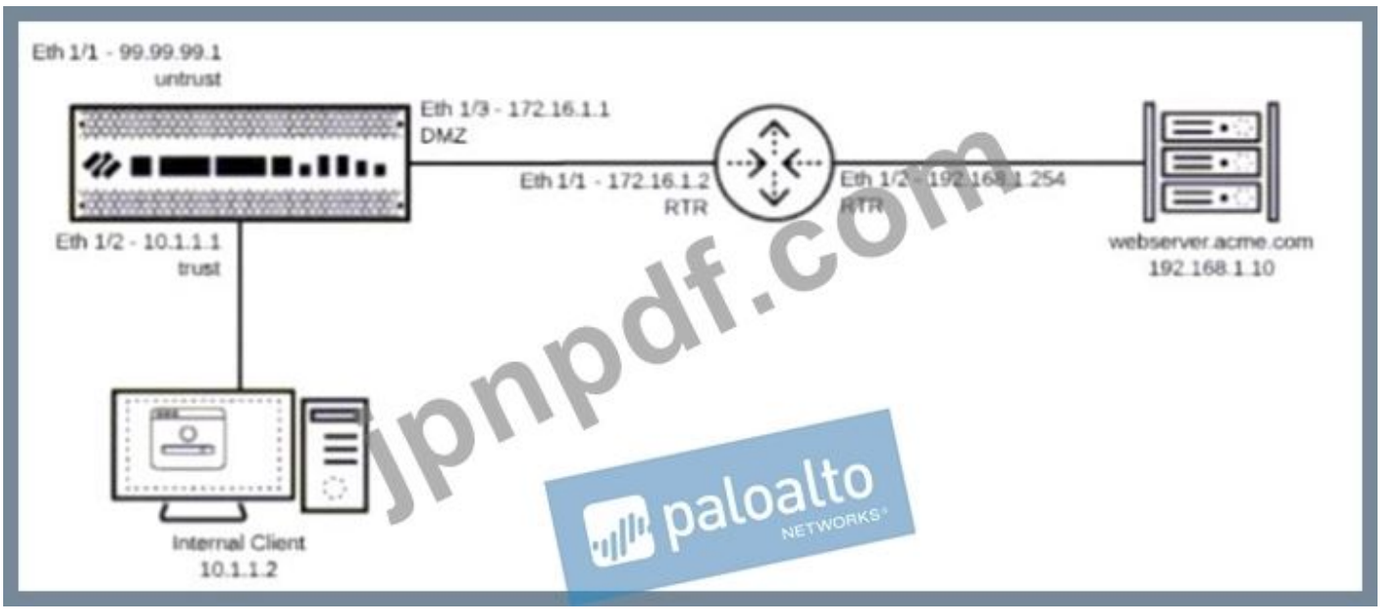


Answer:



Explanation:
Reconnaissance - stage where the attacker scans for network vulnerabilities and services that can be exploited.
Installation - stage where the attacker will explore methods such as a root kit to establish persistence Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

最新問題: 59
You have been tasked to configure access to a new web server located in the DMZ Based on the diagram what configuration changes are required in the NGFW virtual router to route traffic from the 10 1 1 0/24 network to 192 168 1 0/24?



A. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168.1.254

B. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 192.168

1.10

C. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/2 with a next-hop of 172.16.1.2

D. Add a route with the destination of 192 168 1 0/24 using interface Eth 1/3 with a next-hop of 172.16.1.2

Answer: (解答を表示する**)**

最新問題**: 60**

The data plane provides which two data processing features of the firewall? (Choose two.)

A. reporting

B. network processing

C. signature matching

D. logging

Answer: B,C (メーッセージを残す**)**

最新問題**: 61**

Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)

A. XML API

B. log forwarding auto-tagging

C. GlobalProtect agent

D. User-ID Windows-based agent

Answer: (解答を表示する**)**

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

最新問題: **62**
An administrator is reviewing the Security policy rules shown in the screenshot below.
Which statement is correct about the information displayed?

A. The view Rulebase as Groups is checked.
B. Eleven rules use the "Infrastructure* tag.
C. There are seven Security policy rules on this firewall.
D. Highlight Unused Rules is checked.
Answer: A (メーッセージを残す**)**

最新問題: **63**
Which path in PAN-OS 10.0 displays the list of port-based security policy rules?
A. Policies> Security> Rule Usage> No App Specified
B. Policies> Security> Rule Usage> Port only specified
C. Policies> Security> Rule Usage> Port-based Rules
D. Policies> Security> Rule Usage> Unused Apps
Answer: A (メーッセージを残す**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-po

最新問題: **64**

You receive notification about a new malware that infects hosts. An infection results in the infected host attempting to contact a command-and-control server.

Which Security Profile detects and prevents this threat from establishing a command-and-control connection?

A. Vulnerability Protection Profile applied to outbound Security policy rules.

B. Antivirus Profile applied to outbound Security policy rules

C. Anti-Spyware Profile applied to outbound security policies.

D. Data Filtering Profile applied to outbound Security policy rules.

Answer: (解答を表示する**)**

最新問題: **65**

Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. 23

B. 22

C. 53

D. 80

Answer: B (メーッセージを残す**)**

最新問題: **66**

Which dynamic update type includes updated anti-spyware signatures?

A. GlobalProtect Data File

B. Applications and Threats

C. PAN-DB

D. Antivirus

Answer: (解答を表示する**)**

最新問題: **67**

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which

two security profile components will detect and prevent this threat after the firewall's signature database has been updated?
(Choose two.)
A. vulnerability protection profile applied to outbound security policies
B. URL filtering profile applied to outbound security policies
C. anti-spyware profile applied to outbound security policies
D. antivirus profile applied to outbound security policies
Answer: B,C (メーッセージを残す)

最新問題: **68**
Complete the statement. A security profile can block or allow traffic_____
A. on unknown-tcp or unknown-udp traffic
B. after it is matched by a security policy that allows traffic
C. before it is matched by a security policy
D. after it is matched by a security policy that allows or blocks traffic
Answer: D (メーッセージを残す)
Explanation
Security profiles are not used in the match criteria of a traffic flow. The security profile is applied to scan traffic after the application or category is allowed by the security policy.

最新問題: **69**
An administrator is updating Security policy to align with best practices.
Which Policy Optimizer feature is shown in the screenshot below?

A. Rules without App Controls
B. New App Viewer
C. Rule Usage
D. Unused Unused Apps
Answer: C (メーッセージを残す)

最新問題: **70**

ゼロトラスト ファイアウォール展開では保護され、境界専用ファイアウォール展開では保護されないデータ フローの方向はどれですか?

A. 南北

B. 受信

C. 送信

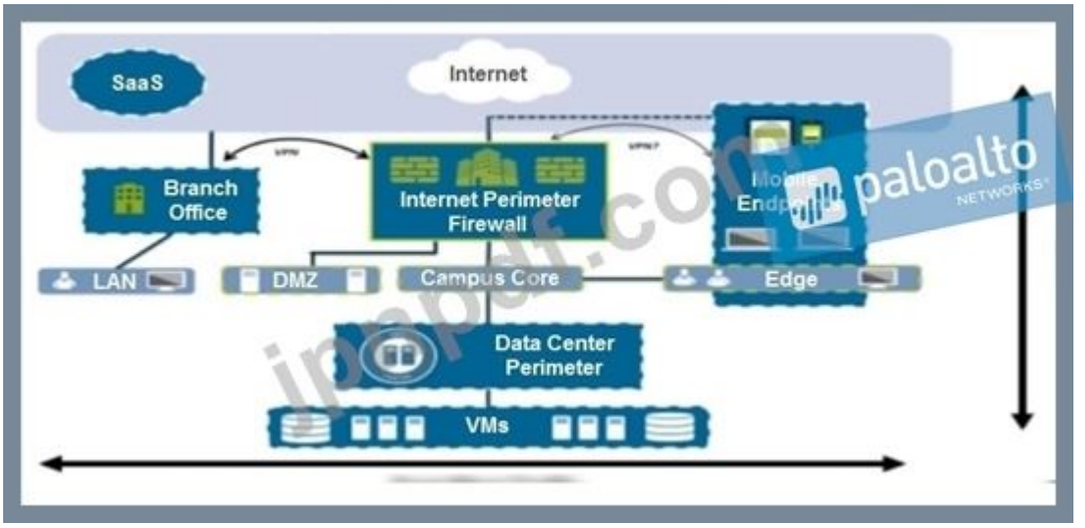
D. 東西

Answer: D (メーッセージを残す**)**

ゼロトラストは、東西を含む方向に関係なく、すべてのトラフィックを保護します。ただし、東西がカバーされていない境界のみの場合は当てはまりません。

最新問題**: 71**

An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?



A. branch office traffic

B. north-south traffic

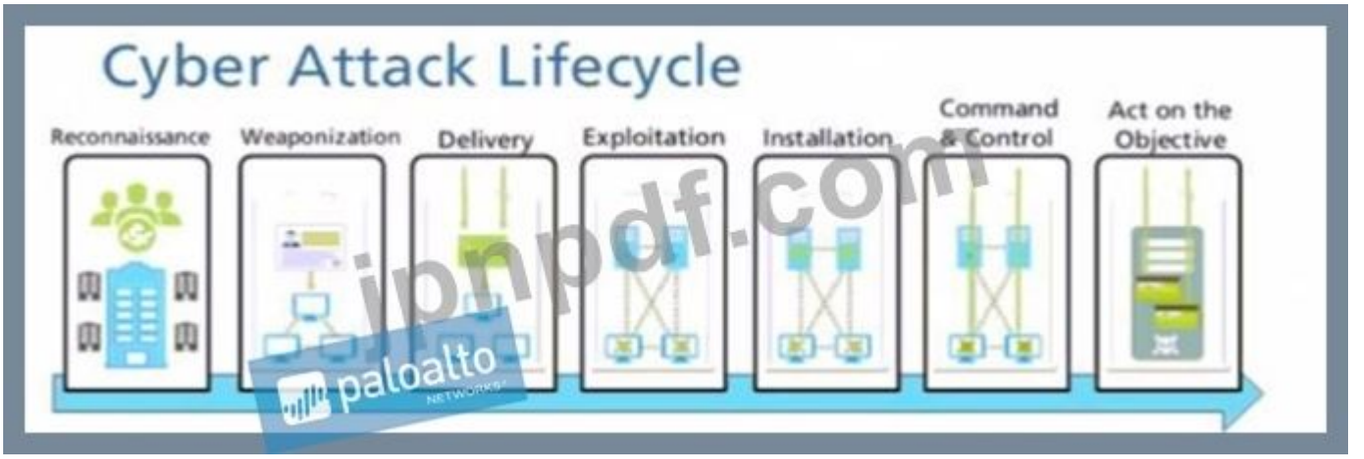
C. east-west traffic

D. perimeter traffic

Answer: C (メーッセージを残す**)**

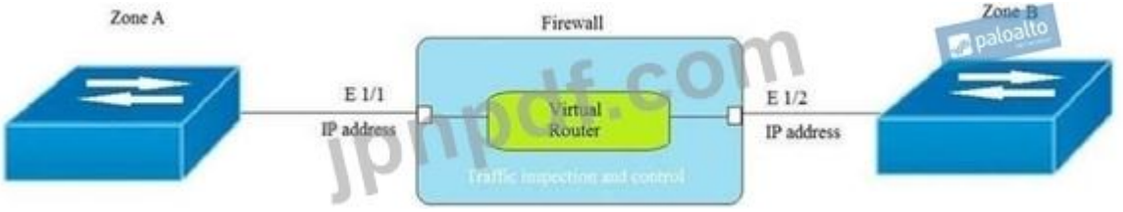
最新問題**: 72**

Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



A. Act on the Objective
B. Installation
C. Exploitation
D. Reconnaissance
Answer: C (メーッセージを残す)

最新問題: **73**
トポロジを考慮すると、ゾーン A とゾーン B をどのゾーン タイプで構成する必要がありますか?



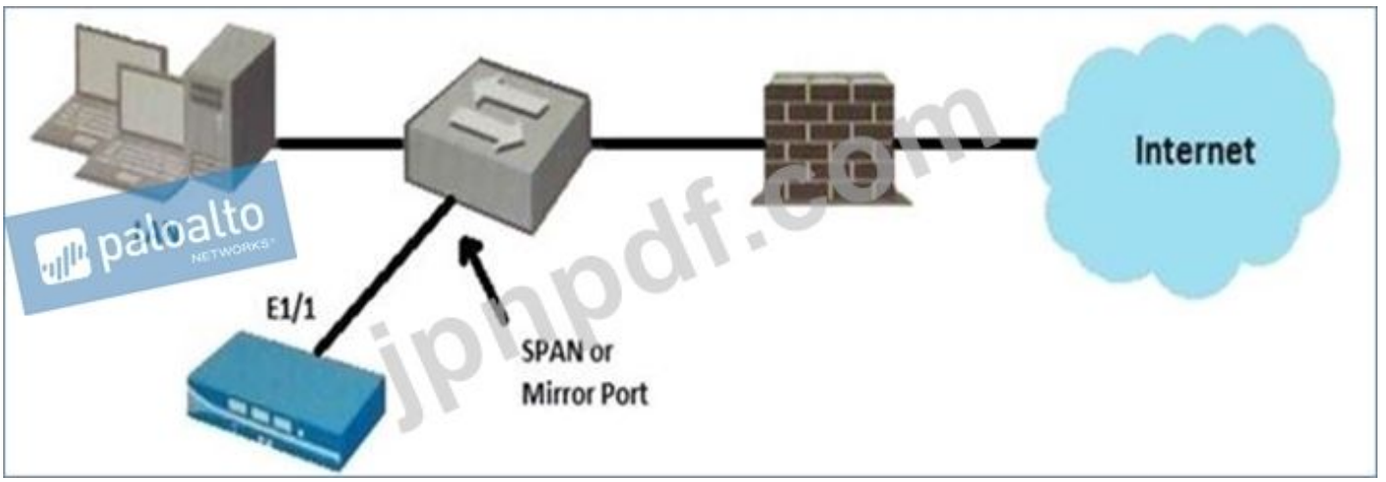
A. レイヤ 2
B. レイヤ 3
C. イーサネット
D. 仮想ワイヤー
Answer: (解答を表示する)

最新問題: **74**
What are three valid ways to map an IP address to a username? (Choose three.)
A. using the XML API
B. DHCP Relay logs
C. a user connecting into a GlobalProtect gateway using a GlobalProtect Agent
D. usernames inserted inside HTTP Headers
E. WildFire verdict reports
Answer: A,C,D (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users

最新問題: **75**
How are service routes used in PAN-OS?

A. By the OSPF protocol, as part of Dijkstra's algorithm, to give access to the various services offered in the network
B. To statically route subnets so they are joinable from, and have access to, the Palo Alto Networks external services
C. For routing, because they are the shortest path selected by the BGP routing protocol
D. To route management plane services through data interfaces rather than the management interface
Answer: (解答を表示する**)**
Service routes are a feature of PAN-OS that allows the administrator to customize the interface that the firewall uses to send requests to external services, such as DNS, email, Palo Alto Networks updates, User-ID agent, syslog, Panorama, dynamic updates, URL updates, licenses, and AutoFocus1.
By default, the firewall uses the management interface for all service routes, unless the packet destination IP address matches the configured destination service route, in which case the source IP address is set to the source address configured for the destination1.
However, in some scenarios, the administrator may want to use a different interface for service routes, such as when the management interface does not have public internet access, or when the administrator wants to isolate or monitor the traffic for certain services23.
To configure service routes, the administrator can select Device > Setup > Services > Service Route Configuration and customize each service with a source interface and a source address. The administrator can also configure destination service routes to specify a destination IP address and a gateway for each service1.
Service routes are not related to routing protocols such as OSPF or BGP, which are used to exchange routing information between routers and determine the best path to reach a network destination. Service routes are only used to change the interface that the firewall uses to communicate with external services.
Therefore, service routes are used to route management plane services through data interfaces rather than the management interface.
References:
1: Configure Service Routes - Palo Alto Networks 2: Setting a Service Route for Services to Use a Dataplane's Interface - Palo Alto Networks 3: How to Perform Updates when Management Interface does not have Public Internet Access - Palo Alto Networks

最新問題: 76



Given the topology, which zone type should you configure for firewall interface E1/1?

A. Layer3

B. Virtual Wire

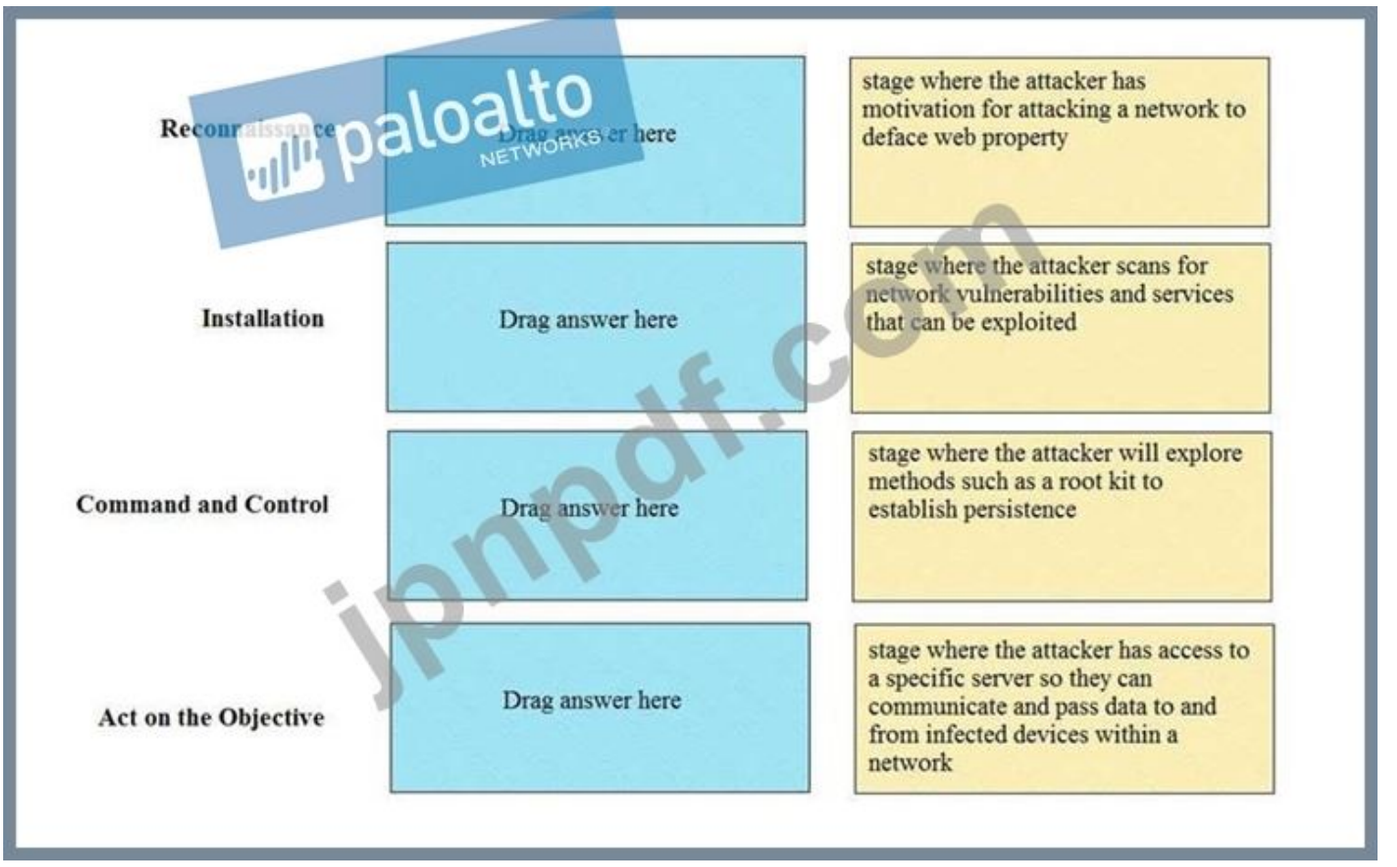
C. Tap

D. Tunnel

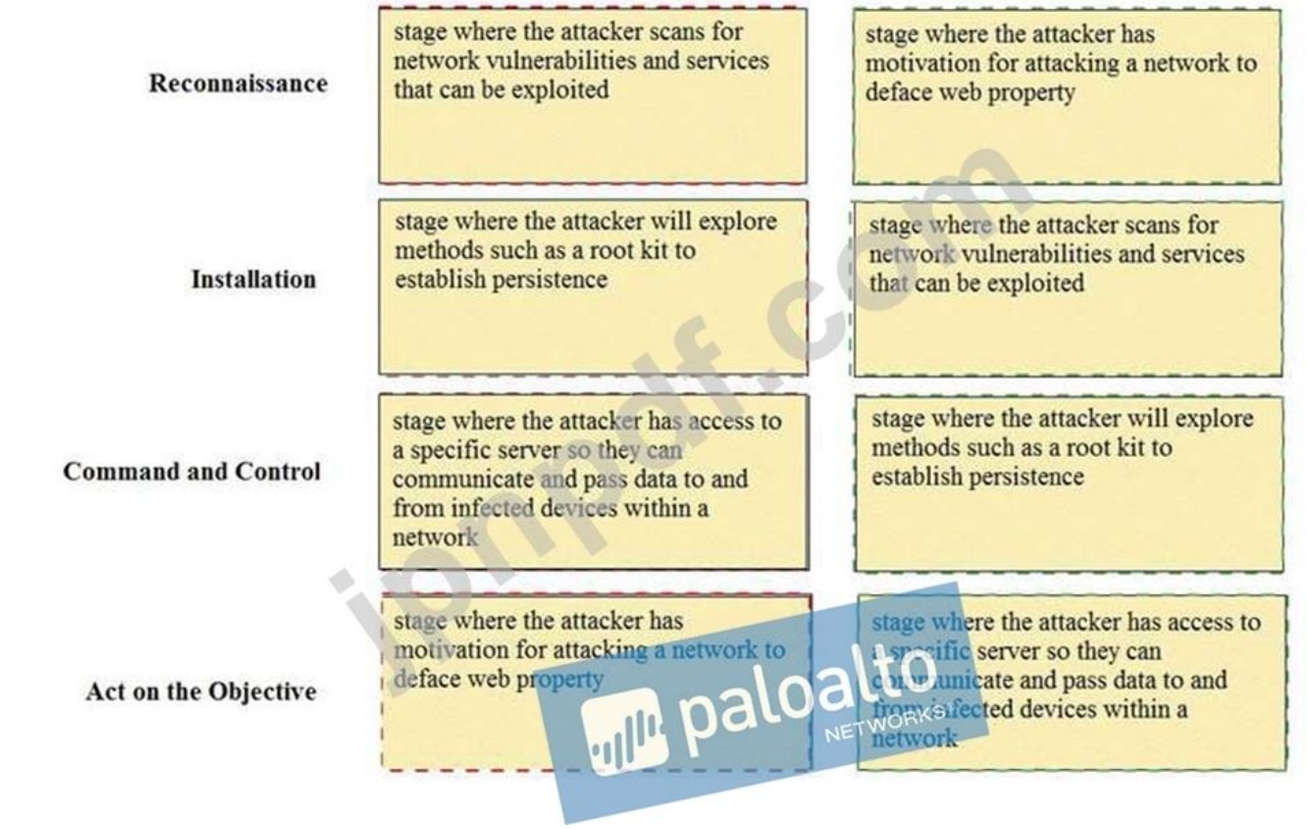
Answer: C (メーッセージを残す**)**

最新問題**: 77**

Match the Cyber-Attack Lifecycle stage to its correct description.



Answer:



Explanation:

Reconnaissance - stage where the attacker scans for network vulnerabilities and services that can be exploited.

Installation - stage where the attacker will explore methods such as a root kit to establish persistence Command and Control - stage where the attacker has access to a specific server so they can communicate and pass data to and from infected devices within a network.
Act on the Objective - stage where an attacker has motivation for attacking a network to deface web property

最新問題: **78**
Which URL Filtering Profile action does not generate a log entry when a user attempts to access a URL?
A. allow
B. block
C. continue
D. override
Answer: A (メーッセージを残す**)**

最新問題: **79**
構成ログには、どの種類のファイアウォール変更に関するエントリが表示されますか?
A. デバッグ
B. 設定
C. システムログ
D. リセット
Answer: B (メーッセージを残す**)**

最新問題: **80**
Employees are shown an application block page when they try to access YouTube. Which security policy is blocking the YouTube application?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. Deny Google
B. interzone-default
C. allowed-security services
D. intrazone-default
Answer: (解答を表示する**)**

最新問題: **81**
Palo Alto Networks ファイアウォールでは、インターフェイスにゾーンをいくつ割り当てることができますか?
A. 2
B. 3
C. 4
D. 1 つ
Answer: D (メーッセージを残す)
説明/参照: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-zones/security-zone-overview

最新問題: **82**
Which three management interface settings must be configured for functional dynamic updates and administrative access on a Palo Alto Networks firewall? (Choose three.)
A. NTP
B. IP address
C. MTU
D. DNS server
E. service routes
Answer: (解答を表示する)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClN7CAK

最新問題: **83**
Within a WildFire Analysis Profile, what match criteria can be defined to forward samples for analysis?
A. Application Category
B. Source
C. File Size
D. Direction
Answer: (解答を表示する)
A WildFire Analysis Profile allows you to specify which files or email links to forward for WildFire analysis based on the application, file type, and transmission direction (upload or download) of the traffic. The direction match criteria determines whether the file or email link was sent from the source zone to the destination zone (upload) or from the destination zone to the source zone (download). You can also select both directions to forward files or email links regardless of the direction of the traffic. Reference: Security Profile: Wildfire Analysis, Objects > Security Profiles > WildFire Analysis

最新問題: **84**

Web セッションが終了したというメッセージをユーザーのブラウザに送信するセキュリティ ポリシー アクションはどれですか?
A. 拒否
B. ドロップ
C. サーバーをリセットします
D. クライアントをリセットします
Answer: A (メーッセージを残す**)**

最新問題**: 85**
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?
A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresse

最新問題**: 86**
Which the app-ID application will you need to allow in your security policy to use facebook-chat?
A. facebook
B. facebook-base
C. facebook-chat
D. facebook-email
Answer: B,C (メーッセージを残す**)**

最新問題**: 87**
Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

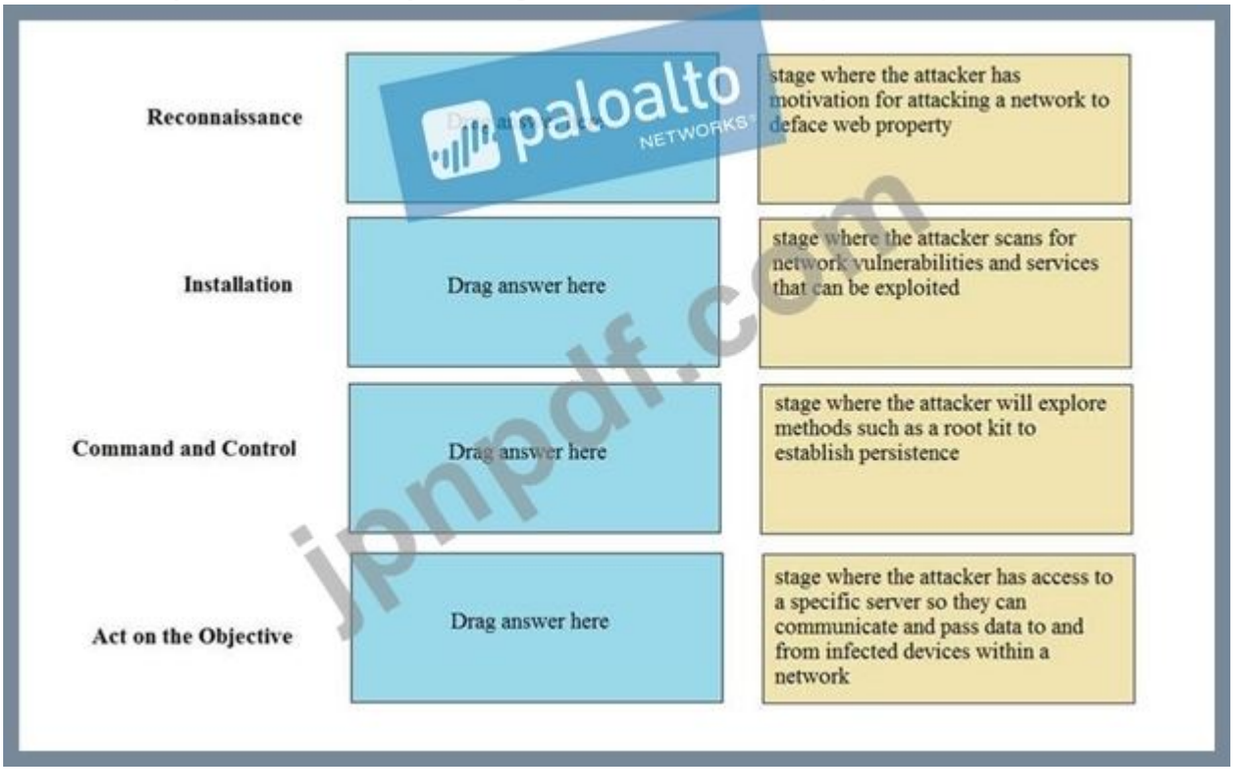
A. 23
B. 80
C. 53

D. 22

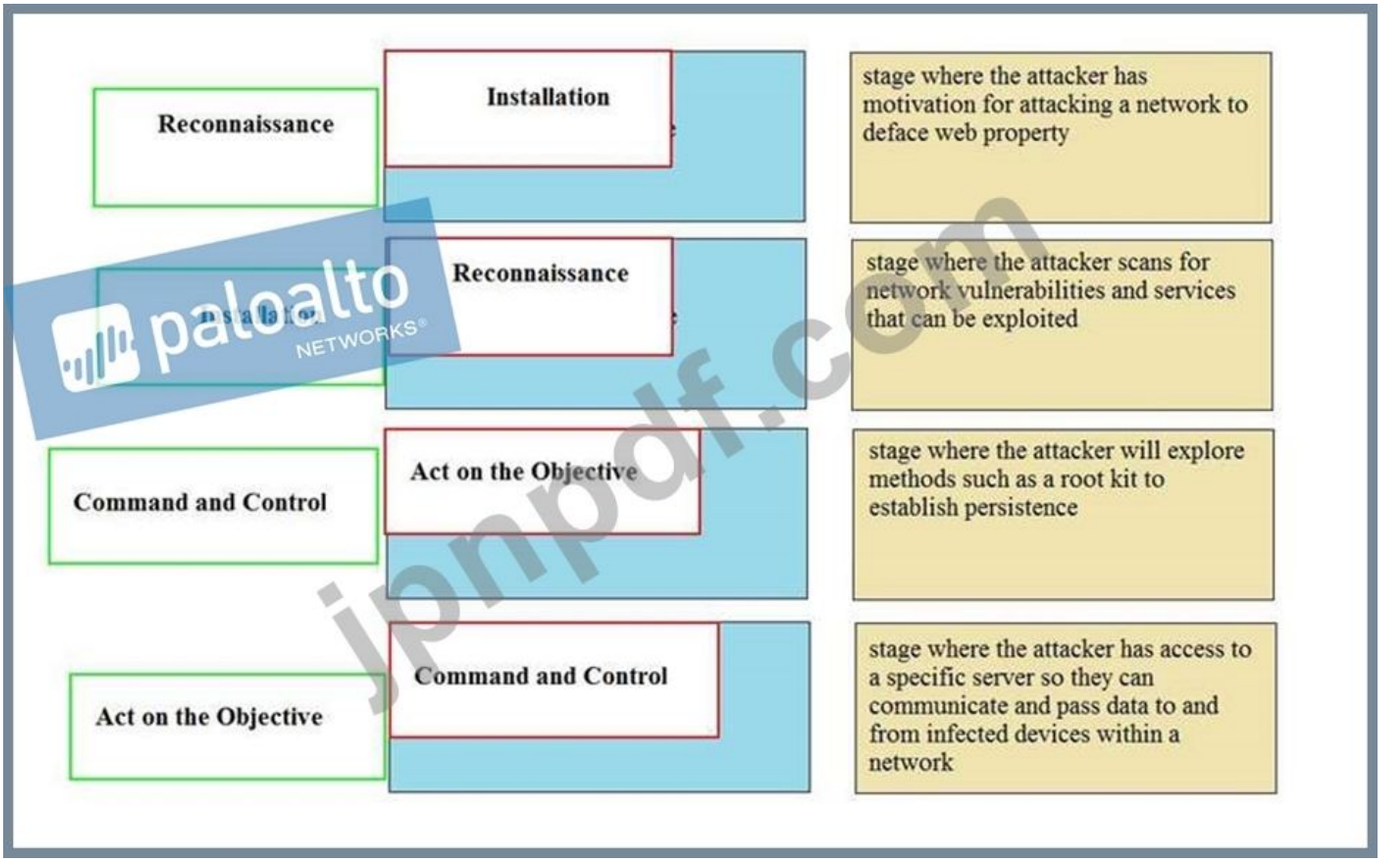
Answer: D (メーッセージを残す)

最新問題: **88**

Match the Cyber-Attack Lifecycle stage to its correct description.



Answer:

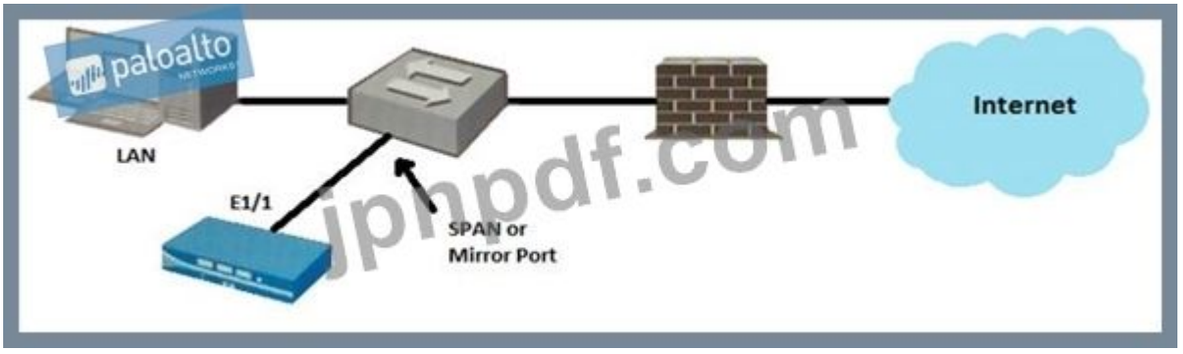


最新問題: **89**
Which three configuration settings are required on a Palo Alto Network firewall management interface? (Choose three.)
A. hostname
B. netmask
C. default gateway
D. auto-negotiation
E. IP address
Answer: B,C,E (メーッセージを残す)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIN7CAK

最新問題: **90**
Which link in the web interface enables a security administrator to view the security policy rules that match new application signatures?
A. Review Policies
B. Review Apps
C. Pre-analyze
D. Review App Matches
Answer: A (メーッセージを残す)

最新問題: **91**
What can be achieved by disabling the Share Unused Address and Service Objects with Devices setting on Panorama?
A. Increase the per-firewall capacity for address and service objects
B. Reduce the configuration and session synchronization time between HA pairs
C. Increase the backup capacity for configuration backups per firewall
D. Reduce the number of objects pushed to a firewall
Answer: D (メーッセージを残す)
Select this option (enabled by default) to share all Panorama shared objects and device-group-specific objects with managed firewalls.
If you disable this option, the appliance checks Panorama policies for references to address, address group, service, and service group objects, and does not share any unreferenced objects. This option reduces the total object count by ensuring that the appliance sends only necessary objects to managed firewalls.
If you have a policy rule that targets specific devices in a device group, then the objects used in that policy are considered used in that device group.

最新問題: **92**



Given the topology, which zone type should interface E1/1 be configured with?

A. Tunnel

B. Virtual Wire

C. Layer3

D. Tap

Answer: D (メーッセージを残す)

最新問題: **93**

During the App-ID update process, what should you click on to confirm whether an existing policy rule is affected by an App-ID update?

A. check now

B. review policies

C. test policy match

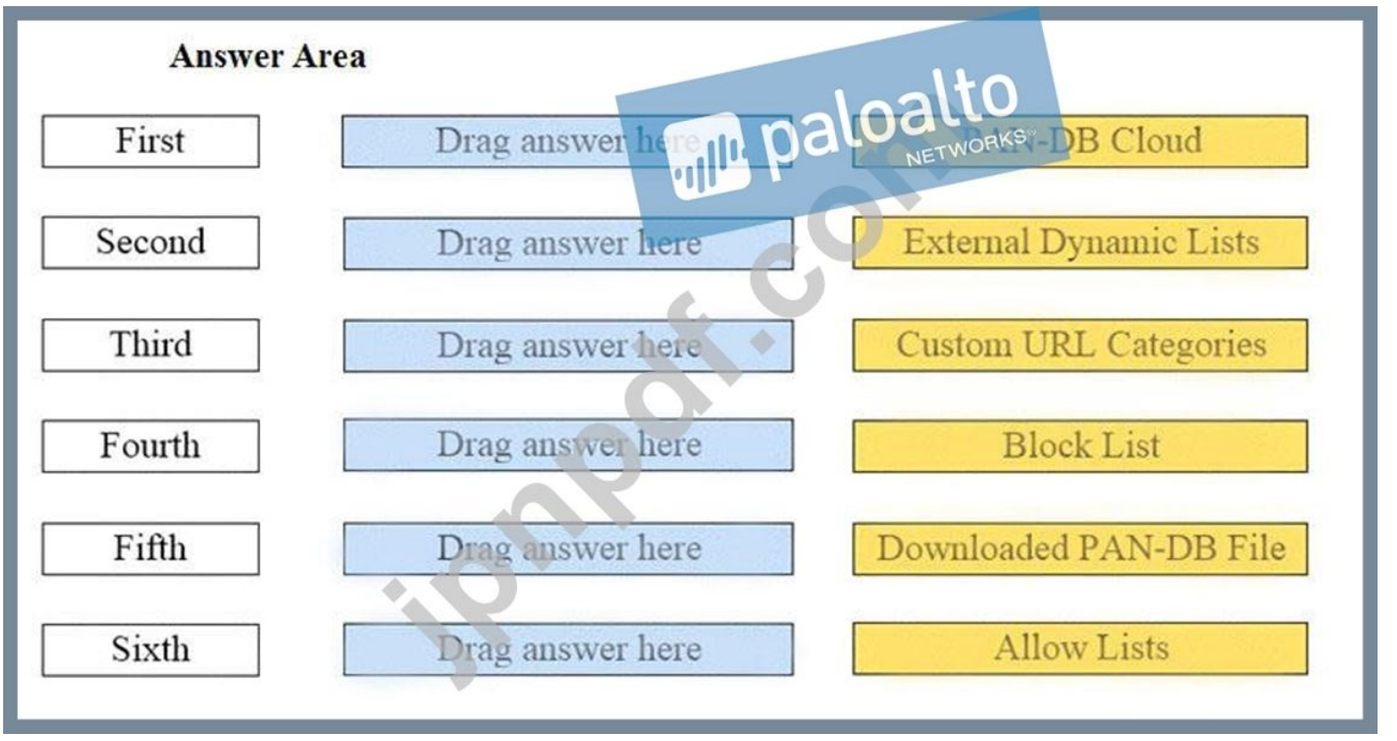
D. download

Answer: B (メーッセージを残す)

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-releases/review-new-app-id-impact-on-existing- policy-rules

最新問題: **94**

Arrange the correct order that the URL classifications are processed within the system.



Answer:

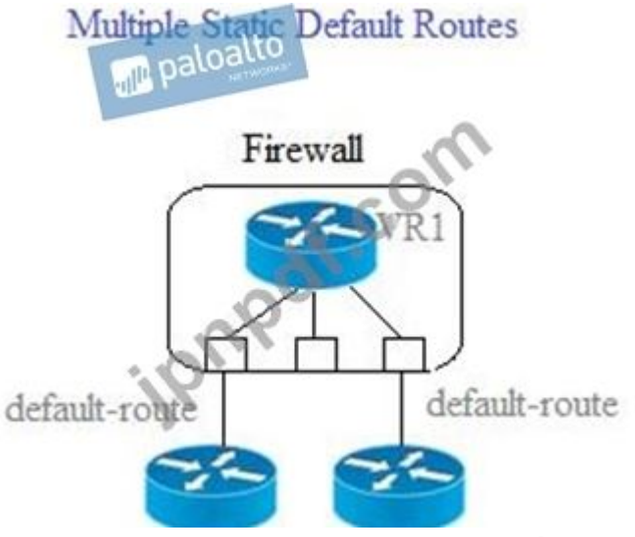
Explanation
First - Block List
Second - Allow List
Third - Custom URL Categories
Fourth - External Dynamic Lists
Fifth - Downloaded PAN-DB Files
Sixth - PAN-DB Cloud

最新問題: **95**
管理者アカウントの作成時に管理者が表示および変更できる内容を決定するためのより詳細なオプションを提供する管理者タイプはどれですか?

A. ルート
B. 動的
C. ロールベース
D. スーパーユーザー
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types#id8b324bf1-eac8-40e1-82d5-6f82ff761fa9

最新問題**: 96**
What is a recommended consideration when deploying content updates to the firewall from Panorama?
A. Before deploying content updates, always check content release version compatibility.
B. Content updates for firewall A/P HA pairs can only be pushed to the active firewall.
C. After deploying content updates, perform a commit and push to Panorama.
D. Content updates for firewall A/A HA pairs need a defined master device.
Answer: (解答を表示する**)**

最新問題**: 97**
Given the scenario, which two statements are correct regarding multiple static default routes? (Choose two.)

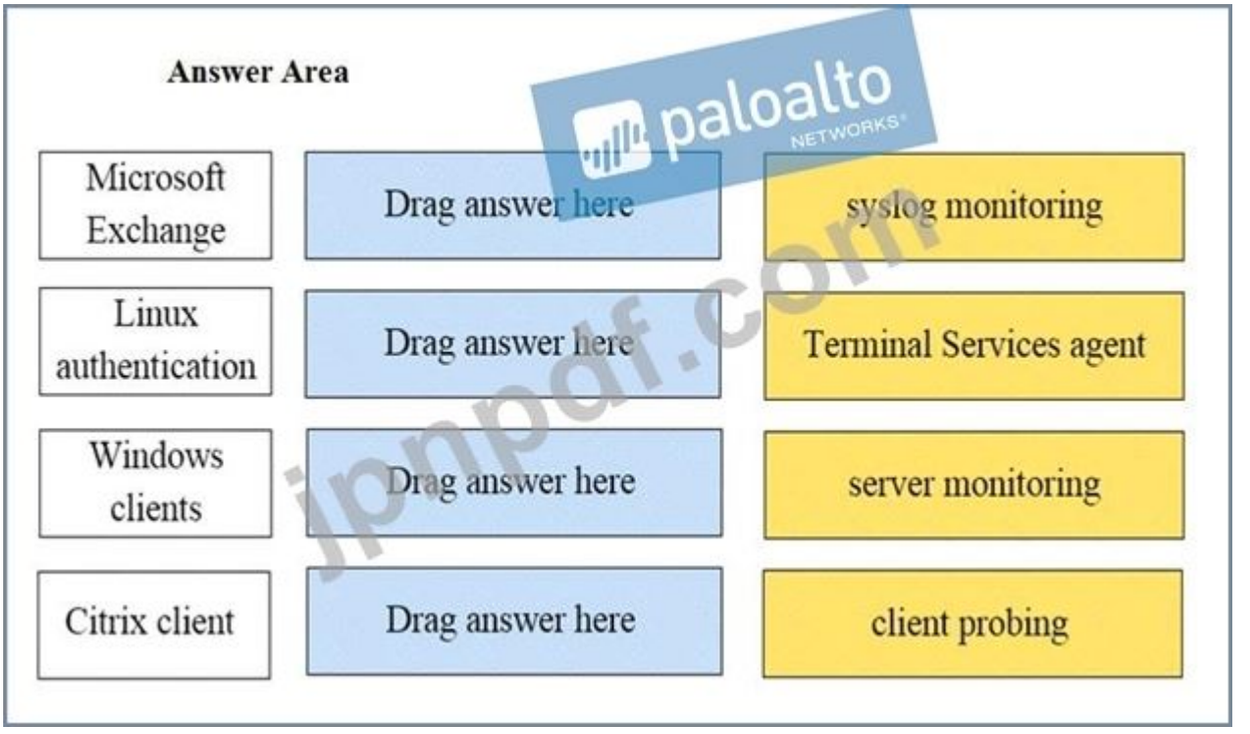


A. Path monitoring does not determine if route is useable
B. Route with highest metric is actively used
C. Path monitoring determines if route is useable
D. Route with lowest metric is actively used
Answer: (解答を表示する**)**

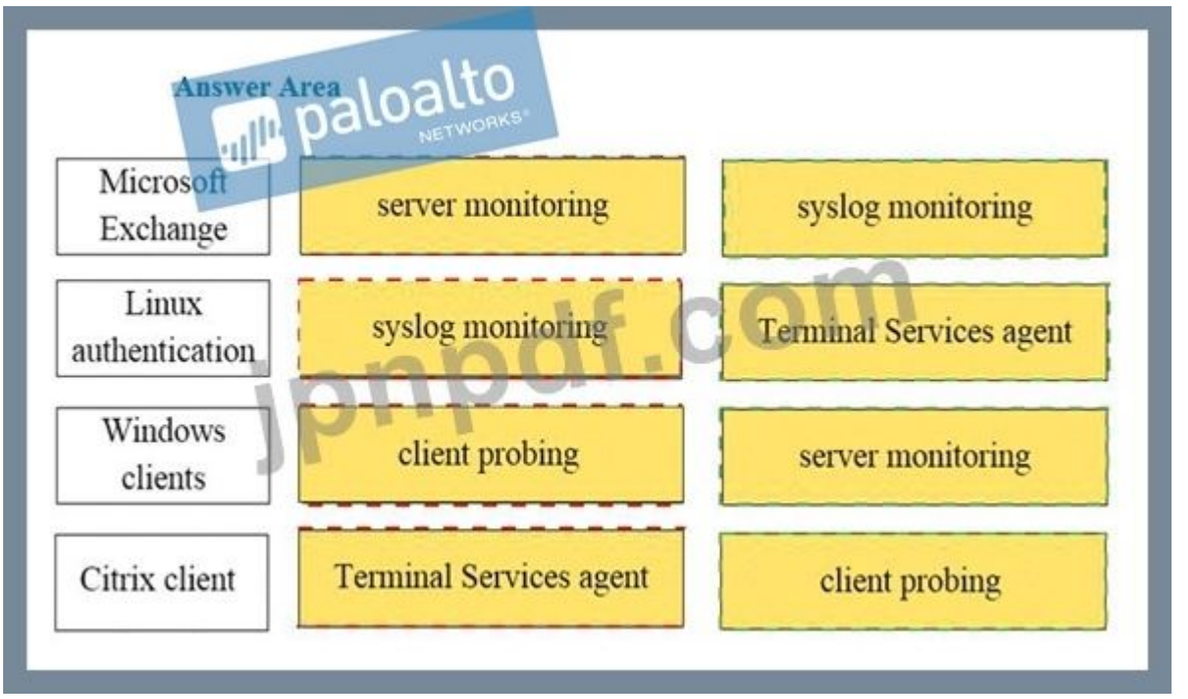
最新問題**: 98**
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?

A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory
B. Create an Application Group and add business-systems to it
C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office
Answer: A (メーッセージを残す)
Explanation
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes y
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html

最新問題: 99
Match the network device with the correct User-ID technology.



Answer:



Explanation:
Microsoft Exchange - Server monitoring
Linux authentication - syslog monitoring
Windows Client - client probing
Citrix client - Terminal Services agent

最新問題: **100**
An administrator is reviewing another administrator s Security policy log settings.
Which log setting configuration is consistent with best practices tor normal traffic?
A. Log at Session Start and Log at Session End both enabled
B. Log at Session Start disabled Log at Session End enabled
C. Log at Session Start enabled Log at Session End disabled
D. Log at Session Start and Log at Session End both disabled
Answer: B (メーッセージを残す**)**

最新問題: **101**
Based on the graphic, which statement accurately describes the output shown in the Server Monitoring panel?

A. The User-ID agent is connected to a domain controller labeled lab-client.

B. The host lab-client has been found by the User-ID agent.

C. The host lab-client has been found by a domain controller.

D. The User-ID agent is connected to the firewall labeled lab-client.

Answer: (解答を表示する**)**

lab-client is not a host, it is the name we are giving to the agent that is connecting to the specified domain controller (Active Directory).

最新問題**: 102**

アプリケーション フィルターを設定するときに選択できる属性をリストするオプションはどれですか?

A. カテゴリ、サブカテゴリ、テクノロジー、リスク、および特性

B. カテゴリ、サブカテゴリ、テクノロジー、および特性

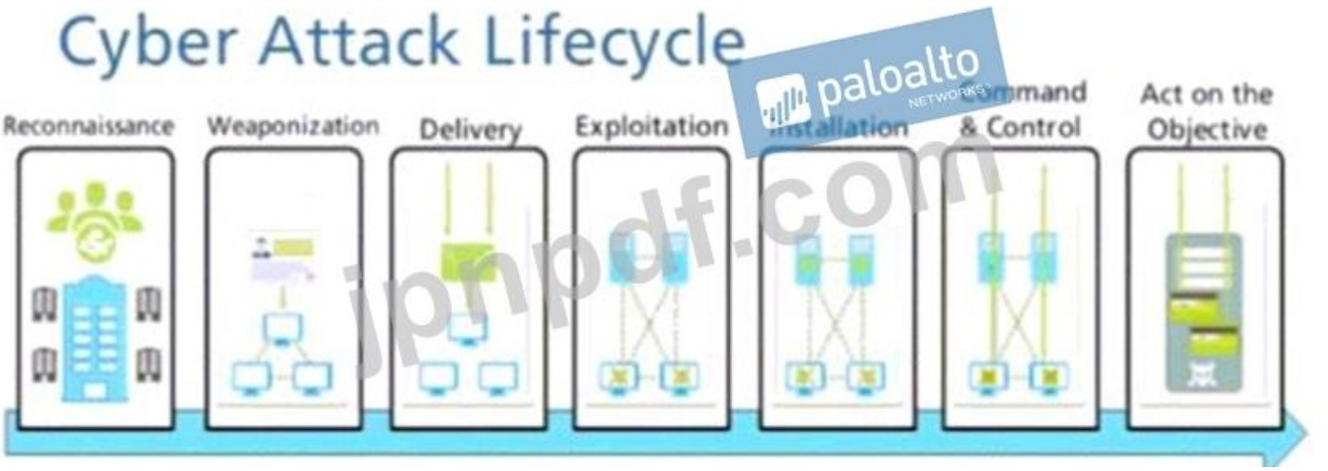
C. 名前、カテゴリ、テクノロジー、リスク、および特性

D. カテゴリ、サブカテゴリ、リスク、標準ポート、およびテクノロジー

Answer: A (メーッセージを残す**)**

最新問題**: 103**

Given the cyber-attack lifecycle diagram identify the stage in which the attacker can run malicious code against a vulnerability in a targeted machine.



A. Installation
B. Exploitation
C. Reconnaissance
D. Act on the Objective
Answer: B (メーッセージを残す)

最新問題: **104**
What are three factors that can be used in domain generation algorithms? (Choose three.)
A. cryptographic keys
B. time of day
C. other unique values
D. URL custom categories
E. IP address
Answer: A,B,C (メーッセージを残す)
Domain generation algorithms (DGAs) are used to auto-generate domains, typically in large numbers within the context of establishing a malicious command-and-control (C2) communications channel. DGA-based malware (such as Pushdo, BankPatch, and CryptoLocker) limit the number of domains from being blocked by hiding the location of their active C2 servers within a large number of possible suspects, and can be algorithmically generated based on factors such as time of day, cryptographic keys, or other unique values.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection

最新問題: **105**
Which prevention technique will prevent attacks based on packet count?
A. antivirus profile
B. zone protection profile
C. vulnerability profile
D. URL filtering profile
Answer: B (メーッセージを残す)

最新問題: **106**
URL フィルタリング セキュリティ プロファイルでアクションを設定できる 2 つの項目はどれですか? (2つお選びください。)
A. ブロックリスト
B. カスタム URL カテゴリ
C. PAN-DB URL カテゴリ
D. 許可リスト
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

最新問題: **107**
An administrator manages a network with 300 addresses that require translation. The administrator configured NAT with an address pool of 240 addresses and found that connections from addresses that needed new translations were being dropped.
Which type of NAT was configured?
A. Dynamic IP
B. Static IP
C. Dynamic IP and Port
D. Destination NAT
Answer: A (メーッセージを残す**)**
The size of the NAT pool should be equal to the number of internal hosts that require address translations. By default, if the source address pool is larger than the NAT address pool and eventually all of the NAT addresses are allocated, new connections that need address translation are dropped. To override this default behavior, use Advanced (Dynamic IP/Port Fallback) to enable the use of DIPP addresses when necessary.

最新問題: **108**
An administrator is troubleshooting an issue with Office365 and expects that this traffic traverses the firewall.
When reviewing Traffic Log entries, there are no logs matching traffic from the test workstation.
What might cause this issue?
A. Office365 traffic is logged in the Authentication Log.

B. Traffic matches the interzone-default rule, which does not log traffic by default.
C. The firewall is blocking the traffic, and all blocked traffic is in the Threat Log.
D. Office365 traffic is logged in the System Log.
Answer: B (メーッセージを残す)

最新問題**: 109**
A Panorama administrator would like to create an address object for the DNS server located in the New York City office, but does not want this object added to the other Panorama managed firewalls.
Which configuration action should the administrator take when creating the address object?
A. Tag the address object with the New York Office tag.
B. Ensure that Disable Override is cleared.
C. Ensure that the Shared option is checked.
D. Ensure that the Shared option is cleared.
Answer: D (メーッセージを残す)
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/manage-device-groups/manage-unused-shared-objects

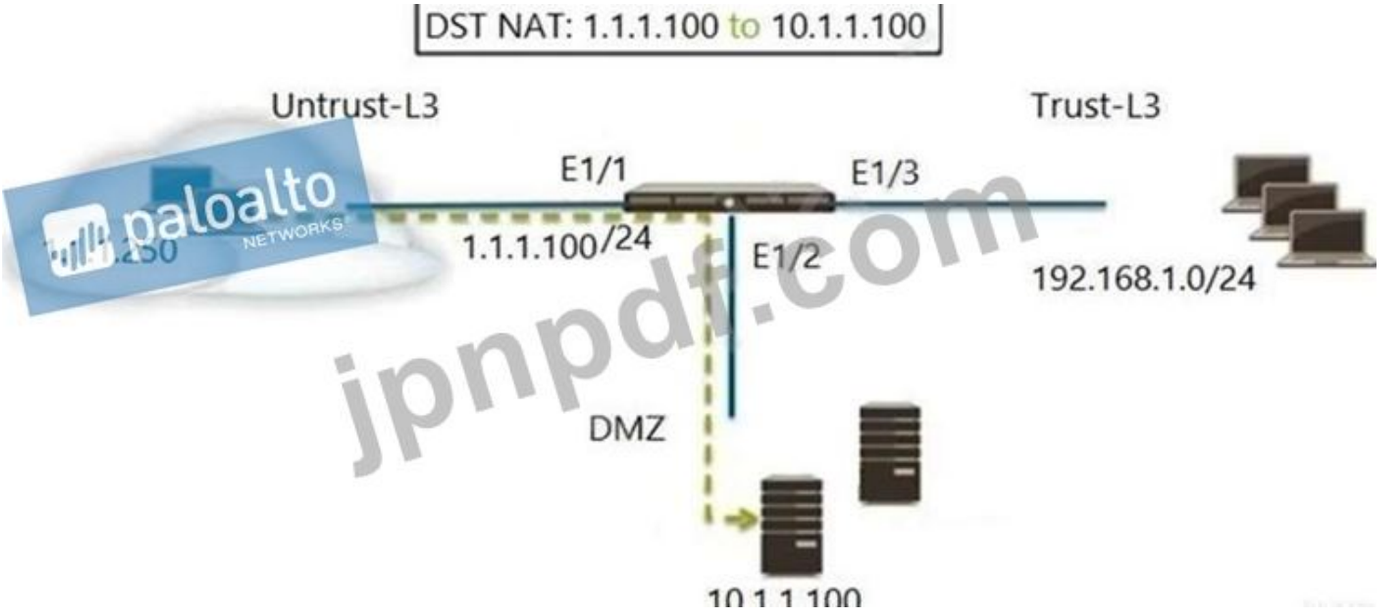
最新問題**: 110**
外部ゾーンと内部ゾーンの間を通過するトラフィックには一致するが、ゾーン内を通過するトラフィックには一致しないセキュリティ ポリシー ルールはどれですか?
A. グローバル
B. イントラゾーン
C. ゾーン間
D. ユニバーサル
Answer: C (メーッセージを残す)
intrazone では、異なるゾーン間のトラフィックではなく、ゾーン内のトラフィックが許可されます。

最新問題**: 111**
At which point in the app-ID update process can you determine if an existing policy rule is affected by an app-ID update?
A. after clicking Check New in the Dynamic Update window
B. after connecting the firewall configuration
C. after installing the update
D. after downloading the update
Answer: B (メーッセージを残す)

最新問題**: 112**
Based on the screenshot what is the purpose of the included groups?

A. They are only groups visible based on the firewall's credentials.
B. They contain only the users you allow to manage the firewall.
C. They are groups that are imported from RADIUS authentication servers.
D. They are used to map usernames to group names.
Answer: (解答を表示する**)**

最新問題**: 113**
Refer to the exhibit. A web server in the DMZ is being mapped to a public address through DNAT.



Which Security policy rule will allow traffic to flow to the web server?
A. Untrust (any) to DMZ (10.1.1.100), web browsing -Allow
B. Untrust (any) to Untrust (1.1.1.100), web browsing -Allow
C. Untrust (any) to Untrust (10.1.1.100), web browsing -Allow
D. Untrust (any) to DMZ (1.1.1.100), web browsing -Allow
Answer: D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

最新問題**: 114**
An administrator is configuring a NAT rule
At a minimum, which three forms of information are required? (Choose three.)
A. destination address
B. destination interface
C. destination zone
D. name
E. source zone

Answer: (解答を表示する)

最新問題**: 115**
The compliance officer requests that all evasive applications need to be blocked on all perimeter firewalls out to the internet. The firewall is configured with two zones:
1. trust for internal networks
2. untrust to the internet
Based on the capabilities of the Palo Alto Networks NGFW, what are two ways to configure a security policy using App-ID to comply with this request? (Choose two)
A. Create a deny rule at the top of the policy from trust to untrust with service application-default and add an application filter with the evasive characteristic
B. Create a deny rule at the top of the policy from trust to untrust with service application-default and select evasive as the application.
C. Create a deny rule at the top of the policy from trust to untrust over any service and select evasive as the application
D. Create a deny rule at the top of the policy from trust to untrust over any service and add an application filter with the evasive characteristic.
Answer: A,D (メーッセージを残す)

最新問題**: 116**
What are the two main reasons a custom application is created? (Choose two.)
A. To correctly identify an internal application in the traffic log
B. To change the default categorization of an application
C. To visually group similar applications
D. To reduce unidentified traffic on a network
Answer: (解答を表示する)
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-custom-application

最新問題**: 117**
An administrator is trying to implement an exception to an external dynamic list manually. Some entries are shown underlined in red.
What would cause this error?
A. Entries contain symbols.
B. Entries are wildcards.
C. Entries contain regular expressions.
D. Entries are duplicated.
Answer: C (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/exclude-entries-from-an-external-dynamic-list

最新問題: **118**
ポートのみに基づいてオブジェクトのグループを設定したい場合は何を構成しますか?
A. アドレスグループ
B. カスタム オブジェクト
C. アプリケーショングループ
D. サービスグループ
Answer: D (メーッセージを残す**)**
サービス = レイヤ 4、アプリケーション = レイヤ 7

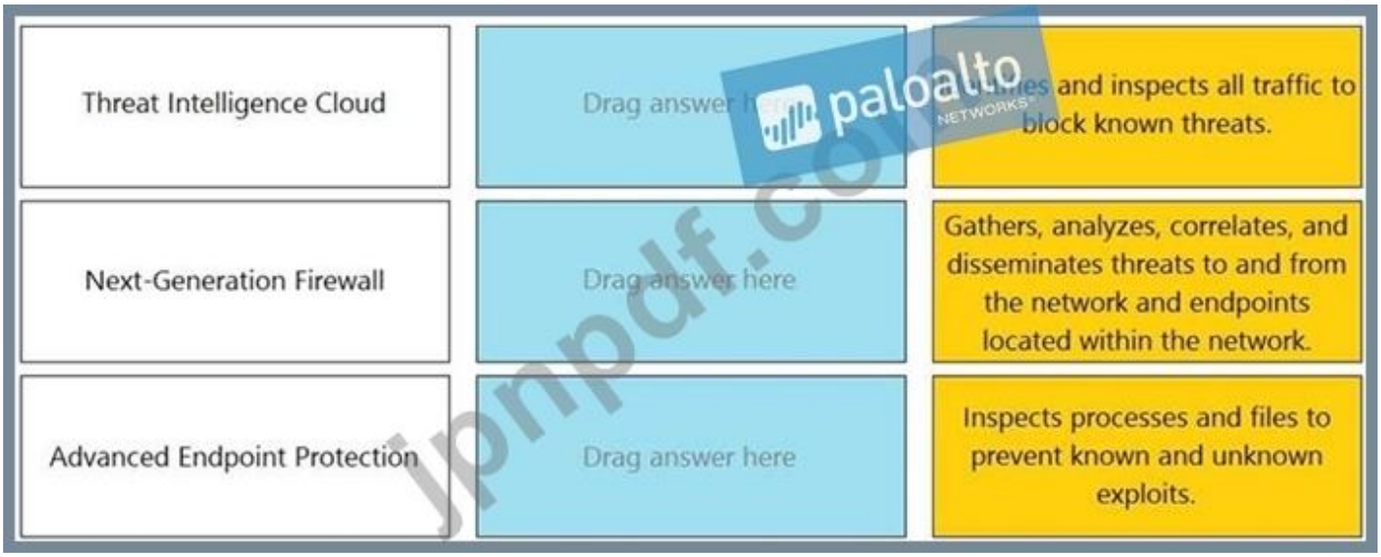
最新問題: **119**
Policy Optimizer の使用法を最もよく説明しているのはどれですか?
A. ポリシー オプティマイザーをスケジュールで使用すると、存在するすべてのレイヤー 4 ポリシーに対して無効なレイヤー 7 App-ID セキュリティ ポリシーを自動的に作成できます。その後、管理者は保持したいポリシーを手動で有効化し、削除したいポリシーを削除できます。
B. Policy Optimizer は、過去 90 日間に使用されなかったセキュリティ ポリシーを表示できます。
C. Policy Optimizer は、選択された各 Secunty ポリシーのログ転送プロファイルを追加または変更できます。
D. VM-50 ファイアウォール上のポリシー オプティマイザーは、どのレイヤ 7 App-ID セキュリティ ポリシーに未使用のアプリケーションがあるかを表示できます。
Answer: B (メーッセージを残す**)**

最新問題: **120**
Which plane on a Palo alto networks firewall provides configuration logging and reporting functions on a separate processor?
A. data
B. network processing
C. management
D. security processing
Answer: (解答を表示する**)**

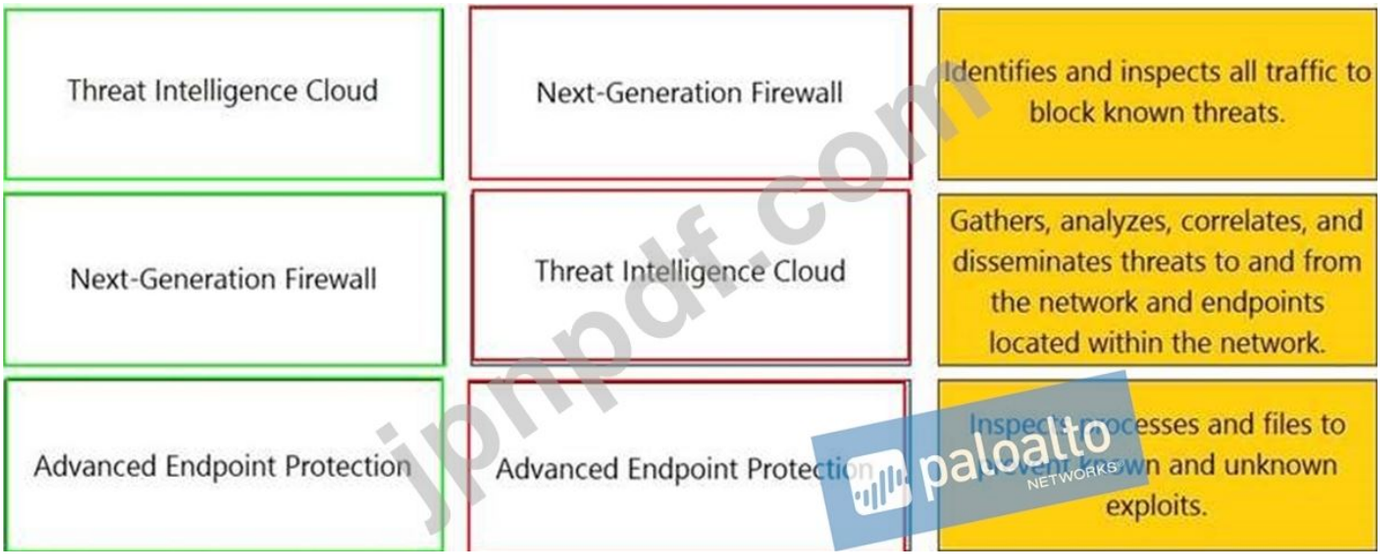
最新問題: **121**
What are two valid selections within an Anti-Spyware profile? (Choose two.)
A. Default
B. Random early drop
C. Deny
D. Drop
Answer: (解答を表示する**)**

最新問題: **122**
このステートメントを正しく完了するオプションを選択してください。セキュリティ プロファイルは、トラフィック _____ をブロックまたは許可できます。
A. データ プレースまたは管理プレーンのいずれか。
B. トラフィックを許可するセキュリティ ポリシー ルールと一致した後。
C. セキュリティ ポリシー ルールと一致する前。
D. トラフィックを許可またはブロックするセキュリティ ポリシー ルールと一致した後。
Answer: B (メーッセージを残す**)**
説明/参照:
参照：
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html

最新問題: **123**
各機能を DoS プロテクション ポリシーまたは DoS プロテクション プロファイルと照合します。



Answer:



最新問題: **124**

画像を考慮して、セキュリティ ポリシー ルールに関して正しい 2 つのオプションはどれですか。(2つお選びください。)

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service...	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. Office プログラムを許可するルールはアプリケーション フィルターを使用しています

B. Web サーバーへの FTP を許可するルールでは、App-ID を使用した FTP が許可されています

C. Office プログラムを許可するルールはアプリケーション グループを使用しています

D. ソーシャル ネットワーキングを許可するルールで、Facebook のすべての機能を許可します。

Answer: A,D (メーッセージを残す)

Web サーバーへの FTP を許可するルールでは、APP-ID ではなくポートベースのルールを使用して FTP が許可されます。

最新問題: **125**

Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?

A. URL traffic

B. vulnerability protection

C. anti-spyware

D. antivirus

Answer: C (メーッセージを残す)

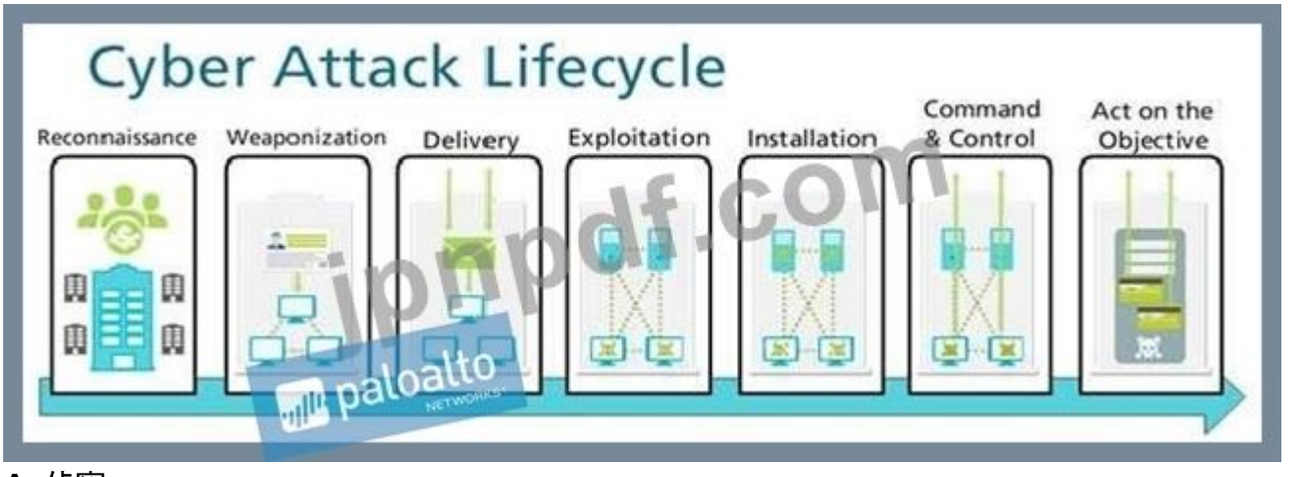
In addition, you can enable the DNS Sinkholing action in Anti-Spyware profiles to enable the firewall to forge a response to a DNS query for a known malicious domain, causing the malicious

domain name to resolve to an IP address that you define. This feature helps to identify infected hosts on the protected network using DNS traffic.

最新問題: **126**
Given the detailed log information above, what was the result of the firewall traffic inspection?
A. It was blocked by the Anti-Virus Security profile action.
B. It was blocked by the Anti-Spyware Profile action.
C. It was blocked by the Security policy action.
D. It was blocked by the Vulnerability Protection profile action.
Answer: B (メーッセージを残す**)**

最新問題: **127**
Which option shows the attributes that are selectable when setting up application filters?
A. Category, Subcategory, Technology, and Characteristic
B. Category, Subcategory, Technology, Risk, and Characteristic
C. Name, Category, Technology, Risk, and Characteristic
D. Category, Subcategory, Risk, Standard Ports, and Technology
Answer: B (メーッセージを残す**)**
Explanation/Reference: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects- application-filters

最新問題: **128**
サイバー攻撃のライフサイクル図を考慮して、攻撃者が標的のマシンに対して悪意のあるコードを実行できる段階を特定します。



A. 偵察
B. 目的に基づいて行動する
C. エクスプロイト
D. インストール
Answer: C (メーッセージを残す**)**

最新問題: **129**

悪意のある Web コンテンツを分類するにはどのセキュリティ プロファイルを使用する必要がありますか?

A. URL フィルタリング

B. ウイルス対策

C. Web コンテンツ

D. 脆弱性保護

Answer: A (メーッセージを残す**)**

URL フィルタリングは、Web サイトの URL カテゴリとレピュテーションに基づいて Web コンテンツを分類できるセキュリティ プロファイルです。URL フィルタリングは、フィッシング、マルウェア、コマンド アンド コントロール サイトなどの悪意のある Web コンテンツへのアクセスをブロックしたり、Web ブラウジングの許容使用ポリシーを強制したりするのに役立ちます。URL フィルタリングは、PAN-DB クラウド サービスを使用して、何百万もの Web サイトの URL カテゴリと評判に関する最新情報を提供します。URL フィルタリング ポリシーを構成して、URL カテゴリとレピュテーションに基づいて Web リクエストを許可、ブロック、アラート、続行、または上書きしたり、さまざまなユーザー グループの応答ページと例外をカスタマイズしたりできます。参考: URL フィルタリング、基本的なセキュリティ ポリシーのセットアップ、PAN-OS 10.1 の更新された認定

最新問題**: 130**

What do dynamic user groups you to do?

A. create a QoS policy that provides auto-remediation for anomalous user behavior and malicious activity

B. create a policy that provides auto-sizing for anomalous user behavior and malicious activity

C. create a policy that provides auto-remediation for anomalous user behavior and malicious activity

D. create a dynamic list of firewall administrators

Answer: C (メーッセージを残す**)**

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text

最新問題**: 131**

Given the screenshot, what are two correct statements about the logged traffic? (Choose two.)

TYPE	FROM ZONE	TO ZONE	INGRESS I/F	SOURCE	NAT APPLIED	EGRESS I/F	DESTINATION	TO PORT	APPLICATION	ACTION	SESSION END REASON	BYTES	ACTION SOURCE	LOG ACTION	BYTES SENT	BYTES RECEIVED	LOG TYPE
end	LAN	internet	ethernet1/2	192.168.200.100	yes	ethernet1/5	198.54.12.97	443	web-browsing	allow	threat	3.3k	from-policy	default	2.7k	541	traffic

A. The web session was unsuccessfully decrypted.

B. The web session was decrypted.

C. The traffic was denied by security profile.

D. The traffic was denied by URL filtering.

Answer: B (メーッセージを残す**)**

最新問題: **132**

Recently changes were made to the firewall to optimize the policies and the security team wants to see if those changes are helping.

What is the quickest way to reset the hit counter to zero in all the security policy rules?

A. Highlight a rule and use the Reset Rule Hit Counter > Selected Rules for each rule

B. Reboot the firewall

C. At the CLI enter the command reset rules and press Enter

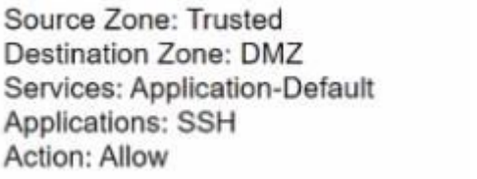
D. Use the Reset Rule Hit Counter > All Rules option

Answer: D (メーッセージを残す)

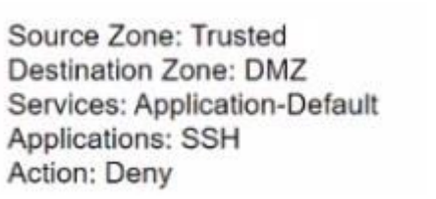
最新問題: **133**

If users from the Trusted zone need to allow traffic to an SFTP server in the DMZ zone, how should a Security policy with App-ID be configured?

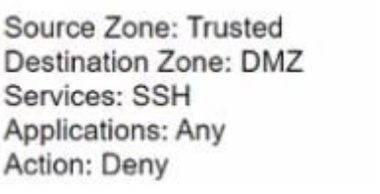
A.



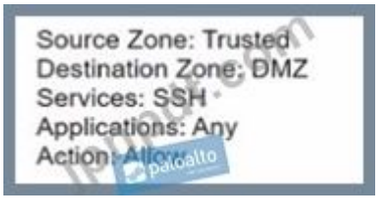
B.



C.



D.



Answer: A (メーッセージを残す)

最新問題: **134**

An administrator needs to add capability to perform real-time signature lookups to block or sinkhole all known malware domains.

Which type of single unified engine will get this result?

A. Content-ID

B. Security Processing Engine

C. App-ID

D. User-ID

Answer: (解答を表示する)

最新問題: **135**
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?
A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent
Answer: C (メーッセージを残す)
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresse

最新問題: **136**
ポリシーが最初に適用されるようにするには、どのセキュリティ ポリシー セットを使用する必要がありますか?
A. 子デバイスグループの事前ルールベース
B. 共有事前ルールベース
C. 親デバイスグループの事前ルールベース
D. ローカル ファイアウォール ポリシー
Answer: B (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/panorama-web-interface/defining-policies-on-panorama

最新問題: **137**
サイバー攻撃のライフサイクル図を考慮して、攻撃者が標的のマシンに対して悪意のあるコードを開始できる段階を特定します。

A. エクスプロイト
B. 偵察
C. 目的に基づいて行動する
D. インストール
Answer: (解答を表示する**)**

最新問題**: 138**
Which profile must be applied to the Security policy rule to block spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers?
A. Anti-spyware
B. File blocking
C. WildFire
D. URL filtering
Answer: A (メーッセージを残す**)**
Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients.
https://docs.paloaltonetworks.com/network-security/security-policy/security-profiles/security-profile-anti-spyware

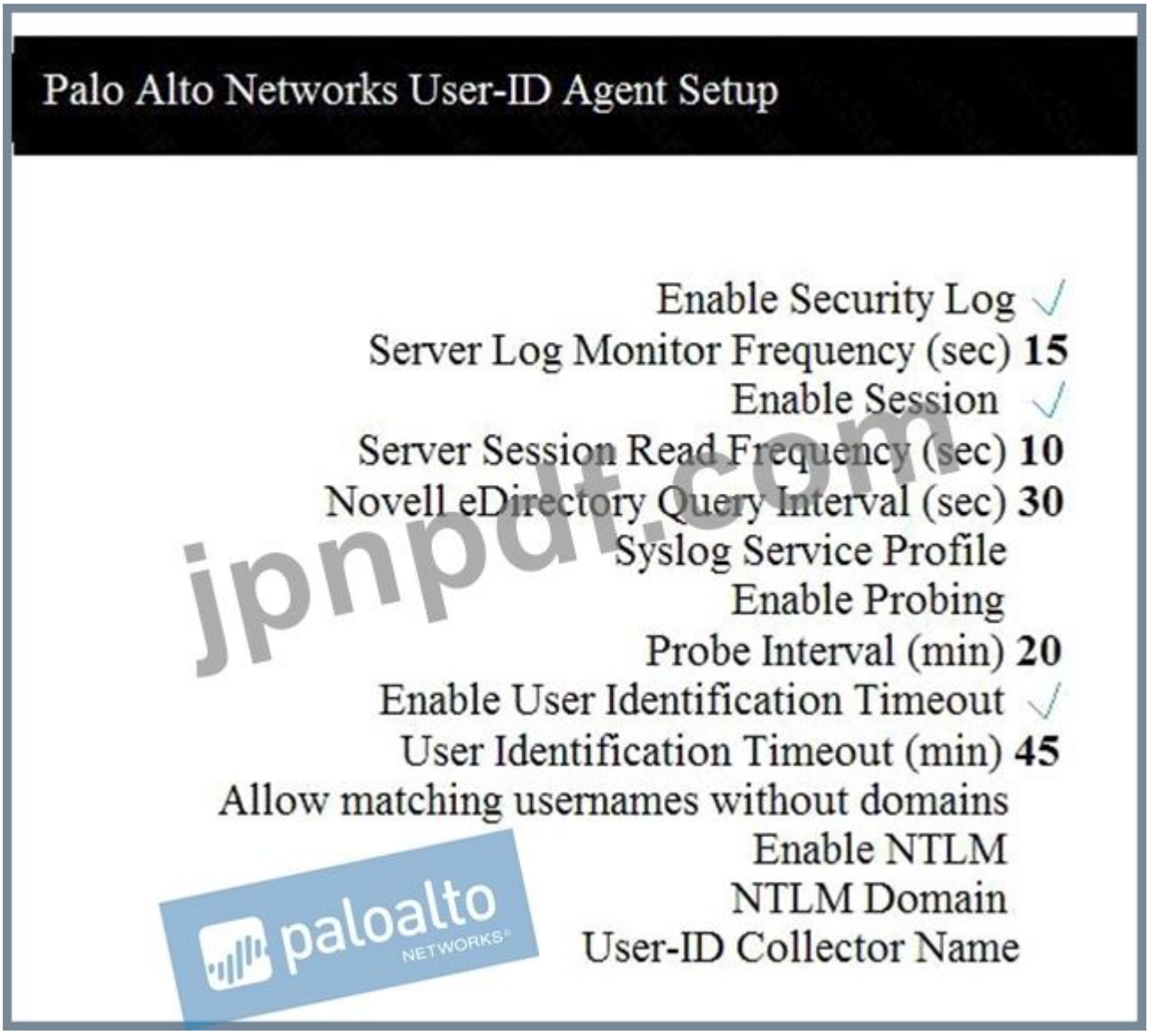
最新問題**: 139**
Based on the screenshot what is the purpose of the included groups?

	Name	Type	Source			Destination		Application	Service	Action
			Zone	Address	User	Zone	Address			
1	allow-it	universal	inside	any	it	dmz	any	it-tools	application-default	Allow

A. They are only groups visible based on the firewall's credentials.
B. They are used to map usernames to group names.
C. They contain only the users you allow to manage the firewall.
D. They are groups that are imported from RADIUS authentication servers.
Answer: B (メーッセージを残す**)**

最新問題: **140**
Panorama を使用して管理対象デバイスへのコンテンツ更新をスケジュールするには、PAN-OS 10.2 のどのパスが使用されますか?
A. [パノラマ] > [デバイス展開] > [動的更新] > [スケジュール] > [追加]
B. [パノラマ] > [デバイス展開] > [コンテンツ更新] > [スケジュール] > [追加]
C. [パノラマ] > [動的更新] > [デバイス展開] > [スケジュール] > [追加]
D. [パノラマ] > [コンテンツ更新] > [デバイス導入] > [スケジュール] > [追加]
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-upgrade/upgrade-panorama/deploy-updates-to-firewalls-log-collectors-and-wildfire-appliances-using-panorama/パノラマを使用したコンテンツ更新のスケジュール

最新問題: **141**
Which two configuration settings shown are not the default? (Choose two.)



A. Enable Probing

B. Server Log Monitor Frequency (sec)
C. Enable Session
D. Enable Security Log
Answer: B,C (メーッセージを残す**)**

最新問題**: 142**
シャドウ ルールが存在する場合に FQDN オブジェクトが解決されているかどうかを確認するのに役立つ CLI コマンドはどれですか?
A. >システム FQDN を表示
B. >FQDN 表示システムを要求します
C. >システム FQDN の表示を要求します
D. >システム FQDN 表示を要求します
Answer: (解答を表示する**)**
show system fqdn コマンドは、ファイアウォール上に設定されている FQDN オブジェクトとその解決された IP アドレスを表示します。これは、FQDN オブジェクトが正しく解決されているかどうか、およびそれらが予想されるトラフィックと一致しているかどうかを確認するのに役立ちます。シャドウ ルールは、前のルールが同じトラフィックをカバーしているため、決して一致しないルールです。シャドウ ルールで FQDN オブジェクトを使用する場合、FQDN オブジェクトが解決されないか、トラフィックと異なる IP アドレスが割り当てられ、ルールが無効になる可能性があります。

最新問題**: 143**
Which statement is true regarding a Best Practice Assessment?
A. It provides a set of questionnaires that help uncover security risk prevention gaps across all areas of network and security architecture.
B. It runs only on firewalls.
C. When guided by an authorized sales engineer, it helps determine the areas of greatest risk where you should focus prevention activities.
D. It shows how current configuration compares to Palo Alto Networks recommendations.
Answer: (解答を表示する**)**

最新問題**: 144**
どのタイプのセキュリティ ポリシー ルールが、内部ゾーン内と外部ゾーン内の内部ゾーンと外部ゾーンの間を流れるトラフィックに一致しますか?
A. イントラゾーン
B. グローバル
C. ゾーン間
D. ユニバーサル
Answer: D (メーッセージを残す**)**

最新問題: **145**
An administrator needs to create a Security policy rule that matches DNS traffic sourced from either the LAN or VPN zones, destined for the DMZ or Untrust zones.
The administrator does not want to match traffic where the source and destination zones are LAN, and also does not want to match traffic where the source and destination zones are VPN.
Which Security policy rule type should they use?
A. Universal
B. Intrazone
C. Interzone
D. Default
Answer: A (メーッセージを残す**)**

最新問題: **146**
Based on the graphic which statement accurately describes the output shown in the server monitoring panel?

A. The host lab-client has been by the User-ID agent.
B. The User-ID agent is connected to a domain controller labeled lab client.
C. The host lab-client has been found by a domain controller.
Answer: B (メーッセージを残す**)**

最新問題: **147**

What in the minimum frequency for which you can configure the firewall too check for new wildfire antivirus signatures?

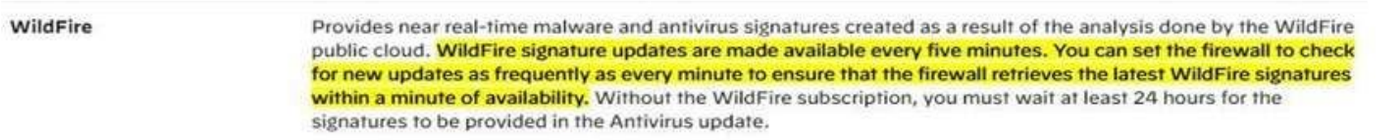
A. every 5 minutes

B. every 1 minute

C. every 24 hours

D. every 30 minutes

Answer: B (メーッセージを残す)



最新問題**: 148**

An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server. Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)

A. vulnerability protection profile applied to outbound security policies

B. anti-spyware profile applied to outbound security policies

C. antivirus profile applied to outbound security policies

D. URL filtering profile applied to outbound security policies

Answer: (解答を表示する)

Antivirus: Includes new and updated antivirus signatures, including WildFire signatures and automatically generated command-and-control (C2) signatures. WildFire signatures detect malware seen first by firewalls from around the world. You must have a Threat Prevention subscription to get these updates.

New antivirus signatures are published daily.

Anti-Spyware profiles blocks spyware on compromised hosts from trying to phone-home or beacon out to external command-and-control (C2) servers, allowing you to detect malicious traffic leaving the network from infected clients. You can apply various levels of protection between zones.

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-profiles

最新問題**: 149**

Prior to a maintenance-window activity, the administrator would like to make a backup of only the running configuration to an external location. What command in Device > Setup > Operations would provide the most operationally efficient way to achieve this outcome?

A. save candidate config

B. save named configuration snapshot

C. export named configuration snapshot

D. export device state

Answer: (解答を表示する)

最新問題: **150**

Which data-plane processor layer of the graphic shown provides uniform matching for spyware and vulnerability exploits on a Palo Alto Networks Firewall?

A. Security Matching

B. Security Processing

C. Network Processing

D. Signature Matching

Answer: (解答を表示する)

最新問題: **151**

Based on the image provided, which two statements apply to the Security policy rules? (Choose two.)

A. The Allow-Office-Programs rule is using an application filter.

B. In the Allow-FTP policy, FTP is allowed using App-ID.

C. The Allow-Office-Programs rule is using an application group.

D. The Allow-Social-Media rule allows all Facebook functions.

Answer: A,D (メーッセージを残す)

最新問題: **152**
ユーザーが URL 管理者パスワードを提供した場合にのみサイトにアクセスできるようにするには、どの URL フィルタリング プロファイル アクションを設定しますか?
A. オーバーライド
B. 認可
C. 認証
D. 続行
Answer: (解答を表示する**)**
参照：
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filteringprofile-actions.html

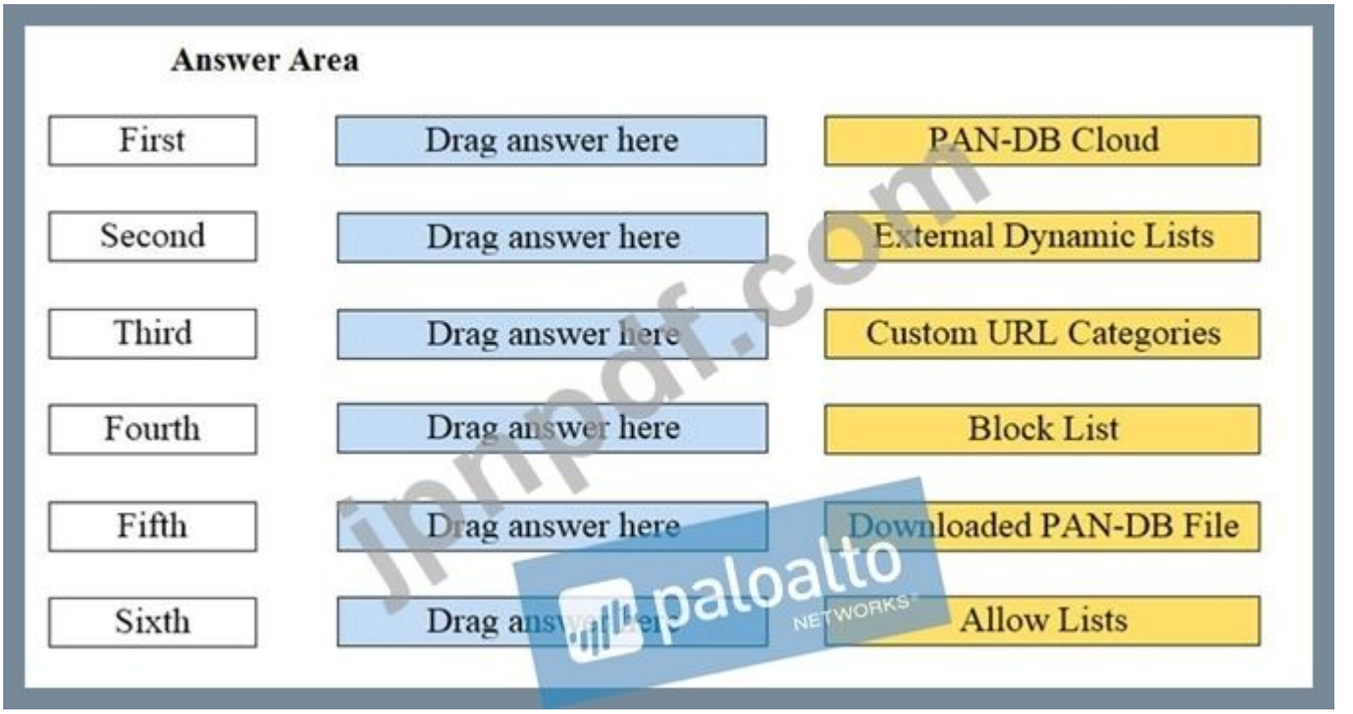
最新問題: **153**
Which path in PAN-OS 11.x would you follow to see how new and modified App-IDs impact a Security policy?
A. Objects > Dynamic Updates > Review App-IDs
B. Device > Dynamic Updates > Review Policies
C. Device > Dynamic Updates > Review App-IDs
D. Objects > Dynamic Updates > Review Policies

Answer: C (メーッセージを残す)

To see how new and modified App-IDs impact your Security policy, you need to follow the path Device > Dynamic Updates > Review App-IDs on PAN-OS 11.x. This option allows you to perform a content update policy review for both downloaded and installed content. You can view the list of new and modified App-IDs and their descriptions, and see which Security policy rules are affected by them. You can also modify the rules or create new ones to adjust your Security policy as needed1. Reference: See How New and Modified App-IDs Impact Your Security Policy, Updated Certifications for PAN-OS 10.1, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

最新問題: 154

Arrange the correct order that the URL classifications are processed within the system.



Answer:

最新問題: **155**
ステートメントを完成させます。セキュリティプロファイルはトラフィックをブロックまたは許可できます
A. 不明な tcp または不明な udp トラフィック上
B. トラフィックを許可するセキュリティ ポリシーによって評価された後
C. セキュリティ ポリシーによって評価される前
D. トラフィックを許可またはブロックするセキュリティ ポリシーによって評価された後
Answer: B (メーッセージを残す)
セキュリティ プロファイルは、許可アクションを使用して構成されたポリシー ルールに追加されるオブジェクトです。

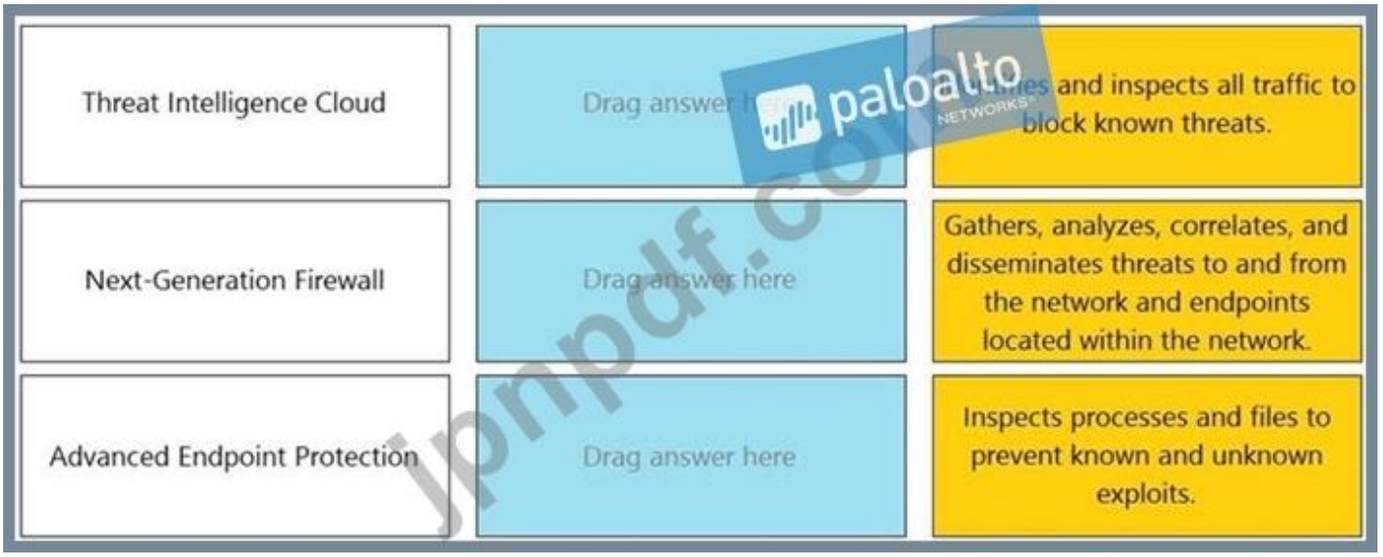
最新問題: **156**
An administrator needs to allow users to use their own office applications. How should the administrator configure the firewall to allow multiple applications in a dynamic environment?
A. Create an Application Filter and name it Office Programs, the filter it on the business-systems category, office-programs subcategory
B. Create an Application Group and add business-systems to it
C. Create an Application Filter and name it Office Programs, then filter it on the business-systems category
D. Create an Application Group and add Office 365, Evernote, Google Docs, and Libre Office
Answer: A (メーッセージを残す)
Explanation
An application filter is an object that dynamically groups applications based on application attributes that you define, including category, subcategory, technology, risk factor, and characteristic. This is useful when you want to safely enable access to applications that you do

not explicitly sanction, but that you want users to be able to access. For example, you may want to enable employees to choose their own office programs (such as Evernote, Google Docs, or Microsoft Office 365) for business use. To safely enable these types of applications, you could create an application filter that matches on the Category business-systems and the Subcategory office-programs. As new applications office programs emerge and new App-IDs get created, these new applications will automatically match the filter you defined; you will not have to make any additional changes to your policy rulebase to safely enable any application that matches the attributes you defined for the filter.
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-an-application-filter.html

最新問題: **157**
Which User-ID agent would be appropriate in a network with multiple WAN links, limited network bandwidth, and limited firewall management plane resources?
A. Citrix terminal server deployed on the internal network
B. Windows-based agent deployed on each of the WAN Links
C. PAN-OS integrated agent deployed on the internal network
D. Windows-based agent deployed on the internal network
Answer: (解答を表示する**)**

最新問題: **158**
What is the main function of Policy Optimizer?
A. reduce load on the management plane by highlighting combinable security rules
B. migrate other firewall vendors' security rules to Palo Alto Networks configuration
C. eliminate "Log at Session Start" security rules
D. convert port-based security rules to application-based security rules
Answer: D (メーッセージを残す**)**
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy- optimizer.html

最新問題: **159**
各機能を DoS プロテクション ポリシーまたは DoS プロテクション プロファイルと照合します。



Answer:

最新問題: **160**

Which action can be performed when grouping rules by group tags?

A. Delete Tagged Rule(s)

B. Edit Selected Rule(s)

C. Apply Tag to the Selected Rule(s)

D. Tag Selected Rule(s)

Answer: D (メーッセージを残す)

When grouping rules by group tags, the action that can be performed is to tag selected rule(s). This action allows you to assign one or more tags to the selected rules, which will group them together and display them under the corresponding tag group. You can use tags to organize and visually distinguish your rules based on different criteria, such as function, location, or priority1. Reference: View Rules by Tag Group, Use Tags to Group and Visually Distinguish Objects, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

最新問題: **161**

Your company is highly concerned with their Intellectual property being accessed by unauthorized resources.

There is a mature process to store and include metadata tags for all confidential documents.

Which Security profile can further ensure that these documents do not exit the corporate network?

A. File Blocking

B. Data Filtering

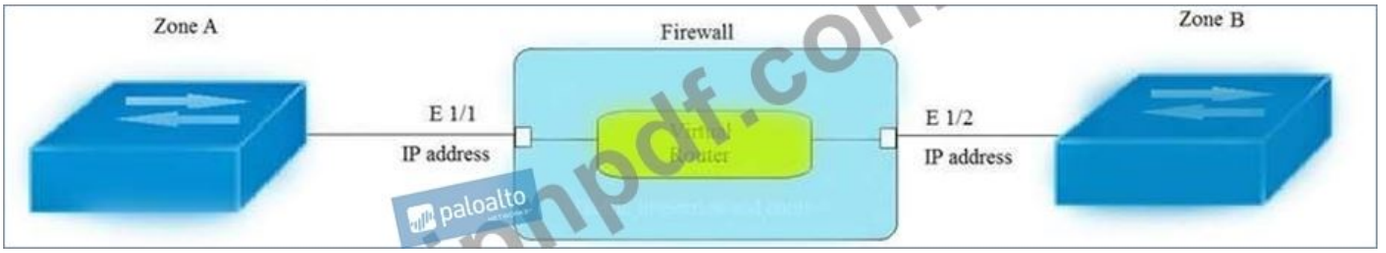
C. Anti-Spyware

D. URL Filtering

Answer: (解答を表示する)

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-data-fi

最新問題: **162**
トポロジを考慮すると、ゾーン A とゾーン B をどのゾーン タイプで構成する必要がありますか?



A. レイヤ 3
B. レイヤ 2
C. 仮想ワイヤー
D. タップ
Answer: (解答を表示する)

最新問題: **163**
Which update option is not available to administrators?
A. New Antivirus Signatures
B. New Malicious Domains
C. New Spyware Notifications
D. New URLs
E. New Application Signatures
Answer: D (メーッセージを残す)

最新問題: **164**
Web セッションが終了したことをユーザーのブラウザにメッセージで送信するセキュリティ ポリシー アクションはどれですか?
A. ドロップ
B. 拒否
C. クライアントをリセットします
D. サーバーをリセットします
Answer: C (メーッセージを残す)
クライアントにのみリセットを送信すると、たとえば、内部ホストがセッションがリセットされた通知を受信し、ブラウザが回転したままにならないようにしたり、リモート サーバーが気づかない間にアプリケーションが確立されたセッションを閉じることができます。https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClltCAC

最新問題: **165**

If a universal security rule was created for source zones A & B and destination zones A & B, to which traffic would the rule apply?

A. Some traffic within A

B. All traffic within zones A & B

C. Some traffic within B

D. Some traffic between A & B

Answer: B (メーッセージを残す**)**

最新問題**: 166**

Which situation is recorded as a system log?

A. An attempt to access a spoofed website has been blocked.

B. A new asset has been discovered on the network.

C. A file that has been analyzed is potentially dangerous for the system.

D. A connection with an authentication server has been dropped.

Answer: D (メーッセージを残す**)**

最新問題**: 167**

Given the image, which two options are true about the Security policy rules. (Choose two.)

	Name	Tags	Type	Source Zone	Source Address	Source User	Source HIP Profile	Destination Zone	Destination Address	Rule Usage Hit Count	Rule Usage Last Hit	Rule Usage First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d...	Allow	None
2	Allow FTP to web ser..	None	Universal	Inside	Any	Any	Any	Outside	ftp-server	-	-	-	any	ftp-service..	Allow	None
3	Allow Social Networkin..	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	facebook	Application-d...	Allow	None

A. The Allow Office Programs rule is using an Application Filter

B. In the Allow FTP to web server rule, FTP is allowed using App-ID

C. The Allow Office Programs rule is using an Application Group

D. In the Allow Social Networking rule, allows all of Facebook's functions

Answer: A,D (メーッセージを残す**)**

In the Allow FTP to web server rule, FTP is allowed using port based rule and not APP-ID.

最新問題**: 168**

What is an advantage for using application tags?
A. They help with the creation of interfaces
B. They help with the design of IP address allocations in DHCP.
C. They are helpful during the creation of new zones
D. They help content updates automate policy updates
Answer: (解答を表示する**)**

最新問題**: 169**
静的ルートを作成する正しい手順はどれですか?
A. 1) ルートとネットマスクを入力します
2) 特定のネクストホップの IP アドレスを入力します。
3) 次のホップに移動するために使用するパケットの送信インターフェイスを指定します。
4) IPv4 または IPv6 ルートを名前で追加します
B. 1) ルートとネットマスクを入力します
2) 次のホップに移動するために使用するパケットの送信インターフェイスを指定します。
3) 特定のネクストホップの IP アドレスを入力します。
4) IPv4 または IPv6 ルートを名前で追加します
C. 1) 特定のネクストホップの IP アドレスを入力します。
2) ルートとネットマスクを入力します
3) IPv4 または IPv6 ルートを名前で追加します
4) 次のホップに移動するために使用するパケットの送信インターフェイスを指定します。
D. 1) 特定のネクストホップの IP アドレスを入力します
2) IPv4 または IPv6 ルートを名前で追加します
3) ルートとネットマスクを入力します
4) 次のホップに移動するために使用するパケットの送信インターフェイスを指定します。
Answer: (解答を表示する**)**
ルートとネットマスクを入力します
特定のネクストホップの IP アドレスを入力します
パケットがネクスト ホップに移動するために使用する送信インターフェイスを指定します。IPv4 または IPv6 ルートを名前で追加します。包括的な説明: これは、ファイアウォール上の仮想ルーターにスタティック ルートを作成する手順の正しい順序です。最初のステップは、宛先ネットワークのルートとネットマスクを入力することです (IPv4 アドレスの場合は 192.168.2.2/24、IPv6 アドレスの場合は 2001:db8:123:1::1/64 など)。2 番目のステップでは、192.168.56.1 や 192.168.56.1 など、特定のネクスト ホップの IP アドレスを入力します。2001:db8:49e:1::1。3 番目のステップは、パケットが次のホップに移動するために使用する送信インターフェイス (ethernet1/1 など) を指定することです。4 番目の手順では、IPv4 または IPv6 ルートを、route11 などの名前で追加します。参考文献:
静的ルートを構成する - パロアルトネットワークス

最新問題**: 170**

What allows a security administrator to preview the Security policy rules that match new application signatures?
A. Review Release Notes
B. Dynamic Updates-Review Policies
C. Dynamic Updates-Review App
D. Policy Optimizer-New App Viewer
Answer: B (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/manage-new-app-ids-introduced-in-content-r

最新問題**: 171**
What are three characteristics of the Palo Alto Networks DNS Security service? (Choose three.)
A. It uses techniques such as DGA/DNS tunneling detection and machine learning
B. It requires a valid Threat Prevention license.
C. It enables users to access real-time protections using advanced predictive analytics.
D. It requires a valid URL Filtering license.
E. It requires an active subscription to a third-party DNS Security service.
Answer: A,B,C (メーッセージを残す)
DNS Security subscription enables users to access real-time protections using advanced predictive analytics. When techniques such as DGA/DNS tunneling detection and machine learning are used, threats hidden within DNS traffic can be proactively identified and shared through an infinitely scalable cloud service. Because the DNS signatures and protections are stored in a cloud-based architecture, you can access the full database of ever-expanding signatures that have been generated using a multitude of data sources. This list of signatures allows you to defend against an array of threats using DNS in real-time against newly generated malicious domains. To combat future threats, updates to the analysis, detection, and prevention capabilities of the DNS Security service will be available through content releases. To access the DNS Security service, you must have a Threat Prevention license and DNS Security license.

最新問題**: 172**
An administrator wishes to follow best practices for logging traffic that traverses the firewall. Which log setting is correct?
A. Enable Log at both Session Start and End
B. Enable Log at Session Start
C. Enable Log at Session End
D. Disable all logging
Answer: C (メーッセージを残す)

最新問題**: 173**
When a security rule is configured as Intrazone, which field cannot be changed?
A. Destination Zone

B. Actions
C. Source Zone
D. Application
Answer: A (メーッセージを残す)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

最新問題**: 174**
Which two features can be used to tag a user name so that it is included in a dynamic user group? (Choose two)
A. User-ID Windows-based agent
B. log forwarding auto-tagging
C. XML API
D. GlobalProtect agent
Answer: A,C (メーッセージを残す)

最新問題**: 175**
An administrator wants to prevent users from submitting corporate credentials in a phishing attack.
Which Security profile should be applied?
A. antivirus
B. vulnerability protection
C. anti-spyware
D. URL filtering
Answer: (解答を表示する)

最新問題**: 176**
An administrator is creating a Security policy rule and sees that the destination zone is grayed out.
While creating the rule, which option was selected to cause this?
A. Interzone
B. Source zone
C. Universal (default)
D. Intrazone
Answer: D (メーッセージを残す)
In Intrazone security rules, no destination zone can be specified.

最新問題**: 177**
信頼ゾーンのユーザーが DMZ ゾーンの SFTP サーバーへのトラフィックを許可する必要がある場合、App-ID を使用したセキュリティ ポリシーをどのように構成する必要がありますか?
A)

Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Deny

B)

Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Allow

C)

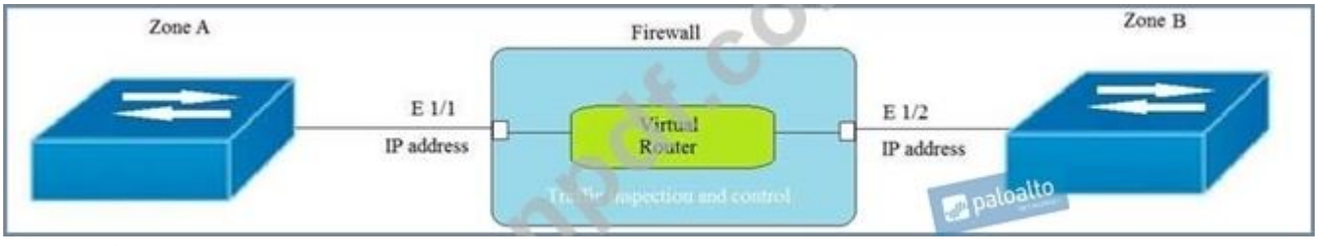
Source Zone: Trusted
Destination Zone: DMZ
Services: SSH
Applications: Any
Action: Deny

D)

Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow

A. オプション C
B. オプション D
C. オプション B
D. オプション A
Answer: B (メーッセージを残す**)**

最新問題**: 178**
トポロジを考慮すると、ゾーン A とゾーン B をどのゾーン タイプで構成する必要がありますか?

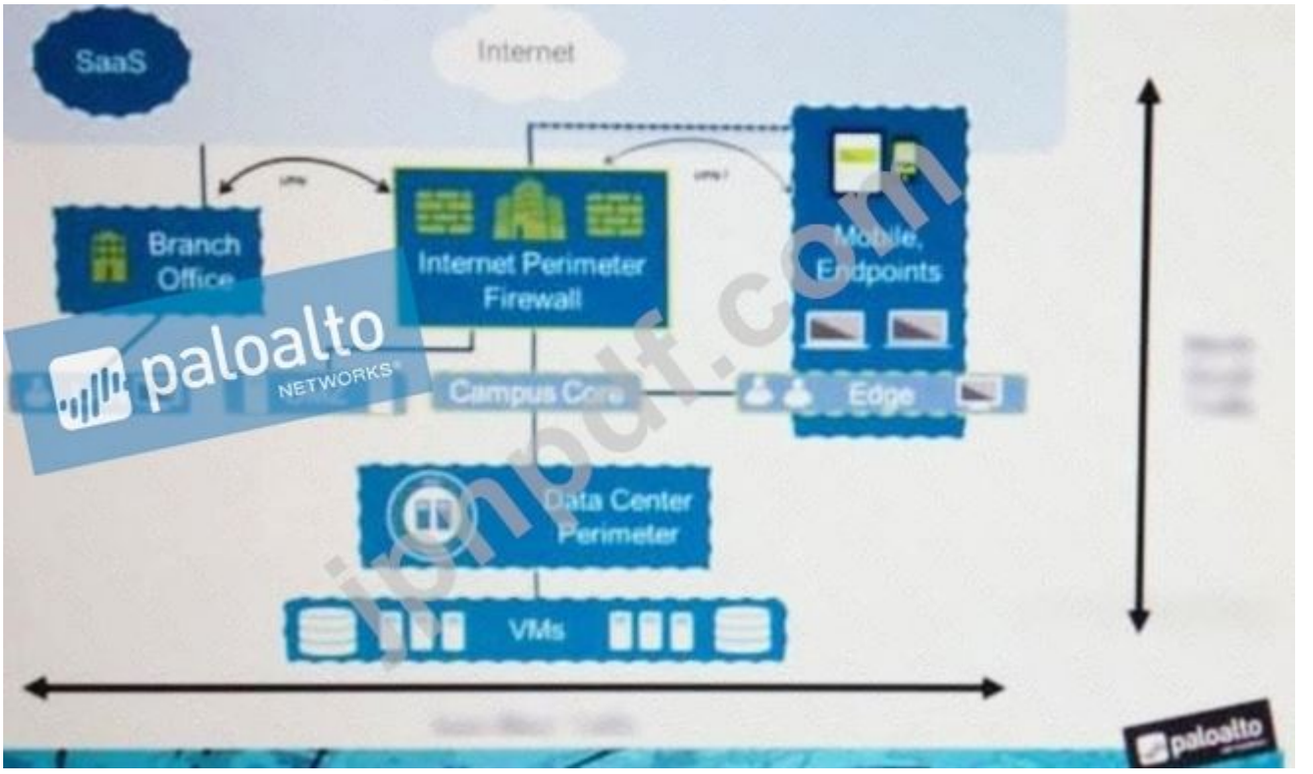


A. レイヤ 3
B. イーサネット
C. レイヤ 2
D. 仮想ワイヤー
Answer: (解答を表示する**)**
レイヤ 3 展開では、ファイアウォールは複数のインターフェイス間でトラフィックをルーティングします。ファイアウォールがレイヤー 3 インターフェイス間でトラフィックをルーティングす

るには、仮想ルーター オブジェクトが存在する必要があります。レイヤ 3 インターフェイスには IP アドレスが割り当てられます。

最新問題: **179**
Which two statements are true for the DNS security service introduced in PAN-OS version 9.0?
A. It removes the 100K limit for DNS entries for the downloaded DNS updates.
B. IT eliminates the need for dynamic DNS updates.
C. IT is automatically enabled and configured.
D. It functions like PAN-DB and requires activation through the app portal.
Answer: A,D (メーッセージを残す**)**

最新問題: **180**
An administrator notices that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would the administrator need to monitor and block to mitigate the malicious activity?

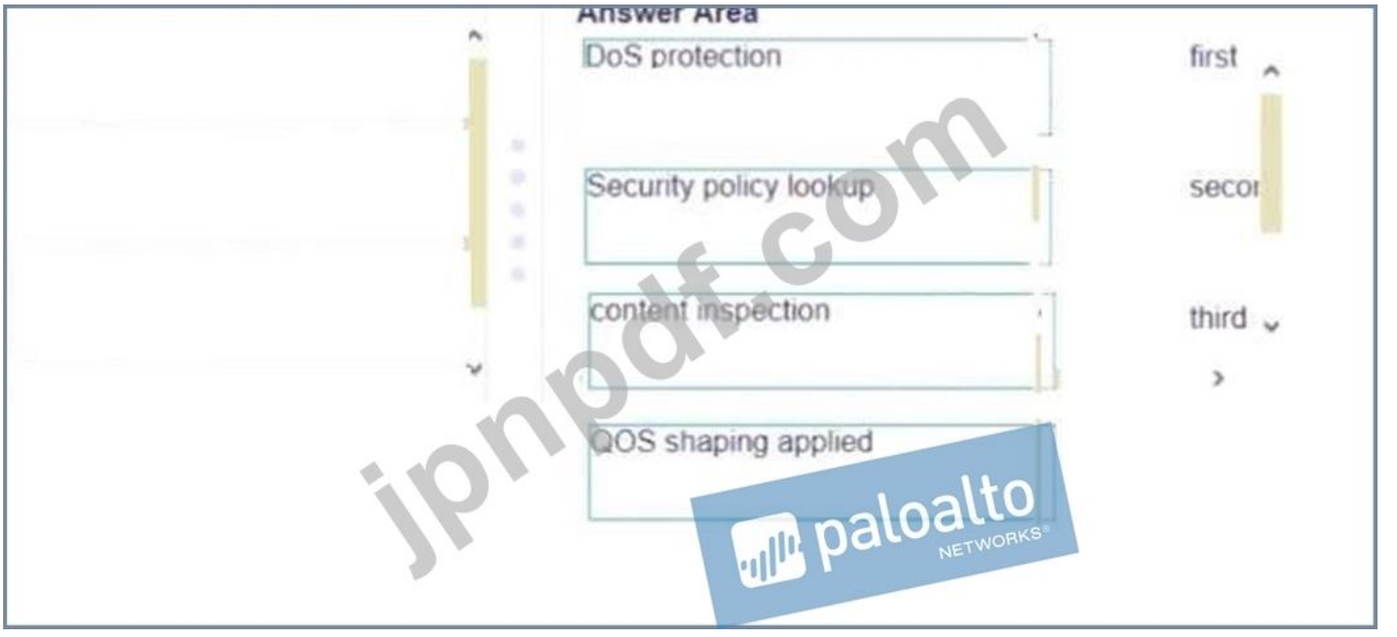


A. branch office traffic
B. east-west traffic
C. perimeter traffic
D. north-south traffic
Answer: B (メーッセージを残す**)**

最新問題: **181**
ドラッグ アンド ドロップの質問
次のステップを、パケット処理操作の最初から最後までの順序で配置します。

選択して配置します:

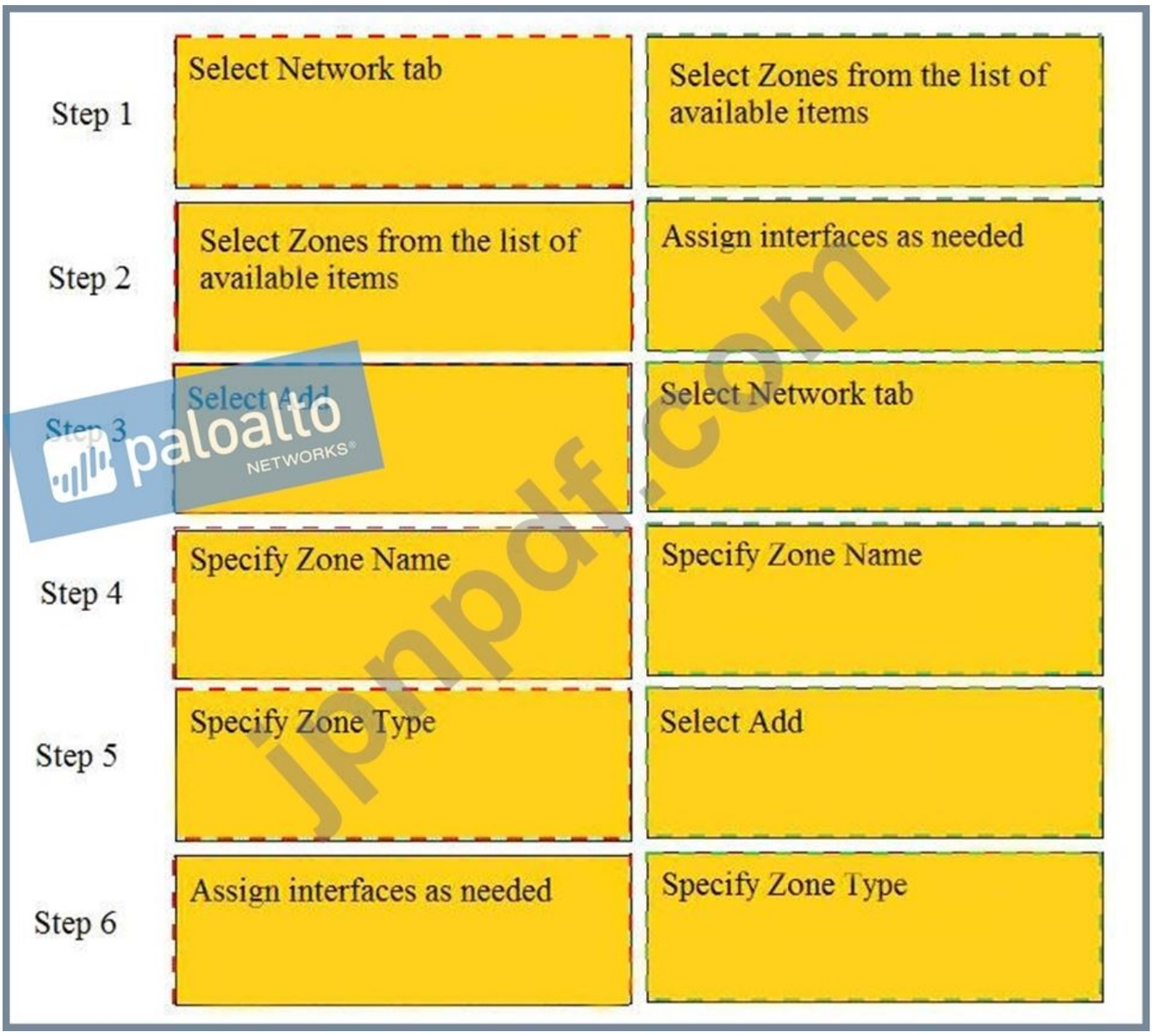
Answer:



最新問題**: 182**
パロアルトネットワーク ファイアウォールを使用して新しいセキュリティ ゾーンを作成するために必要な手順を指示します。

Step 1	Drag answer here	Select Zones from the list of available items
Step 2	Drag answer here	Assign interfaces as needed
Step 3	Drag answer here	Select Network tab
Step 4	Drag answer here	Specify Zone Name
Step 5	Drag answer here	Select Add
Step 6	Drag answer here	Specify Zone Type

Answer:



説明
ステップ 1 - [ネットワーク] タブを選択します
ステップ 2 - 使用可能なアイテムのリストからゾーンを選択します
ステップ 3 - [追加] を選択します
ステップ 4 - ゾーン名の指定
ステップ 5 - ゾーンのタイプを指定する
ステップ 6 - 必要に応じてインターフェイスを割り当てる

最新問題: **183**
How are Application Fillers or Application Groups used in firewall policy?
A. An Application Group is a dynamic way of grouping applications and can be configured as a nested member of an Application Group
B. An Application Filter is a dynamic way to group applications and can be configured as a nested member of an Application Group

C. An Application Group is a static way of grouping applications and cannot be configured as a nested member of Application Group
D. An Application Filter is a static way of grouping applications and can be configured as a nested member of an Application Group
Answer: (解答を表示する**)**

最新問題**: 184**
What must first be created on the firewall for SAML authentication to be configured?
A. Server Policy
B. Server Profile
C. Server Location
D. Server Group
Answer: B (メーッセージを残す**)**
A server profile identifies the external authentication service and instructs the firewall on how to connect to that authentication service and access the authentication credentials for your users. To configure SAML authentication, you must create a server profile and register the firewall and the identity provider (IdP) with each other. You can import a SAML metadata file from the IdP to automatically create a server profile and populate the connection, registration, and IdP certificate information. Reference: Configure SAML Authentication, Set Up SAML Authentication, Introduction to SAML

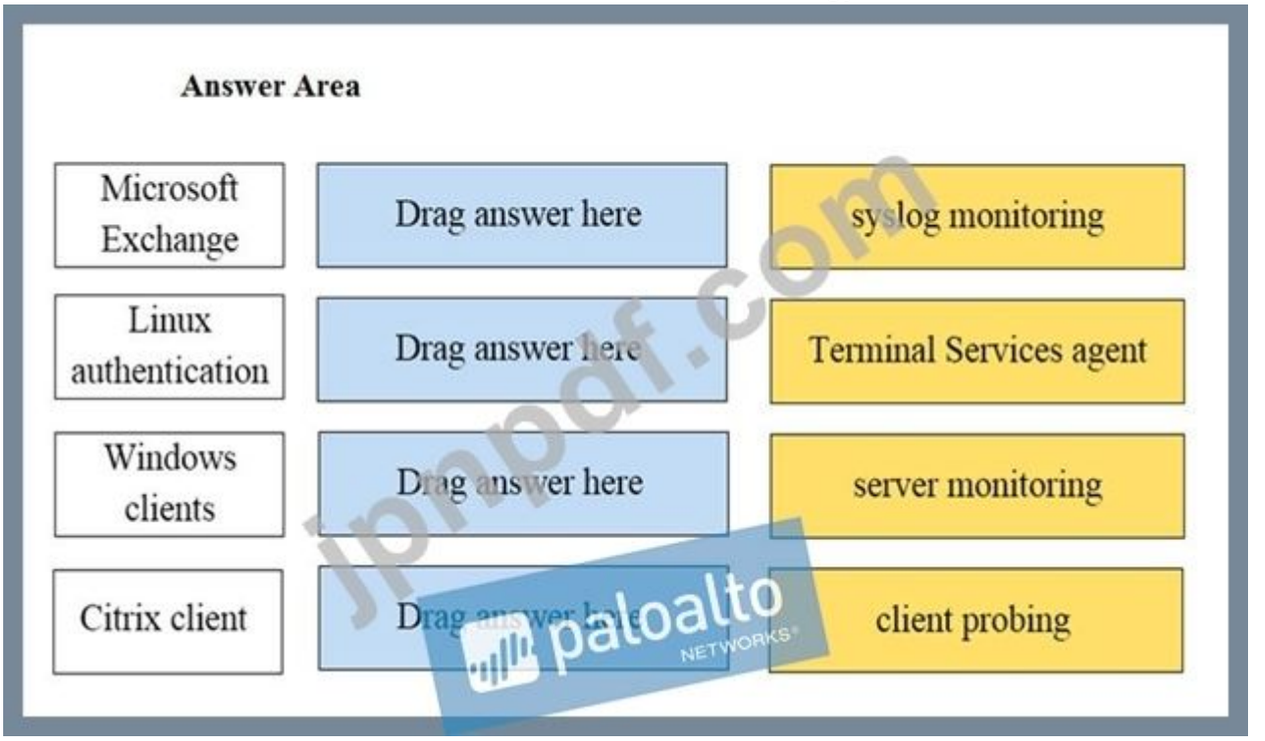
最新問題**: 185**
ファイアウォールで使用するウイルス対策アップデートをダウンロードする前に、管理者はどのライセンスを取得する必要がありますか?
A. 脅威の防止
B. 山火事
C. ウイルス対策
D. URL フィルタリング
Answer: A (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/subscriptions/all-subscriptions.html#idcaa6fc0b-3d53-4870-884d-a00d474bf98e

最新問題**: 186**
Which object would an administrator create to block access to all high-risk applications?
A. HIP profile
B. application filter
C. application group
D. Vulnerability Protection profile
Answer: B (メーッセージを残す**)**
Explanation/Reference:
Reference:

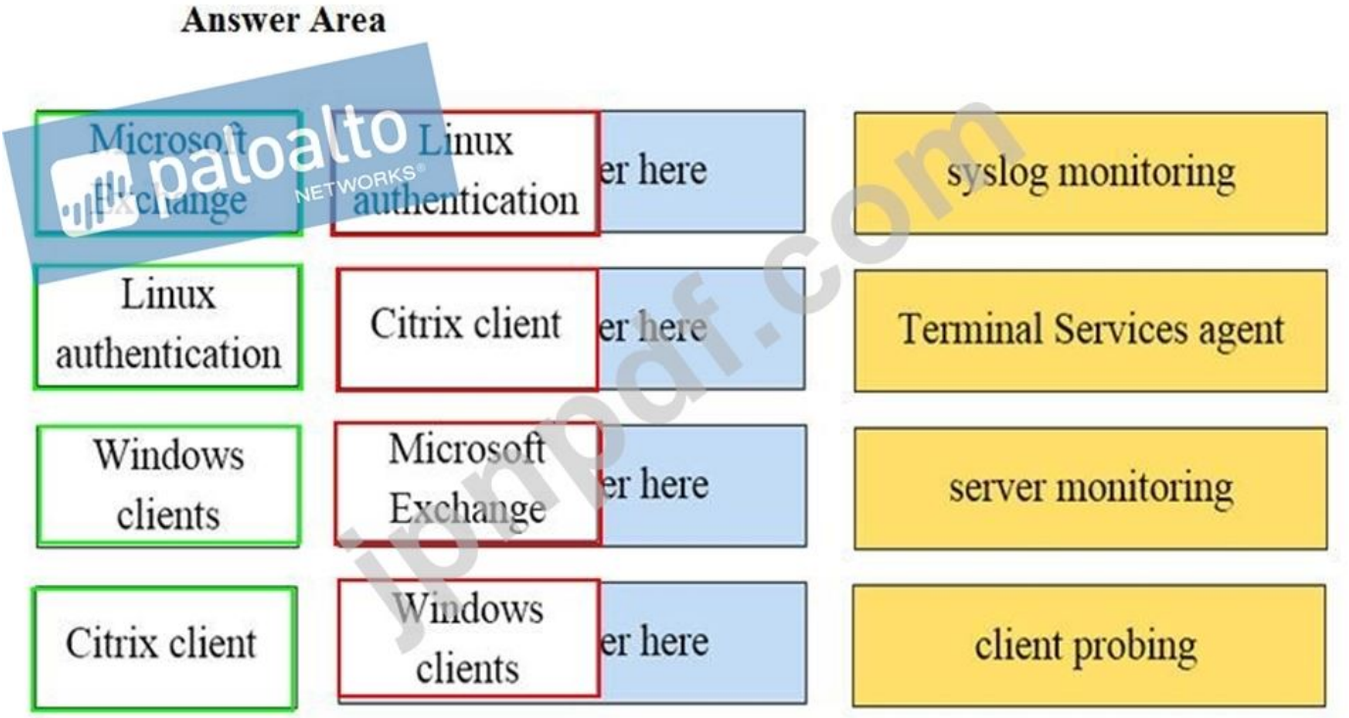
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKECA0

最新問題: 187

Match the network device with the correct User-ID technology.



Answer:



最新問題: 188

Based on the security policy rules shown, ssh will be allowed on which port?

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	None
3	Intrazone-default	Intrazone	Any	Any	(intrazone)	Any	Any	Any	Any	Allow	None
4	Interzone-default	Interzone	Any	Any	Any	Any	Any	Any	Any	Deny	None

A. same port as ssl and snmpv3
B. any port
C. only ephemeral ports
D. the default port
Answer: D (メーッセージを残す)

最新問題**: 189**
Choose the option that correctly completes this statement. A Security Profile can block or allow traffic _____.
A. on either the data place or the management plane.
B. after it is matched by a security policy rule that allows traffic.
C. before it is matched to a Security policy rule.
D. after it is matched by a security policy rule that allows or blocks traffic.
Answer: B (メーッセージを残す)
Reference:
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy.html

最新問題**: 190**
Place the following steps in the packet processing order of operations from first to last.

Answer:

最新問題: **191**

What is the minimum timeframe that can be set on the firewall to check for new WildFire signatures?

A. every 30 minutes

B. every 5 minutes

C. once every 24 hours

D. every 1 minute

Answer: B (メーッセージを残す**)**

Explanation

Firewalls with an active WildFire WildFire signatures every five minutes. If you do not have a WildFire subscription, are made available within 24-48 hours as part of the antivirus update for firewalls with an active Threat Prevention license.

https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-concepts/wildfire-sign

最新問題: **192**

An administrator would like to create a URL Filtering log entry when users browse to any gambling website. What combination of Security policy and Security profile actions is correct?

A. Security policy = allow, Gambling category in URL profile = alert

B. Security policy = deny. Gambling category in URL profile = block
C. Security policy = drop, Gambling category in URL profile = allow
D. Security policy = allow. Gambling category in URL profile = allow
Answer: (解答を表示する**)**

最新問題**: 193**
What are the two default behaviors for the intrazone-default policy? (Choose two.)
A. Allow
B. Logging disabled
C. Log at Session End
D. Deny
Answer: A,C (メーッセージを残す**)**
By default, the firewall implicitly allows intrazone traffic (within a zone) and implicitly denies interzone traffic (between zones).
By default, traffic allowed or denied by the implicit Security policy rules is not logged on the firewall.

最新問題**: 194**
あなたの会社は 1 つの建物の 1 フロアを占めており、単一のネットワーク上に 2 つの Active Directory ドメイン コントローラがあり、ファイアウォールの管理プレーンはわずかしか利用されていません。
ネットワーク内で十分なユーザー ID エージェントはどれですか?
A. ファイアウォールに展開された PAN-OS 統合エージェント
B. ドメイン メンバーの内部ネットワークにデプロイされた Windows ベースのエージェント
C. ネットワーク上に展開された Citrix ターミナル サーバー エージェント
D. 各ドメイン コントローラーにデプロイされた Windows ベースのエージェント
Answer: D (メーッセージを残す**)**
説明/参照:
参照：
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configureuser-mapping-using-the-windows-user- id-agent/configure-the-windows-based-user-id-agent-for-usermapping.html

最新問題**: 195**
An administrator wants to reference the same address object in Security policies on 100 Panorama managed firewalls, across 10 device groups and five templates.
Which configuration action should the administrator take when creating the address object?
A. Ensure that the Shared option is checked.
B. Ensure that the Shared option is cleared.
C. Ensure that Disable Override is cleared.

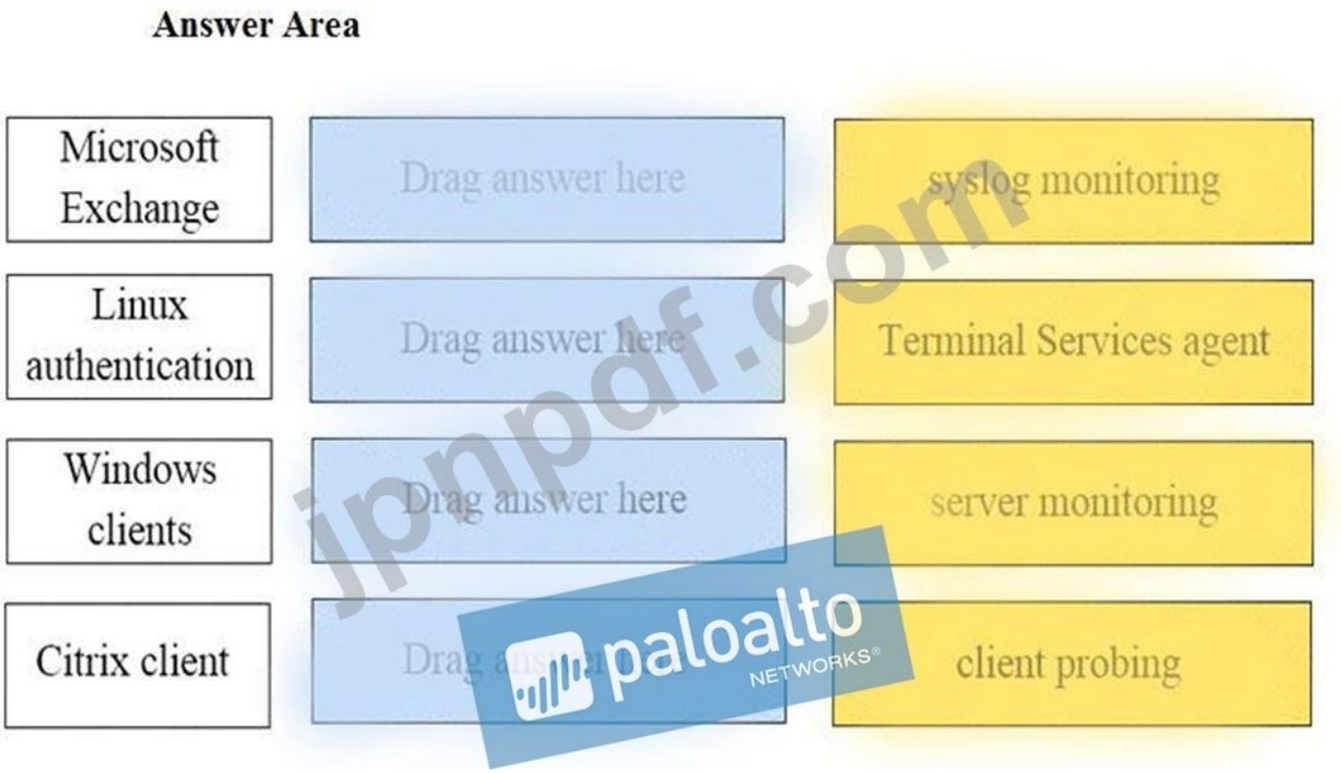
D. Tag the address object with the Global tag.

Answer: (解答を表示する)

To reference the same address object in Security policies on 100 Panorama-managed firewalls, across 10 device groups and five templates, the administrator should ensure that the Shared option is checked when creating the address object. This option allows the administrator to create a shared address object that is available to all device groups and templates on Panorama. The shared address object can then be used in multiple firewall policy rules, filters, and other functions1. This reduces the complexity and duplication of managing address objects across multiple firewalls2. References: Address Objects, Create a Shared Address Object, Certifications - Palo Alto Networks, Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) or [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)].

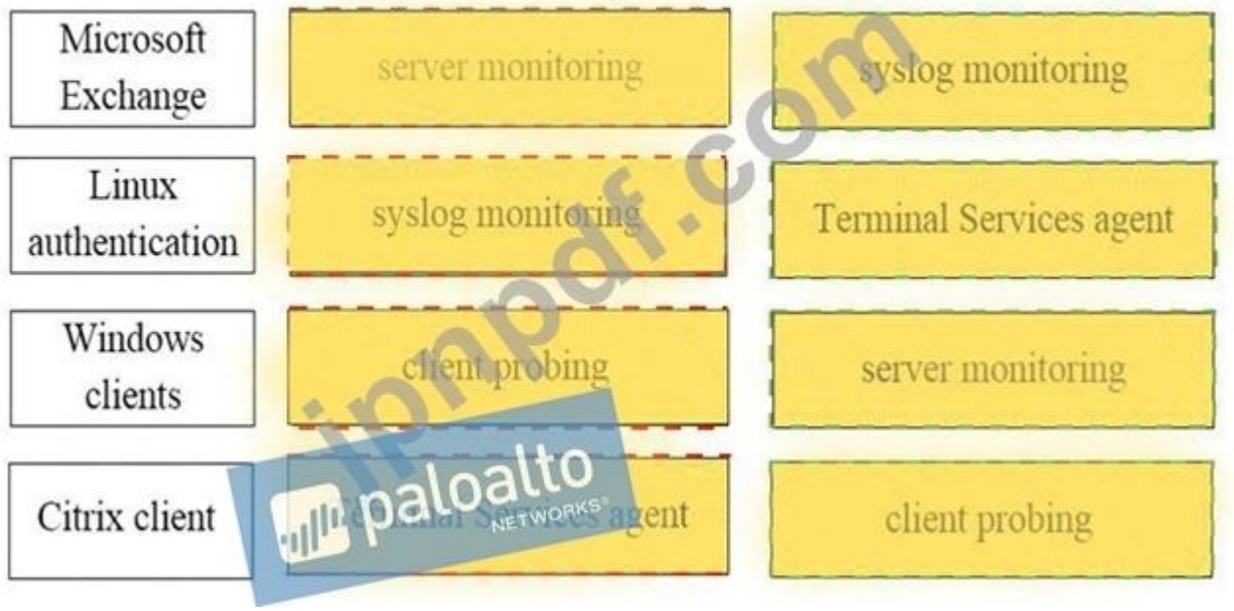
最新問題: 196

Match the network device with the correct User-ID technology.



Answer:

Answer Area



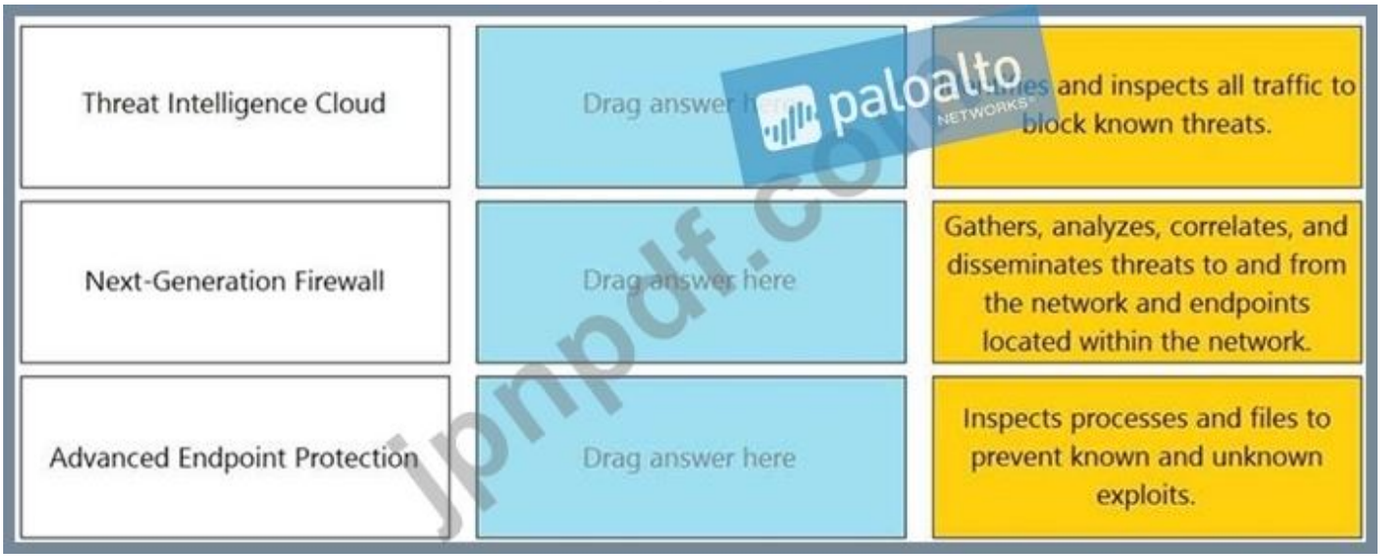
Explanation
Microsoft Exchange - Server monitoring
Linux authentication - syslog monitoring
Windows Client - client probing
Citrix client - Terminal Services agent

最新問題: **197**
An administrator receives a global notification for a new malware that infects hosts. The infection will result in the infected host attempting to contact a command-and-control (C2) server.
Which two security profile components will detect and prevent this threat after the firewall's signature database has been updated? (Choose two.)
A. vulnerability protection profile applied to outbound security policies
B. anti-spyware profile applied to outbound security policies
C. antivirus profile applied to outbound security policies
D. URL filtering profile applied to outbound security policies
Answer: B,D (メーッセージを残す)
Explanation/Reference:

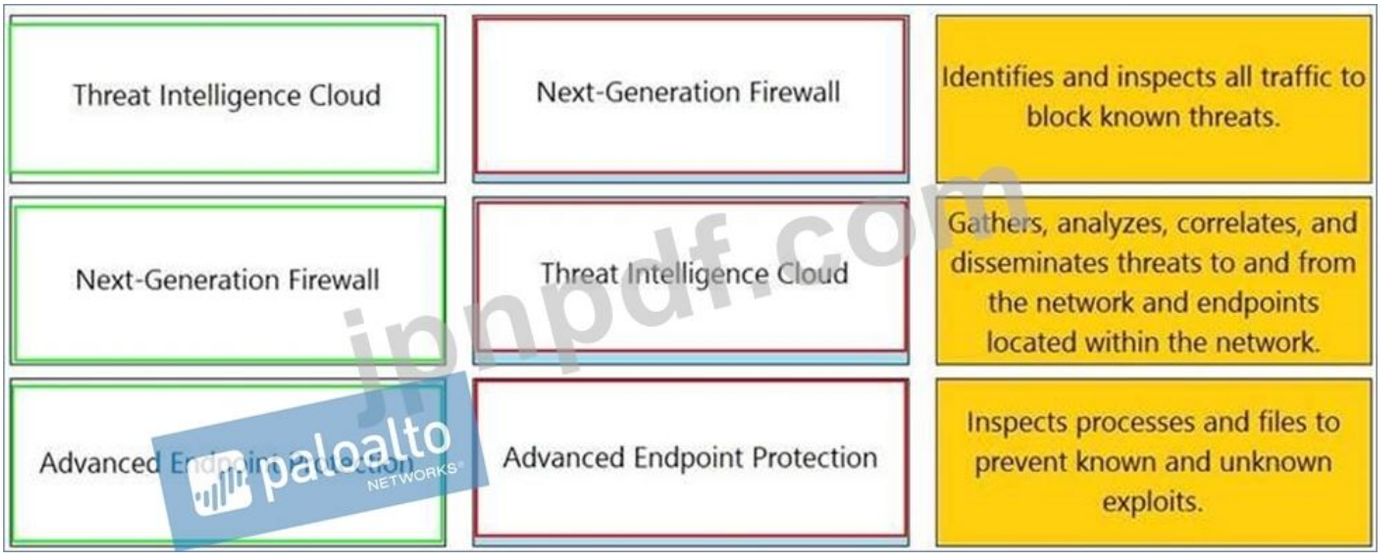
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/policy/create-best-practice-security-profiles

最新問題: **198**

Match each feature to the DoS Protection Policy or the DoS Protection Profile.



Answer:



最新問題: **199**

Which two configurations does an administrator need to compare in order to see differences between the active configuration and potential changes if committed? (Choose two.)

A. Running

B. Active

C. Device state

D. Candidate

Answer: A,D (メーッセージを残す**)**

最新問題: **200**

In which threat profile object would you configure the DNS Security service?
A. Anti-Spyware
B. URL Filtering
C. Antivirus
D. WildFire
Answer: A (メーッセージを残す**)**

最新問題**: 201**
管理者は、office-program サブカテゴリ内のすべてのアプリケーションにアクセスできるようにするには、どのオブジェクトを作成しますか?
A. HIP プロファイル
B. アプリケーションフィルター
C. URL カテゴリ
D. アプリケーショングループ
Answer: C (メーッセージを残す**)**

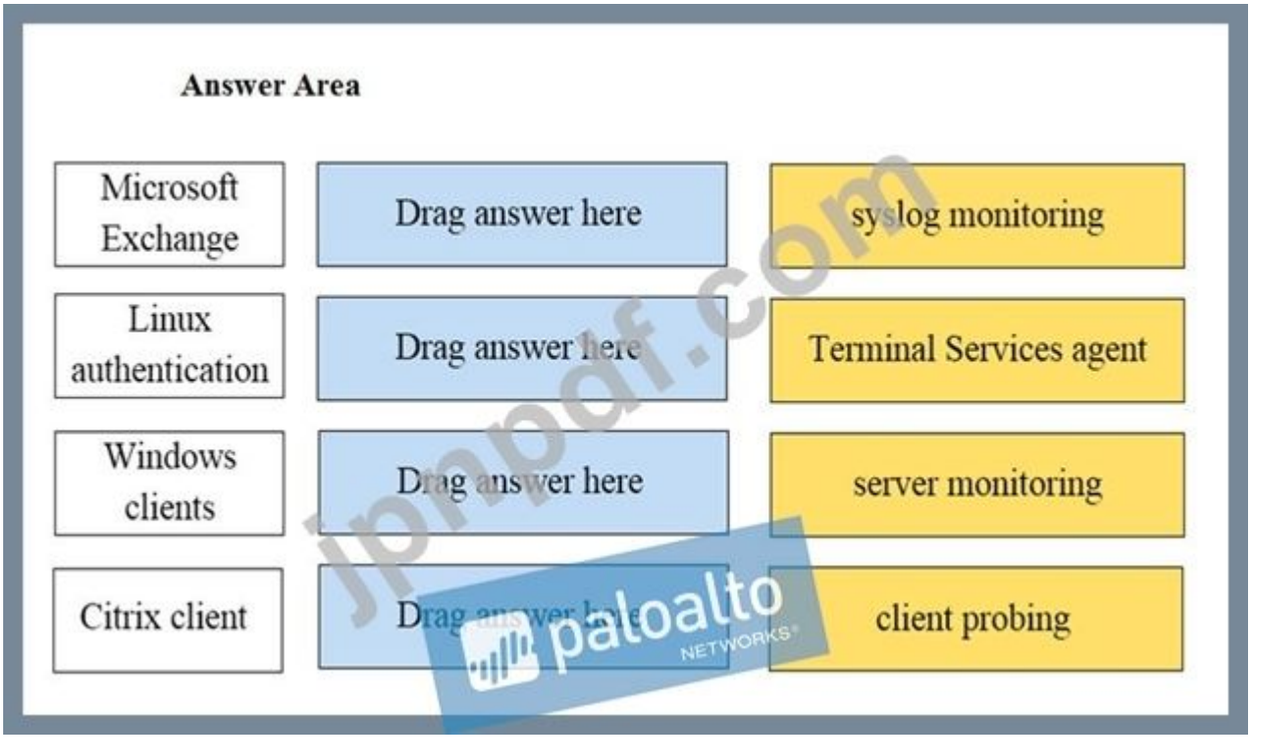
最新問題**: 202**
When creating an Admin Role profile, if no changes are made, which two administrative methods will you have full access to? (Choose two.)
A. web UI
B. XML API
C. command line
D. RESTAPI
Answer: A,D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-an-admin-role-profile

最新問題**: 203**
ローカル管理者アカウントの事前定義されたロールを利用する管理者タイプはどれですか?
A. スーパーユーザー
B. ロールベース
C. 動的
D. デバイス管理者
Answer: C (メーッセージを残す**)**
説明/参照: https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-cli-quick-start/get-started-with-the-cli/give-administrators-access-to- the-cli/administrative-privileges?PageSpeed=noscript

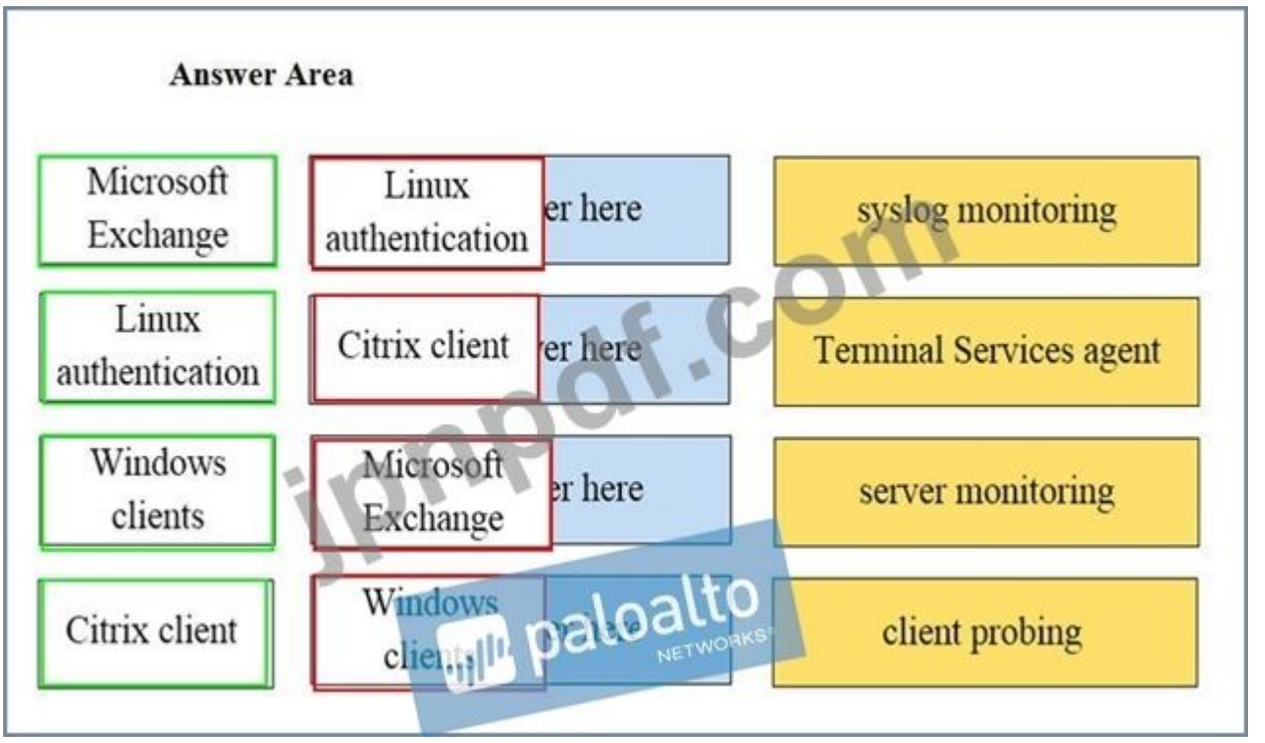
最新問題**: 204**
Which User-ID mapping method should be used for an environment with clients that do not authenticate to Windows Active Directory?

A. Windows session monitoring via a domain controller
B. passive server monitoring using the Windows-based agent
C. Captive Portal
D. passive server monitoring using a PAN-OS integrated User-ID agent
Answer: C (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/user-id/map-ip-addresses-to-users/map-ip-addresses-to-usernames-using-captive-portal.html

最新問題**: 205**
ネットワーク デバイスを正しい User-ID テクノロジと照合します。



Answer:



最新問題: **206**

表示されたスクリーンショットに基づいて、クリックするとポリシー ルールに一致するすべてのアプリケーションを表示するウィンドウが開くリンクが含まれる列はどれですか?

A. 確認されたアプリ

B. 許可されたアプリ

C. サービス

D. 名前

Answer: D (メーッセージを残す**)**

最新問題: **207**

When is an event displayed under threat logs?

A. When traffic matches a corresponding Security Profile

B. When traffic matches any Security policy

C. Every time a session is blocked

D. Every time the firewall drops a connection

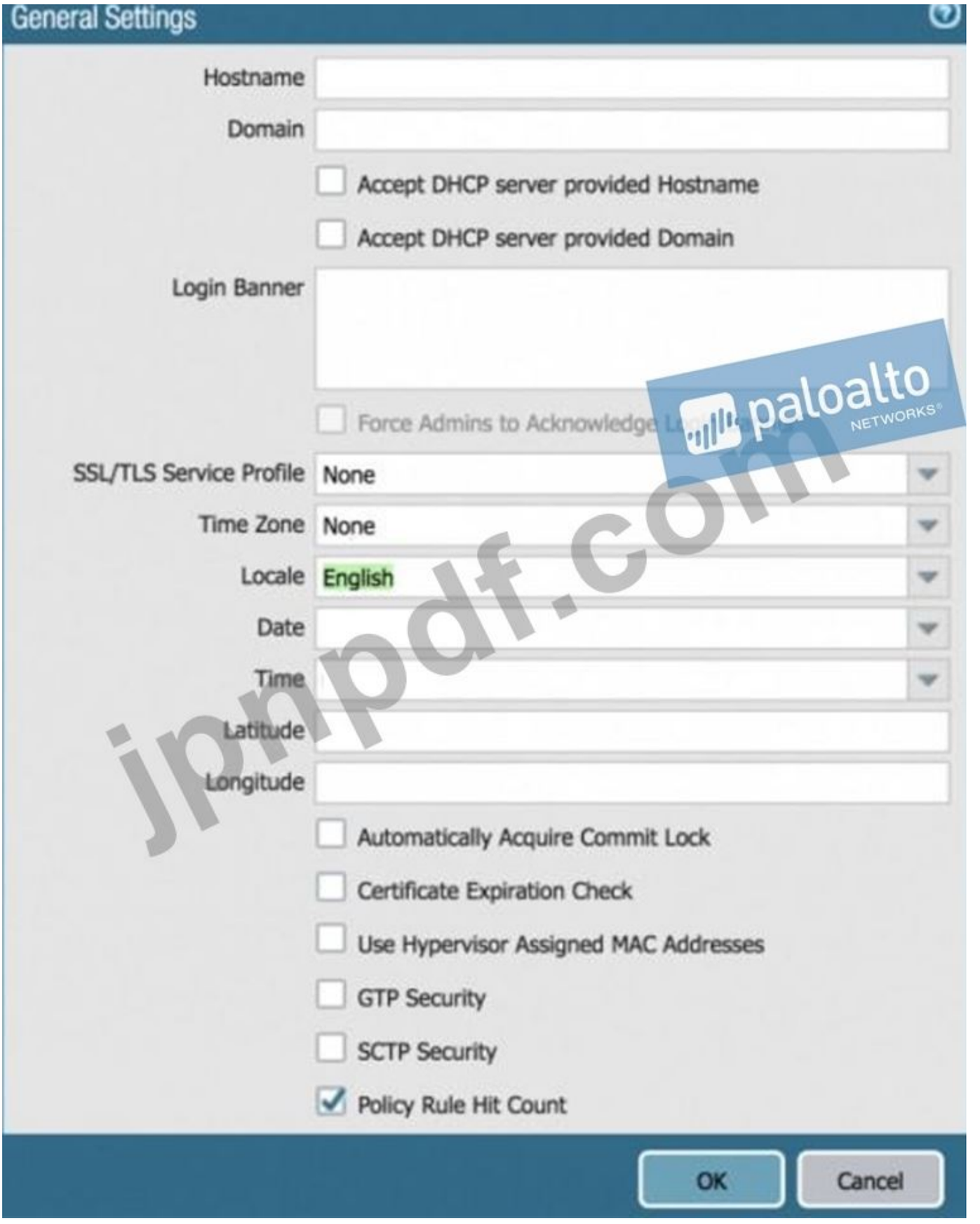
Answer: (解答を表示する**)**

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs#:~:text=Threat%20logs%20display%20entries%20when,security%20rule%20on%20the%20firewall.

最新問題: **208**
Which information is included in device state other than the local configuration?
A. uncommitted changes
B. audit logs to provide information of administrative account changes
C. system logs to provide information of PAN-OS changes
D. device group and template settings pushed from Panorama
Answer: D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-setup-operations.html

最新問題: **209**
管理用の HTTPS と GlobalProtect が同じインターフェイスで有効になっている場合、管理アクセスにはどの TCP ポートが使用されますか?
A. 80
B. 8443
C. 443
D. 4443
Answer: (解答を表示する**)**

最新問題: **210**
Based on the graphic, what is the purpose of the SSL/TLS Service profile configuration option?



A. It defines the SSUTLS encryption strength used to protect the management interface.

B. It defines the certificate to send to the client's browser from the management interface.

C. It defines the firewall's global SSL/TLS timeout values.

D. It defines the CA certificate used to verify the client's browser.

Answer: (解答を表示する**)**

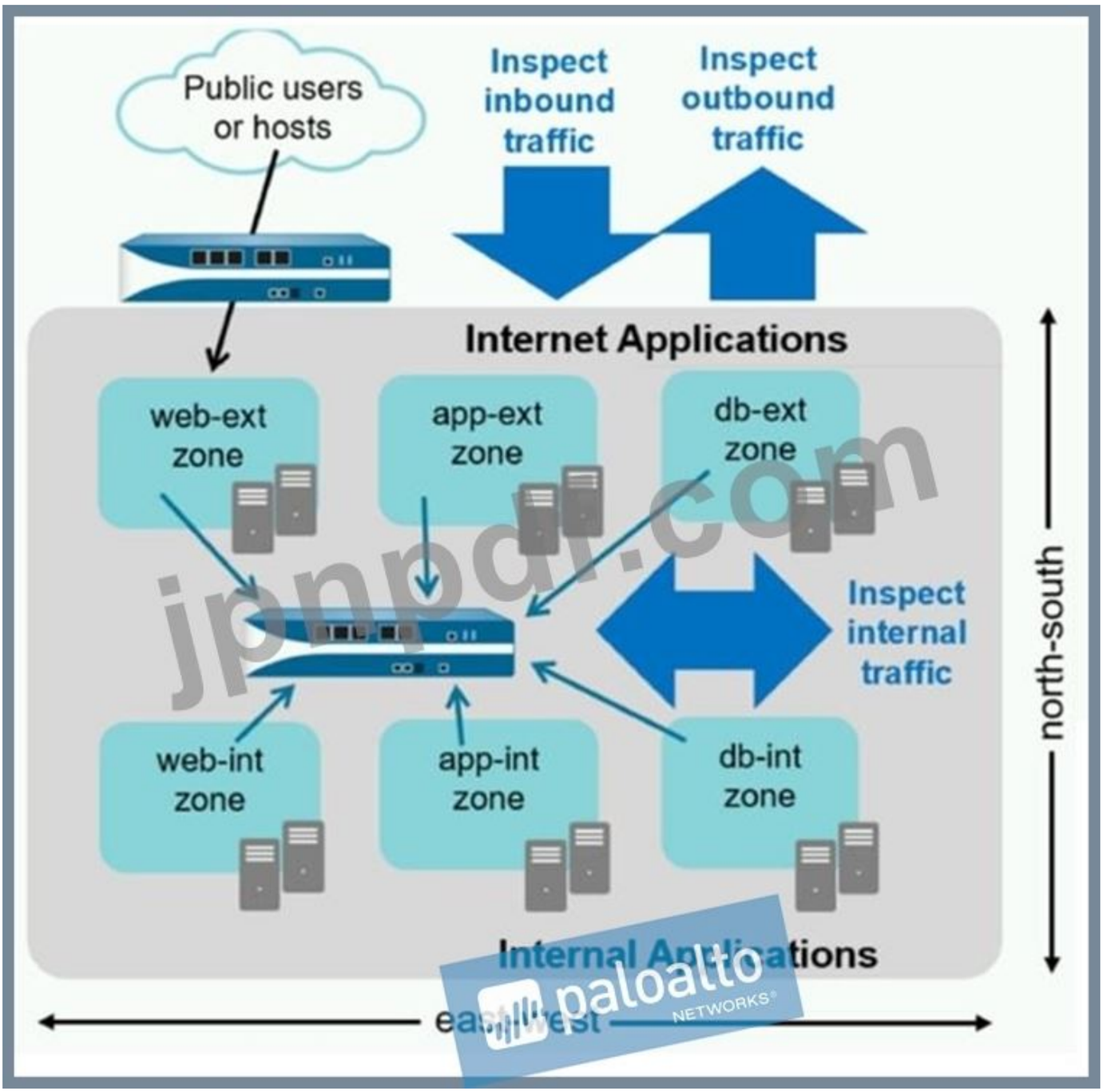
最新問題**: 211**
IP ワイルドカード マスク タイプのアドレス オブジェクトは、構成のどの部分で参照できますか?
A. セキュリティ ポリシー ルール
B. ACC グローバル フィルター
C. 外部動的リスト
D. NAT アドレス プール
Answer: A (メーッセージを残す**)**
IP ワイルドカード マスク タイプのアドレス オブジェクトは、セキュリティ ポリシー ルールでのみ使用できます。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/objects/objects-addresses IP ワイルドカード マスク
-- IP ワイルドカード アドレスを、IPv4 アドレスの後にスラッシュとマスク (ゼロで始まる必要があります) の形式で入力します。例えば、
10.182.1.1/0.127.248.0。ワイルドカード マスクのゼロ (0) ビットは、比較されるビットが 0 でカバーされる IP アドレスのビットと一致する必要があることを示します。マスク内の 1 ビットはワイルドカード ビットであり、そのビットは比較対象となる IP アドレスのビットと一致する必要はありません。1. IP アドレスとワイルドカード マスクをバイナリに変換します。マッチングを説明すると、バイナリ スニペット 0011 では、ワイルドカード マスク 1010 は 4 つの一致 (0001、0011、1001、および 1011) になります。

最新問題**: 212**
Which Security profile would you apply to identify infected hosts on the protected network using DNS traffic?
A. URL traffic
B. vulnerability protection
C. anti-spyware
D. antivirus
Answer: C (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

最新問題: **213**
An internal host needs to connect through the firewall using source NAT to servers of the internet. Which policy is required to enable source NAT on the firewall?
A. NAT policy with no internal or internet zone selected
B. pre-NAT policy with external source and any destination address
C. NAT policy with internal zone and internet zone specified
D. post-NAT policy with external source and any destination address
Answer: C (メーッセージを残す)

最新問題: **214**
In which threat profile object would you configure the DNS Security service?
A. Antivirus
B. Anti-Spyware
C. WildFire
D. URL Filtering
Answer: (解答を表示する)
https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security#:~:text=To%20enable%20DNS%20Security%2C%20you,to%20a%20security%20policy%20rule.

最新問題: **215**
You notice that protection is needed for traffic within the network due to malicious lateral movement activity. Based on the image shown, which traffic would you need to monitor and block to mitigate the malicious activity?



A. east-west traffic

B. perimeter traffic

C. branch office traffic

D. north-south traffic

Answer: A (メーッセージを残す**)**

最新問題**: 216**

Given the topology, which zone type should you configure for firewall interface E1/1?

A. Tap
B. Tunnel
C. Virtual Wire
D. Layer3
Answer: A (メーッセージを残す**)**
Tap - A Tap interface monitors traffic that is connected to a network switch's MIRROR/SPAN port.

最新問題**: 217**
管理者は、LAN ゾーン内の DNS トラフィックと一致するセキュリティ ポリシー ルールを作成する必要があり、さらに DMZ ゾーン内の DNS トラフィックと一致する必要もあります。管理者は、DMZ ゾーンと LAN ゾーン間のトラフィックを許可したくないです。
どのセキュリティ ポリシー ルール タイプを使用する必要がありますか?
A. ユニバーサル
B. ゾーン間
C. イントラゾーン
D. デフォルト
Answer: D (メーッセージを残す**)**

最新問題**: 218**
IP アドレスをユーザー名にマッピングする有効な 3 つの方法は何ですか? 3つお選びください。）
A. XML API を使用する
B. DHCP リレー ログ
C. GlobalProtect エージェントを使用して GlobalProtect ゲートウェイに接続するユーザー
D. HTTP ヘッダー内に挿入されたユーザー名
E. WildFire 評決レポート
Answer: (解答を表示する**)**
Palo Alto Networks ファイアウォールは、User-ID エージェント、Captive Portal、GlobalProtect、XML API、HTTP ヘッダーなどのさまざまな方法を使用して、IP アドレスをユーザー名にマップできます。これらの方法により、ファイアウォールは IP アドレスだけではなくユーザー ID に基づいてセキュリティ ポリシーを適用できます。これらの方法には次のようなものがあります。

XML API の使用: XML API を使用すると、外部システムは HTTPS 要求を使用してユーザー マッピング情報をファイアウォールに送信できます。ファイアウォールはこの情報を使用して、IP アドレスの背後にあるユーザーを識別し、適切なポリシーを適用できます1。
GlobalProtect エージェントを使用して GlobalProtect ゲートウェイに接続するユーザー: GlobalProtect は、ユーザーのデバイスとファイアウォールの間に VPN トンネルを確立することにより、ネットワークへの安全なリモート アクセスを提供します。ユーザーが GlobalProtect エージェントを使用して GlobalProtect ゲートウェイに接続すると、ファイアウォールはユーザーを認証し、ユーザーの IP アドレスをユーザー名 1 にマップできます。
HTTP ヘッダー内に挿入されたユーザー名: ファイアウォールは、Web トラフィックの HTTP ヘッダーからユーザー名を抽出することもできます。この方法では、Web サーバーまたはプロキシ サーバーが、ファイアウォールが読み取れるカスタム HTTP ヘッダーにユーザー名を挿入する必要があります。ファイアウォールはこの情報を使用して、IP アドレスをユーザー名 1 にマッピングできます。
参考資料: IP アドレスをユーザーにマップする、認定資格 - Palo Alto Networks、Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0) または Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)。

最新問題**: 219**
以下のスクリーンショットを確認してください。含まれる情報に基づいて、どのプロトコル デコーダーが機械学習の一致を検出し、脅威ログ エントリを作成し、トラフィックを許可しますか?

A. smb

B. 画像
C. ftp
D. http2
Answer: (解答を表示する**)**
スクリーンショットによると、imap、pop3、smtp のみがデフォルト (アラート) アクションを持ち、アプリケーション トラフィック フローごとにアラートを生成します。アラートは脅威ログに保存されます。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-profiles

最新問題**: 220**
Which user mapping method could be used to discover user IDs in an environment with multiple Windows domain controllers?
A. Active Directory monitoring
B. Windows session monitoring
C. Windows client probing
D. domain controller monitoring
Answer: D (メーッセージを残す**)**
To ensure the most comprehensive mapping of users, you must monitor all domain controllers that process authentication for users you want to map. You might need to install multiple User-ID agents to efficiently monitor all of your resources.

最新問題**: 221**
Which two settings allow you to restrict access to the management interface? (Choose two)
A. restricting HTTP and telnet using App-ID
B. permitted IP addresses
C. administrative management services
D. enabling the Content-ID filter
Answer: (解答を表示する**)**

最新問題**: 222**
Drag and Drop Question
Match the cyber-attack lifecycle stage to its correct description.
Select and Place:

Answer:

最新問題: **223**

Which administrator type utilizes predefined roles for a local administrator account?

A. Superuser

B. Role-based

C. Dynamic

D. Device administrator

Answer: (解答を表示する**)**

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-role-types#id8b324bf1-eac8-40e1-82d5-6f82ff761fa9

最新問題: **224**

What is a prerequisite before enabling an administrative account which relies on a local firewall user database?

A. Configure an authentication policy

B. Configure an authentication sequence

C. Configure an authentication profile

D. Isolate the management interface on a dedicated management VLAN

Answer: C (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-a-firewall-administrator-account

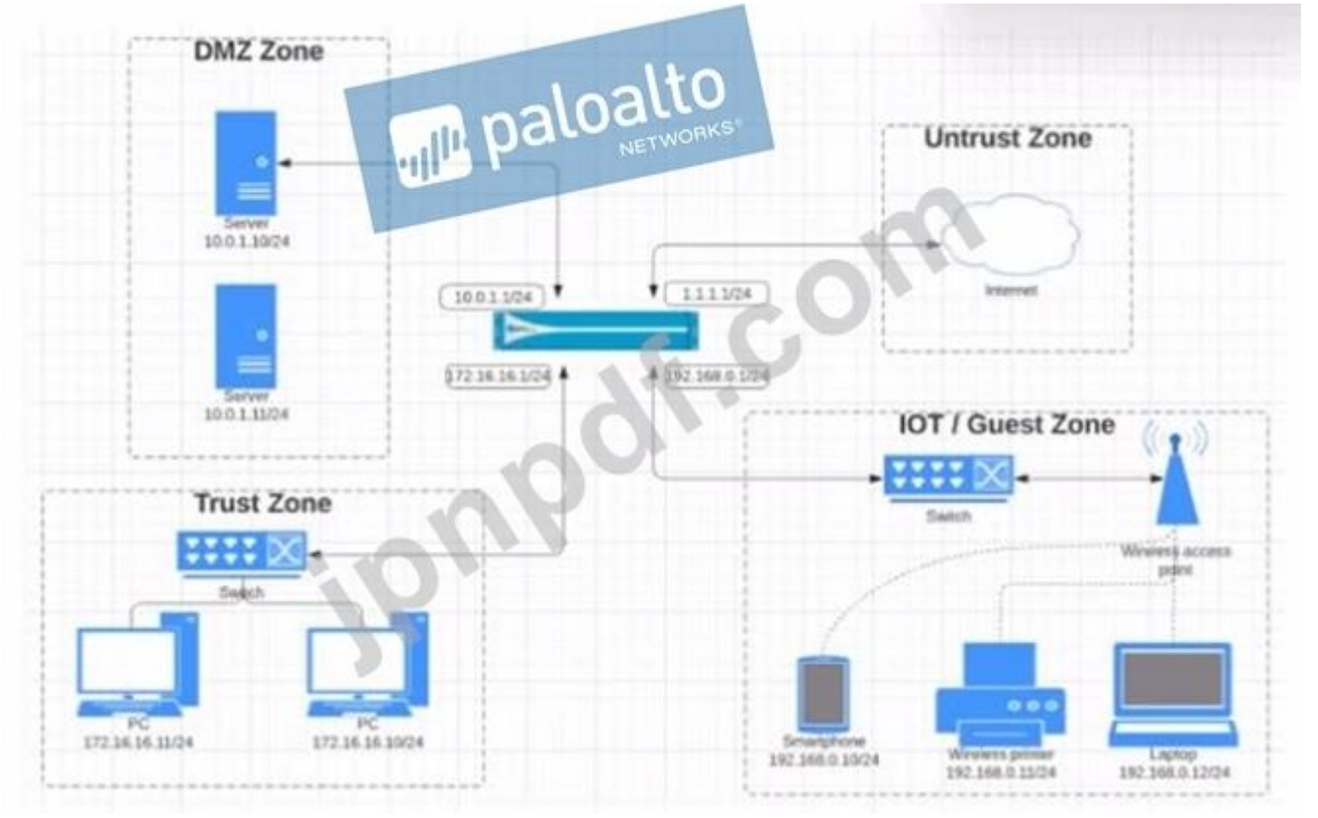
最新問題: **225**
A network has 10 domain controllers, multiple WAN links, and a network infrastructure with bandwidth needed to support mission-critical applications. Given the scenario, which type of User-ID agent is considered a best practice by Palo Alto Networks?
A. Windows-based agent on a domain controller
B. Citrix terminal server with adequate data-plane resources
C. PAN-OS integrated agent
D. Captive Portal
Answer: A (メーッセージを残す)

最新問題: **226**
NAT を含むセキュリティ ポリシーを作成するときに使用される 2 つの一致基準はどれですか? (2つお選びください。)
A. Pre-NAT ゾーン
B. NAT 後のアドレス
C. NAT 前のアドレス
D. NAT 後のゾーン
Answer: (解答を表示する)

最新問題: **227**
In a File Blocking profile, which two actions should be taken to allow file types that support critical apps?
(Choose two.)
A. Clone and edit the Strict profile.
B. Edit the Strict profile.
C. Use URL filtering to limit categories in which users can transfer files.
D. Set the action to Continue.
Answer: (解答を表示する)

最新問題: **228**

View the diagram. What is the most restrictive, yet fully functional rule, to allow general Internet and SSH traffic into both the DMZ and Untrust/Internet zones from each of the IOT/Guest and Trust Zones?



A.

B.

C.

D.

Answer: (解答を表示する)

最新問題: **229**
Which Security policy match condition would an administrator use to block traffic from IP addresses on the Palo Alto Networks EDL of Known Malicious IP Addresses list?
A. destination address
B. source address
C. destination zone
D. source zone
Answer: B (メーッセージを残す)
There are many ways to enforce web page access beyond only blocking and allowing certain sites. For example, you can use multiple categories per URL to allow users to access a site, but block particular functions like submitting corporate credentials or downloading files. You can also use URL categories to enforce different types of policy, such as Authentication, Decryption, QoS, and Security.
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-category-as-policy-match-criteria.html

最新問題: **230**
Which solution is a viable option to capture user identification when Active Directory is not in use?
A. Authentication Portal
B. group mapping
C. Directory Sync Service
D. Cloud Identity Engine
Answer: A (メーッセージを残す)