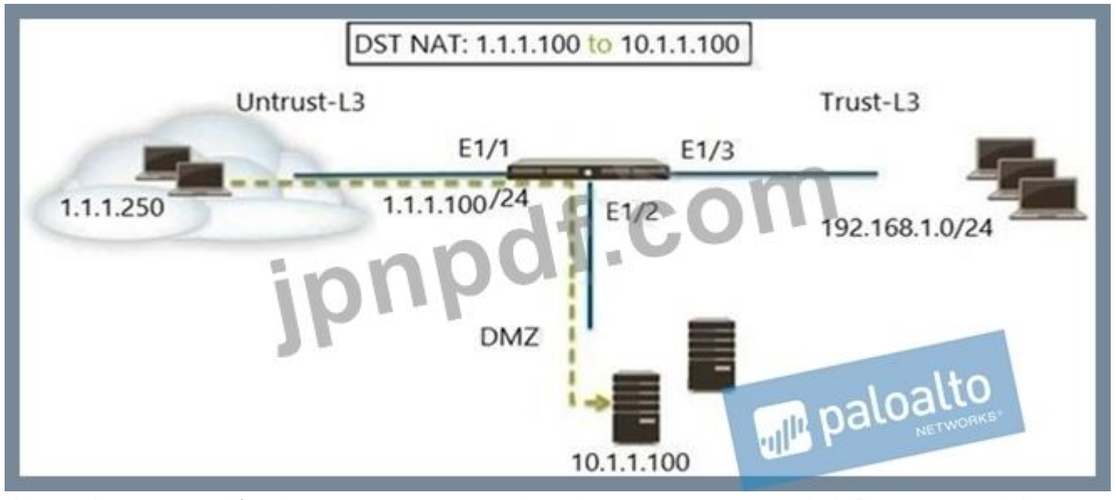
PaloAltoNetworks.PCNSA.v2026-08-03.q289

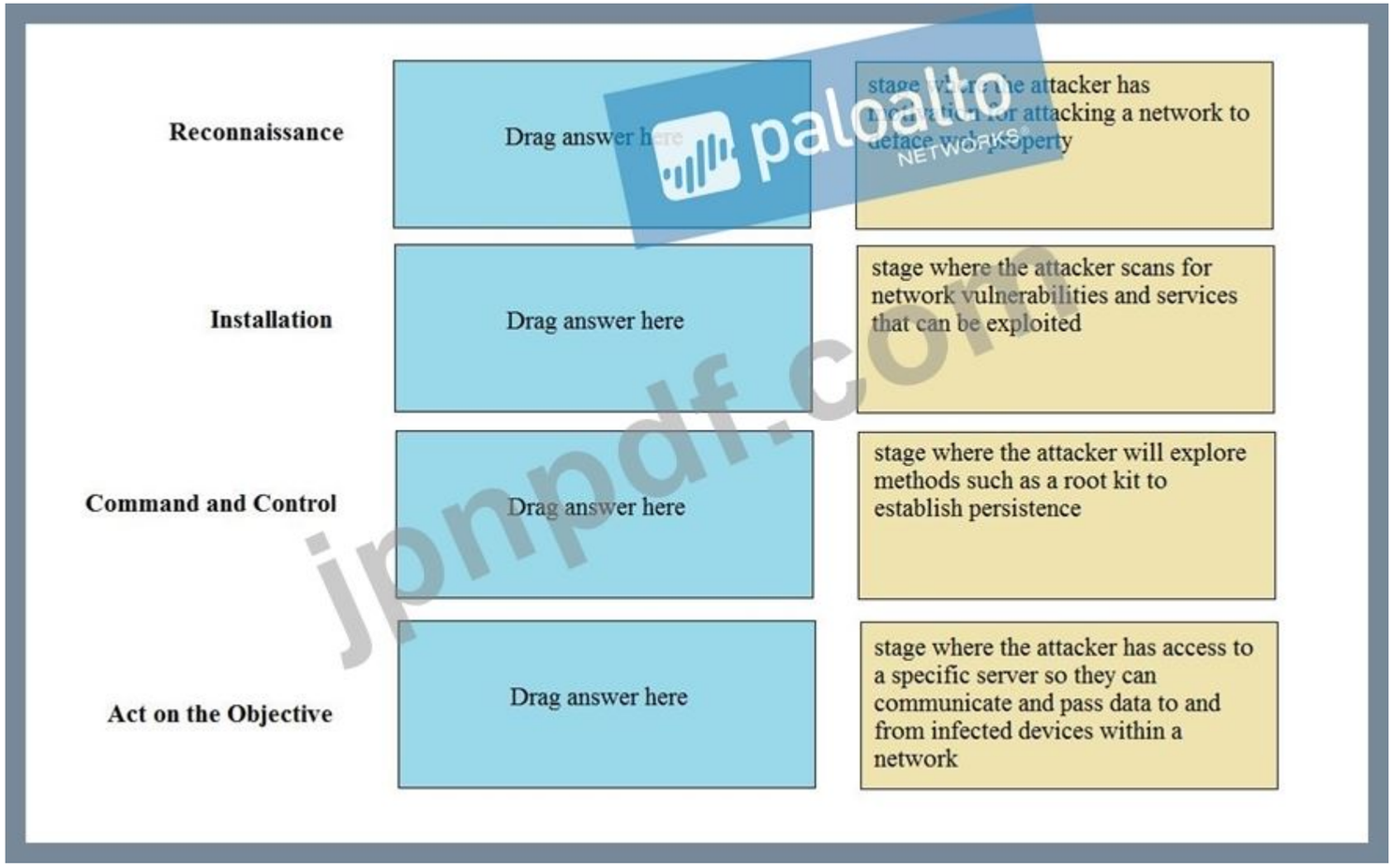
試験コード:	PCNSA
試験名称:	Palo Alto Networks Certified Network Security Administrator
認定資格:	Palo Alto Networks
無料問題数:	289
バージョン:	v2026-08-03
アクセス数:	115
ページビュー数:	2890
https://www.jpnpdf.com/PaloAltoNetworks.PCNSA.v2026-08-03.q289-mondaishu.html	

最新問題: **1**
図を参照してください。DMZ内のWebサーバーが、DNATによってパブリックアドレスにマッピングされています。



どのセキュリティポリシールールで、Webサーバーへのトラフィックが許可されますか？
A. DMZ (10.1.1.100) への不信 (任意)、ウェブブラウジング - 許可
B. DMZ (1.1.1.100) への不信 (任意)、ウェブブラウジング - 許可
C. 信頼しない (任意) から信頼しない (1.1.1.100)、ウェブブラウジング - 許可
D. Untrust (any) から Untrust (10.1.1.100)、Web ブラウジング - 許可
Answer: (解答を表示する**)**

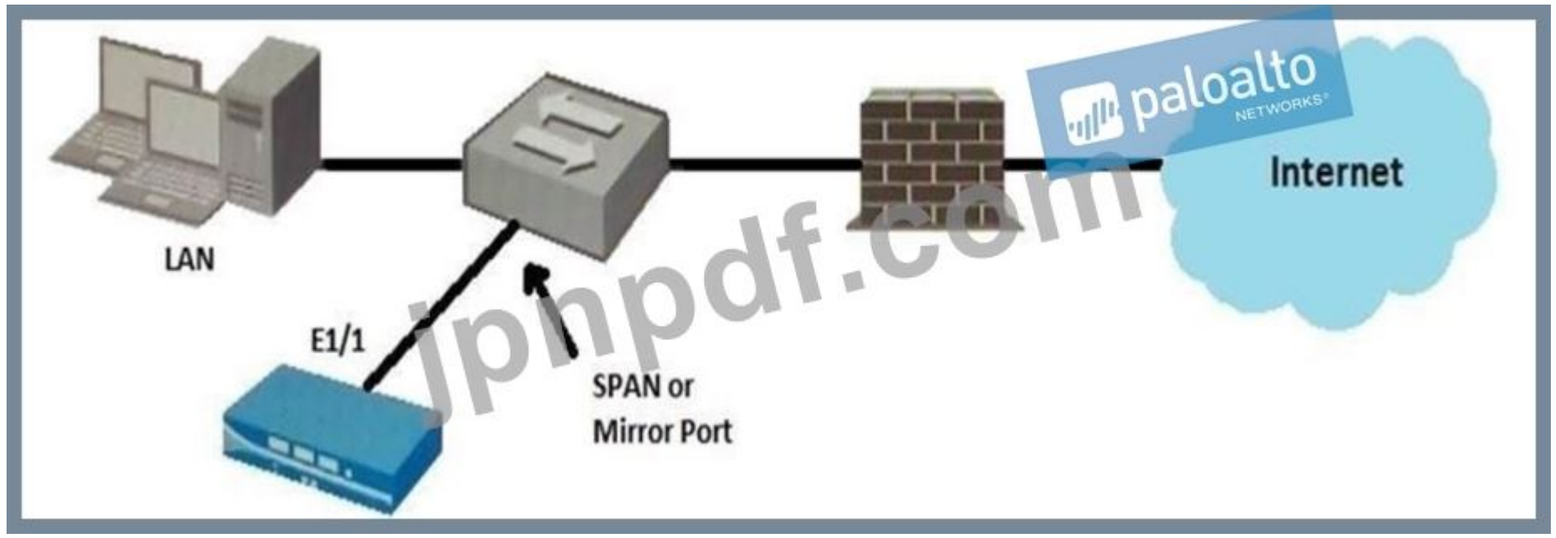
最新問題: **2**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。



Answer:

Reconnaissance	stage where the attacker scans for network vulnerabilities and services that can be exploited	stage where the attacker has motivation for attacking a network to deface web property
Installation	stage where the attacker will explore methods such as a root kit to establish persistence	stage where the attacker scans for network vulnerabilities and services that can be exploited
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	stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective	stage where the attacker has motivation for attacking a network to deface web property	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

最新問題: **3**



トポロジーを考慮すると、ファイアウォールインターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？

A. バーチャルワイヤー

B. タップ

C. レイヤー3

D. トンネル

Answer: B (メーッセージを残す**)**

最新問題: 4

PAN-OS 10.0でポートベースのセキュリティポリシールールの一覧を表示するパスはどれですか？

A. ポリシー > セキュリティ > ルールの使用 > アプリが指定されていません

B. ポリシー > セキュリティ > ルール使用 > ポートのみ指定

C. ポリシー > セキュリティ > ルールの使用 > ポートベースのルール

D. ポリシー > セキュリティ > ルールの使用状況 > 未使用のアプリ

Answer: A (メーッセージを残す**)**

https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-port-based-to-app-id-based-security-policy-rules.html

最新問題: 5

スクリーンショットに基づいて、Userグループ内の ĩt」というラベルの付いたグループの目的は何ですか？

			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. グループ ĩt」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. 全てのポートでITアプリケーションへのアクセスを許可します。

C. DMZゾーン内のサーバーに ĩ任意の」ユーザーがアクセスできるようにします。

D. グループ DMZ」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。

Answer: A (メーッセージを残す**)**

最新問題: **6**
Palo Alto Networksファイアウォールで設定可能なイーサネットインターフェースの種類はどれですか？ 3つ選択してください。）
A. バーチャルワイヤー
B. タップ
C. ダイナミック
D. レイヤー3
E. 静電気
Answer: A,B,D (メーッセージを残す**)**
Palo Alto Networksのファイアウォールは、ファイアウォール上で設定可能な3種類のイーサネットインターフェイスをサポートしています。
仮想ワイヤ、タップ、レイヤー31。これらのインターフェースタイプは、ファイアウォールがトラフィックを処理し、セキュリティポリシーを適用する方法を決定します。これらのインターフェースタイプの特性の一部を以下に示します。
仮想ワイヤ：仮想ワイヤインターフェイスを使用すると、ファイアウォールはパケットを変更したりルーティングに影響を与えたりすることなく、2 つのネットワークセグメント間でトラフィックを透過的に通過させることができます。ファイアウォールは、仮想ワイヤの送信元および宛先ゾーンに基づいて、セキュリティポリシーを適用したり、トラフィックを検査したりすることができます。
タップ :タップインターフェイスを使用すると、ファイアウォールはネットワークスイッチまたはルータからのトラフィックを、トラフィックフローに影響を与えることなく受動的に監視できます。ファイアウォールはタップインターフェイスからトラフィックを受信することしかできず、そこからトラフィックを送信することはできません。ファイアウォールは、タップインターフェイスの送信元ゾーンと宛先ゾーンに基づいてセキュリティポリシーを適用し、トラフィックを検査できます。
レイヤ 3: レイヤ 3 インターフェイスを使用すると、ファイアウォールはルータとして機能し、ネットワーク ルーティングに参加できます。ファイアウォールはレイヤ 3 インターフェイスからトラフィックを送受信し、セキュリティ ポリシーを適用し、インターフェイスの送信元および宛先 IP アドレスとゾーンに基づいてトラフィックを検査できます 4。
参考資料: Ethernet インターフェイスの種類、仮想ワイヤ インターフェイス、タップ インターフェイス、レイヤ 3 インターフェイス、PAN-OS 10.1 の更新された認定、[Palo Alto Networks 認定ネットワーク セキュリティ管理者 (PAN-OS
[10.0)] または [Palo Alto Networks Certified Network Security Administrator (PAN-OS 10.0)]。

最新問題: **7**
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、どのような設定が必要ですか？
A. カスタムオブジェクト
B. サービスグループ
C. アドレスグループ
D. アプリケーショングループ
Answer: (解答を表示する**)**

最新問題: **8**
DNSセキュリティのサブスクリプションをご利用の場合、クラウドベースの署名データベースはいつから、新しく追加されたDNS署名へのアクセスをユーザーに提供し始めますか？
A. アップデートをダウンロードしてから5分以内に
B. アップデートをダウンロードするとすぐに
C. アップデートをダウンロードせずに5分以内に
D. アップデートをダウンロードすることなく、即座に
Answer: D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/cloud-delivered-dns-signatures

最新問題: **9**
セキュリティプロファイルは、どの時点でトラフィックをブロックまたは許可できますか？
A. データプレーンまたは管理プレーンのいずれか
B. セキュリティポリシールールに一致し、トラフィックが許可された後
C. セキュリティポリシールールに一致する前
D. セキュリティポリシールールに一致し、トラフィックを許可またはブロックした後
Answer: B (メーッセージを残す**)**

最新問題: **10**
ネットワーク図を考慮すると、信頼済みユーザーとゲストユーザーの両方が、SSH、Webブラウジング、SSLアプリケーションを使用して、一般的なインターネットおよびDMZサーバーにアクセスできるようにする必要があります。目的の結果を達成するポリシーはどれですか？
A.


B.


C.


D.


Answer: (解答を表示する**)**

最新問題: **11**
管理者は、外部動的リストにIPアドレス範囲を持っており、そのアドレス範囲内の特定のIPアドレスに対して例外を作成したいと考えています。
管理者はどのような手順を踏むべきでしょうか？
A. リストエントリー覧からアドレス範囲を選択します。IPアドレスが表示された列が開きます。除外するエントリを選択します。
B. 正規表現を使用してエントリを定義し、アドレス範囲から特定の IP アドレスを手動例外リストに追加します。
C. アドレス範囲を手動例外リストに追加し、エントリを選択して IP アドレスを除外します。

D. 範囲内の各IPアドレスをリストエントリとして追加し、手動例外リストに追加することでIPアドレスを除外します。
Answer: B (メーッセージを残す**)**

最新問題**: 12**
NetSec マネージャーは、カスタマイズされた権限を持つ新しいファイアウォール管理者プロファイルを作成するよう依頼されました。新しいファイアウォール管理者は、TSF ファイルのダウンロードとダンプファイルの起動は可能である必要がありますが、デバイスの再起動はできないようにする必要があります。
NetSecマネージャーは、新しいファイアウォール管理者ロールプロファイルをどこで設定すればよいですか？
A. デバイス > 管理者ロール > 追加 > XML API > 設定
B. デバイス > 管理者ロール > 追加 > XML API > 操作リクエスト
C. デバイス > 管理者ロール > 追加 > Web UI > サポート
D. デバイス > 管理者ロール > 追加 > Web UI > 操作
Answer: (解答を表示する**)**

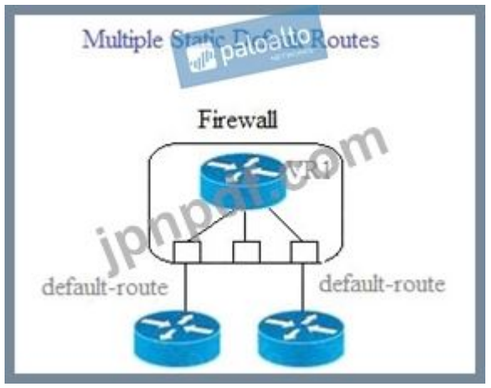
最新問題**: 13**
Palo Alto Networksのどのファイアウォールセキュリティプラットフォームが、インターネットゲートウェイとして展開されたトラフィックを検査することで、モバイルエンドポイントのネットワークセキュリティを提供しますか？
A. 絞り
B. グローバルプロテクト
C. パノラマ
D. オートフォーカス
Answer: B (メーッセージを残す**)**

最新問題**: 14**
ユーザー名を動的ユーザーグループに含めるためにタグ付けするには、どの2つの機能を利用できますか？ 2つ選択してください）
A. XML API
B. ログ転送の自動タグ付け
C. GlobalProtectエージェント
D. ユーザーID Windowsベースエージェント
Answer: A,D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profil

最新問題**: 15**
管理者は、インターネットからFTPサーバーへのトラフィックを密かに遮断したいと考えている。
管理者はどのセキュリティポリシーアクションを選択すべきでしょうか？
A. サーバーリセット
B. ドロップ
C. 拒否する
D. ブロック
Answer: B (メーッセージを残す**)**

最新問題: **16**
セキュリティ管理者がApp-IDのアップデートを自動的にダウンロードしてインストールするように設定しました。同社は現在、App-IDでSuperApp_baseとして識別されるアプリケーションを使用しています。
コンテンツ更新通知によると、パロアルトネットワークスはSuperApp_chatとSuperApp_downloadというラベルの新しいアプリ署名を追加し、30日以内に展開する予定だ。
この情報に基づくと、30日経過後、スーパーアプリのトラフィックはどのように影響を受けるのでしょうか？
A. SuperApp_chatおよびSuperApp_downloadに一致するすべてのトラフィックは、SuperAppベースのアプリケーションに一致しなくなったため拒否されます。
B. アプリは自動的にダウンロードおよびインストールされたため、影響はありません。
C. ファイアウォールがルールをApp-IDインターフェースに自動的に追加するため、影響はありません。
D. SuperApp_base、SuperApp_chat、SuperApp_download に一致するすべてのトラフィックは、セキュリティ管理者がアプリケーションを承認するまで拒否されます。
Answer: A (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: **17**
このシナリオにおいて、複数の静的デフォルトルートに関して正しい記述はどれですか？ 2つ選択してください。）



A. 経路監視では、経路が使用可能かどうかは判断されません。
B. 最も指標値が低いルートが積極的に利用されています
C. 最も高い指標を持つルートが積極的に利用されています
D. 経路監視により、経路が使用可能かどうかを判断します。
Answer: B,D (メーッセージを残す**)**

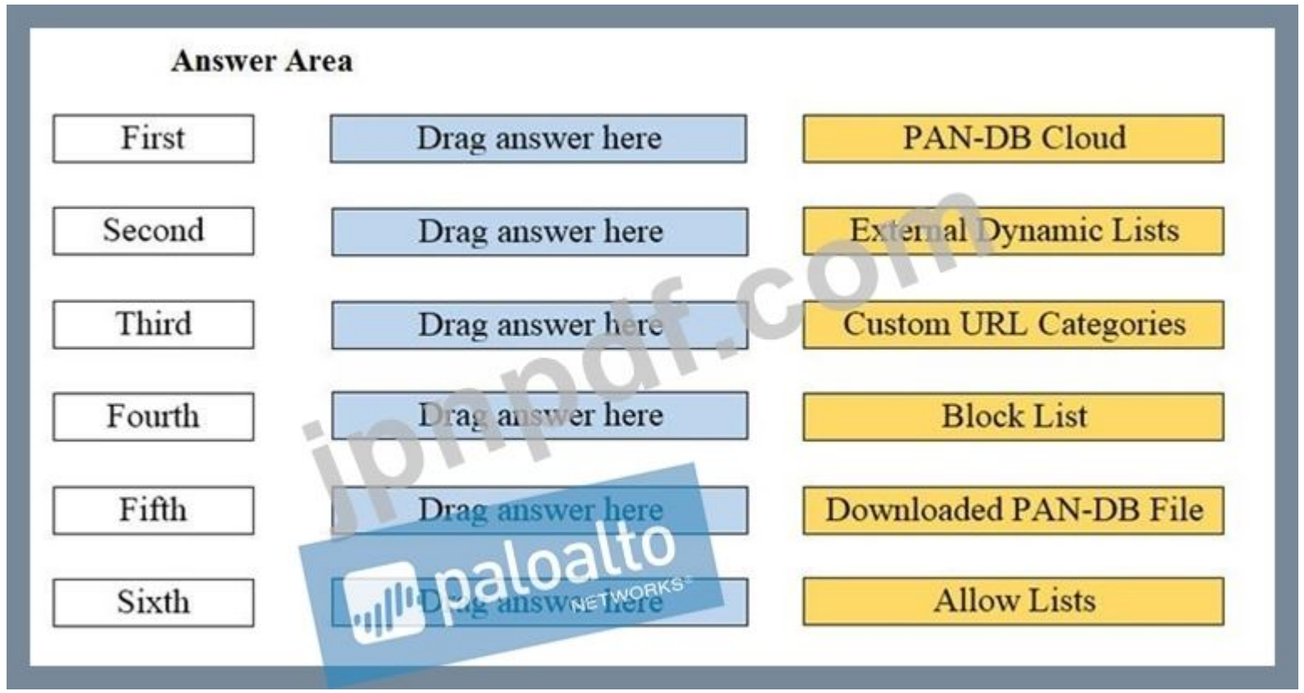
最新問題: **18**
ポリシーオプティマイザの主な機能は何ですか？
A. 他のファイアウォールベンダーのセキュリティルールをPalo Alto Networksの設定に移行する
B. セッション開始時にログを記録する」セキュリティルールを削除する
C. ポートベースのセキュリティルールをアプリケーションベースのセキュリティルールに変換する

D. 組み合わせ可能なセキュリティルールを強調表示することで、管理プレーンの負荷を軽減します。
Answer: C (メーッセージを残す)

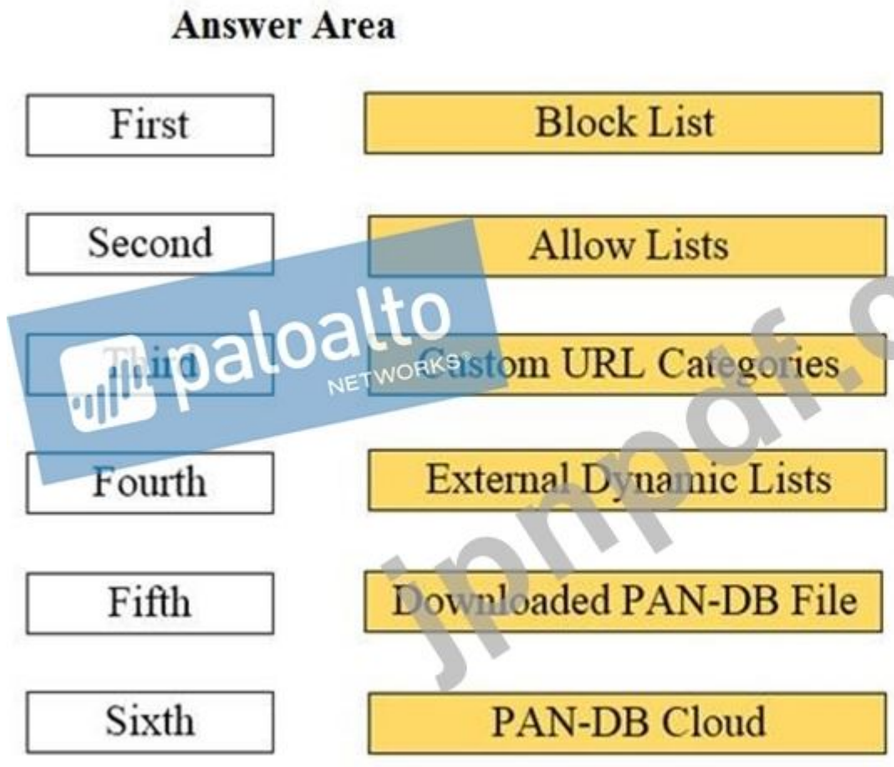
最新問題**: 19**
URLフィルタリングのセキュリティプロファイルにおいて、アクションを設定できる項目はどれですか？ 2つ選択してください。）
A. 許可リスト
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions
B. ブロックリスト
C. カスタムURLカテゴリ
D. PAN-DB URLカテゴリ
Answer: (解答を表示する)

最新問題**: 20**
ファイアウォールがActive Directoryを使用してユーザー認証を行う場合、認証プロファイルにはどのサーバープロファイルが必要ですか？
A. TACACS+
B. 半径
C. LDAP
D. SAML
Answer: C (メーッセージを残す)
説明/参考資料: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/configure-an-authentication-profile-and-sequence

最新問題**: 21**
ドラッグアンドドロップ問題
システム内でURL分類が処理される正しい順序を設定してください。
選択して配置する：



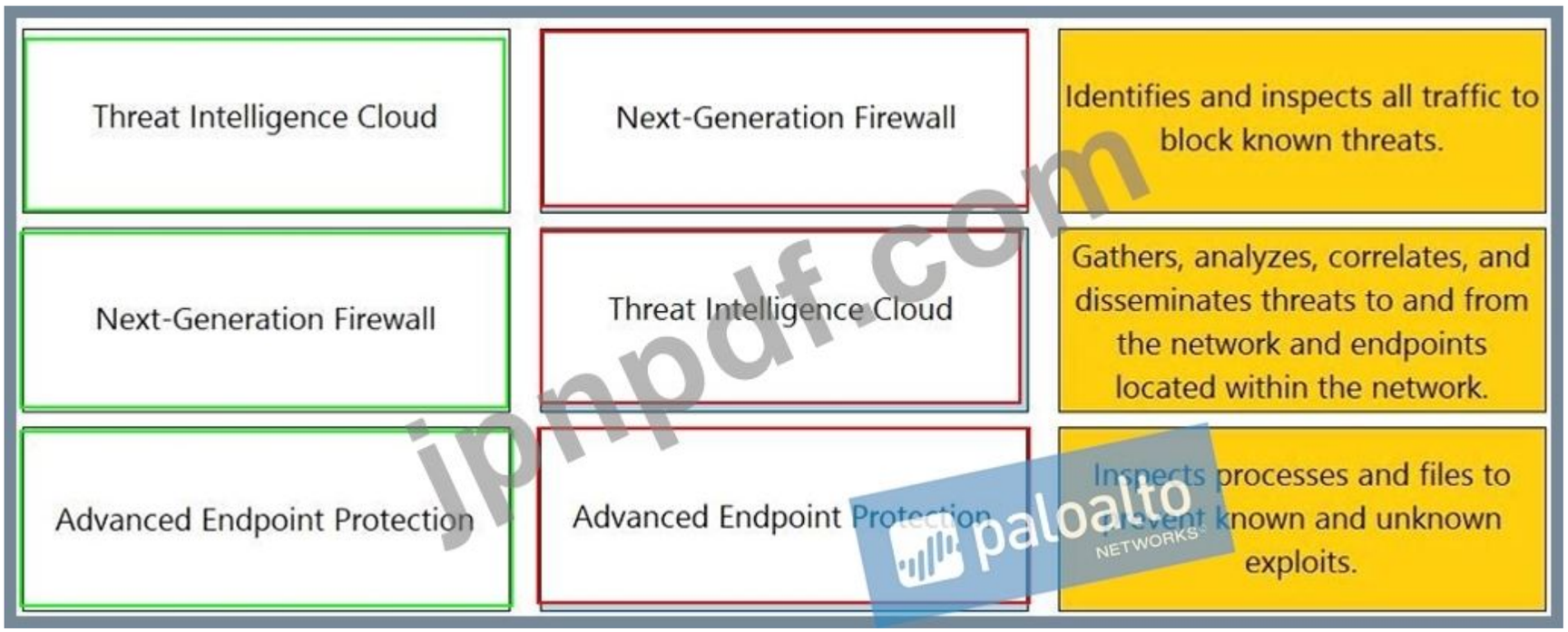
Answer:



最新問題: **22**

各機能をDoS攻撃対策ポリシーまたはDoS攻撃対策プロファイルに一致させてください。

Answer:



最新問題: **23**
脅威ログにイベントが表示されるのはどのような場合ですか？
A. トラフィックが対応するセキュリティプロファイルに一致する場合
B. トラフィックがセキュリティポリシーに一致する場合
C. セッションがブロックされるたびに
D. ファイアウォールが接続を切断するたびに

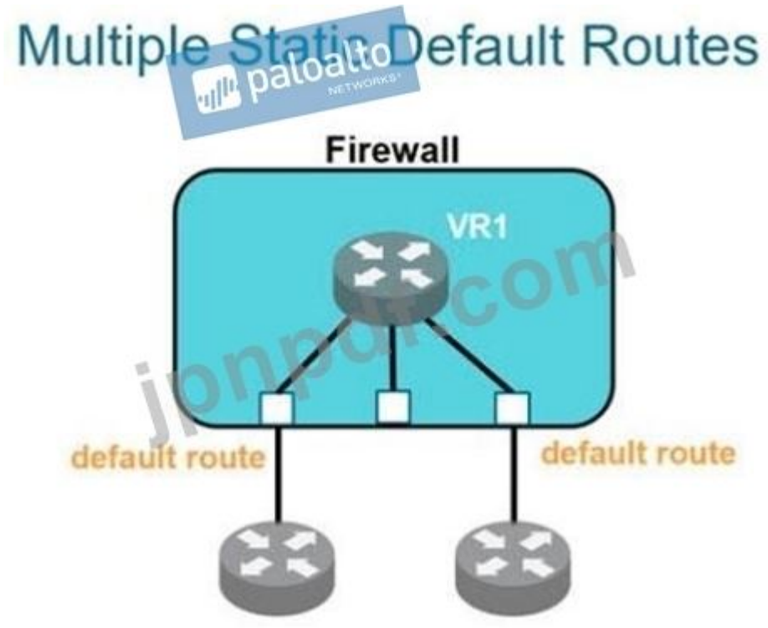
Answer: A (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/view-and-manage-logs/log-types-and-severity-levels/threat-logs#:~:text=Threat%20logs%20display%20entries%20when,security%20rule%20on%20the%20firewall.

最新問題**: 24**
セキュリティポリシーのルールベースをグループとして表示するには、どのパラメータを使用しますか？
A. タグ
B. サービス
C. タイプ
D. アクション
Answer: A (メーッセージを残す)
ルールをグループ化するには、まずタグを作成する必要があります。タグでグループ化されたルールを割り当てた後、〝ルールベースをグループとして表示」を選択すると、割り当てられたタグに基づいてポリシーのルールベースが視覚的に表示されます。ルールベースをグループとして表示している間も、ポリシーの順序と優先順位は維持されます。このビューで、グループタグを選択すると、そのタグでグループ化されたすべてのルールが表示されます。
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-tags

最新問題**: 25**
以下のスクリーンショットを確認してください。このスクリーンショットに含まれる情報に基づいて、どのプロトコルデコーダが機械学習による一致を検出し、脅威ログエントリを作成し、トラフィックを許可するでしょうか？

A. smb
B. イマップ
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、デフォルトの（アラート）アクションが設定されているのは、IMAP、POP3、SMTPのみで、各アプリケーションのトラフィックフローごとにアラートが生成されます。
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**: 26**
画像に示されているように複数の静的デフォルトルートが設定されている場合、正しい記述は次のうちどれですか？（2つ選択してください。）



A. 経路監視では、経路が使用可能かどうかは判断されません。
B. 最も高い指標を持つルートが積極的に利用されている
C. 経路監視により、経路が使用可能かどうかを判断します
D. 最も指標値が低いルートが積極的に利用されています
Answer: C,D (メーッセージを残す)

最新問題**: 27**
提示された画像に基づいて、セキュリティポリシー規則について正しい選択肢を2つ選びなさい。2つ選択してください。）

	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
1	Allow Office Programs	none	universal	inside	any	any	any	outside	any	-	-	-	office-progra...	application-d...	Allow
2	Allow FTP to web ser...	none	universal	inside	any	any	any	outside	ftp-server	-	-	-	any	ftp-service	Allow
3	Allow Social Network...	none	universal	inside	any	any	any	outside	any	-	-	-	facebook	application-d...	Allow

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を使用してFTPが許可されます。
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」ルールでは、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、FTPはAPP-IDではなくポートベースのルールを使用して許可されます。

最新問題**: 28**
WildFireはどのくらいの頻度で動的アップデートをリリースしますか？
A. 5分ごと
B. 15分ごと

C. 60分ごと
D. 30分ごと
Answer: A (メーッセージを残す**)**
WildFireは、WildFireパブリッククラウドによる分析結果に基づいて作成された、ほぼリアルタイムのマルウェアおよびウイルス対策シグネチャを提供します。WildFireシグネチャの更新は5分ごとに提供されます。ファイアウォールが最新のWildFireシグネチャを利用可能になってから1分以内に取得できるように、ファイアウォールを1分ごとに新しい更新を確認するように設定できます。WildFireのサブスクリプションがない場合、ウイルス対策ソフトのアップデートで署名が提供されるまで少なくとも24時間待つ必要があります。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/software-and-content-updates/dynamic-content-updates

最新問題**: 29**
セキュリティルールが「ゾーン内」として設定されている場合、変更できないフィールドはどれですか？
A. 目的地ゾーン
B. アクション
C. 発生源ゾーン
D. アプリケーション
Answer: A (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

最新問題**: 30**
提供された画像に基づいて、セキュリティポリシー規則に当てはまる記述を2つ選択してください。

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source DEVICE	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	[illegible]	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

A. Allow-Social-Mediaルールは、すべてのFacebook機能を許可します。
B. Allow-FTP ポリシーでは、App-ID を使用して FTP が許可されます。
C. Allow-Office-Programs ルールはアプリケーションフィルタを使用しています。
D. Allow-Office-Programs ルールはアプリケーション グループを使用しています。
Answer: A,C (メーッセージを残す**)**

最新問題**: 31**
スクリーンショットに基づいて、含まれているグループの目的は何ですか？

	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. これらはファイアウォールの認証情報に基づいてのみ表示されるグループです。
B. これらはユーザー名をグループ名にマッピングするために使用されます。
C. ファイアウォールの管理を許可したユーザーのみが含まれます。
D. これらはRADIUS認証サーバーからインポートされたグループです。
Answer: (解答を表示する**)**
説明／参考資料：
参照：
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups.html

最新問題: **32**
スクリーンショットに基づいて、含まれているグループの目的は何ですか？

	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. ユーザー名をグループ名にマッピングするために使用されます。
B. これらはファイアウォールの認証情報に基づいてのみ表示されるグループです。
C. これらはRADIUS認証サーバーからインポートされたグループです。
D. ファイアウォールの管理を許可したユーザーのみが含まれます。
Answer: (解答を表示する**)**

最新問題: **33**
ホストへの攻撃に使用されている新しいマルウェアに関する通知を受け取ります。このマルウェアは、一般的なアプリケーションのソフトウェアのバグを悪用します。ファイアウォールの脅威シグネチャデータベースを更新した後、どのセキュリティプロファイルがこの脅威を検出し、アクセスをブロックしますか？
A. 受信セキュリティポリシールールに適用される脆弱性プロファイル
B. 送信セキュリティポリシールールに適用されるデータフィルタリングプロファイル
C. 受信セキュリティポリシールールに適用されるデータフィルタリングプロファイル
D. 送信セキュリティポリシールールに適用されるウイルス対策プロファイル
Answer: A (メーッセージを残す**)**

最新問題: **34**

動的なユーザーグループにユーザーをタグ付けする際に使用できる、有効な情報源を3つ挙げてください。
（3つ選択してください。）
A. iOSデバイスからのBiometricスキャン結果
B. カスタムAPIスクリプト
C. セキュリティ情報およびイベント管理システム（SIEM）、例えばSplunkなど
D. DNSセキュリティサービス
E. ファイアウォールログ
Answer: B,D,E (メーッセージを残す**)**

最新問題**: 35**
従業員がYouTubeにアクセスしようとすると、アプリケーションブロックページが表示されます。YouTubeアプリケーションをブロックしているセキュリティポリシーは何ですか？

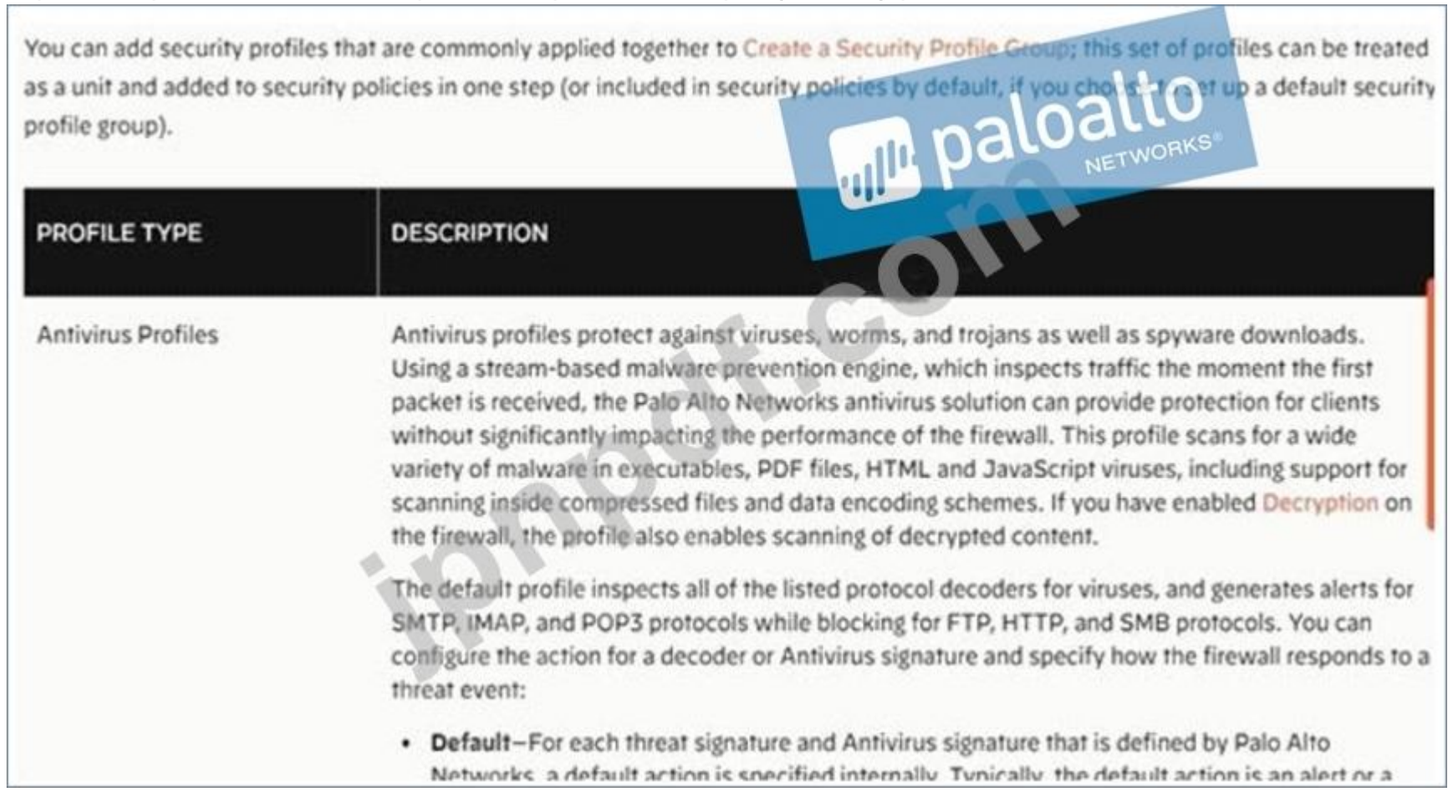
			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	Application	Service	URL Category	Action	Profile
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	Snmpv3 Ssh ssl	Application-d	Any	Allow	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. ゾーン内デフォルト
B. Googleを拒否する
C. インターゾーンデフォルト
D. 許可されたセキュリティサービス
Answer: C (メーッセージを残す**)**

最新問題**: 36**
Active Directoryユニバーサルグループでグループマッピングを使用する場合、ユーザーIDを設定する際に何をする必要がありますか？
A. LDAPサーバープロファイルを作成し、ポート3268またはSSLの場合は3269でグローバルカタログサーバーのルートドメインに接続します。
B. グループマッピングキャッシュをクリアする頻度スケジュールを設定します。
C. ユーザーベースのセキュリティポリシーのプライマリ従業員ID番号を設定します
D. LDAPSを使用してドメインコントローラに接続するためのRADIUSサーバープロファイルをポート636または389で作成します。
Answer: B (メーッセージを残す**)**
ユニバーサルグループを使用している場合は、まずLDAPサーバープロファイルを作成し、ポート3268（SSLの場合は3269）でグローバルカタログサーバーのルートドメインに接続します。次に、別のLDAPサーバープロファイルを作成し、ポート389でルートドメインコントローラーに接続します。これにより、すべてのドメインとサブドメインでユーザーとグループの情報が確実に利用できるようになります。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

最新問題**: 37**
SYNフラッド攻撃対策のしきい値を設定できるファイアウォールコンポーネントはどれですか？（2つ選択してください。）

A. QoSプロファイル
B. DoS攻撃対策プロファイル
C. ゾーン保護プロファイル
D. DoS攻撃対策ポリシー
Answer: B,C (メーッセージを残す)
説明
参照：
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles


You can add security profiles that are commonly applied together to Create a Security Profile Group; this set of profiles can be treated as a unit and added to security policies in one step (or included in security policies by default, if you choose to set up a default security profile group).

PROFILE TYPE	DESCRIPTION
Antivirus Profiles	Antivirus profiles protect against viruses, worms, and trojans as well as spyware downloads. Using a stream-based malware prevention engine, which inspects traffic the moment the first packet is received, the Palo Alto Networks antivirus solution can provide protection for clients without significantly impacting the performance of the firewall. This profile scans for a wide variety of malware in executables, PDF files, HTML and JavaScript viruses, including support for scanning inside compressed files and data encoding schemes. If you have enabled Decryption on the firewall, the profile also enables scanning of decrypted content. The default profile inspects all of the listed protocol decoders for viruses, and generates alerts for SMTP, IMAP, and POP3 protocols while blocking for FTP, HTTP, and SMB protocols. You can configure the action for a decoder or Antivirus signature and specify how the firewall responds to a threat event: • **Default**–For each threat signature and Antivirus signature that is defined by Palo Alto Networks, a default action is specified internally. Typically, the default action is an alert or a

最新問題: **38**
URLフィルタリングのセキュリティプロファイルにおいて、アクションを設定できる項目はどれですか？ 2つ選択してください。）
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-profil

最新問題: **39**
スクリーンショットに基づいて、ft」とラベル付けされたユーザー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」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. グループ it」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。
C. DMZゾーン内のサーバーへの 任意の」ユーザーのアクセスを許可します。
D. 全てのポートでITアプリケーションへのアクセスを可能にします
Answer: (解答を表示する**)**

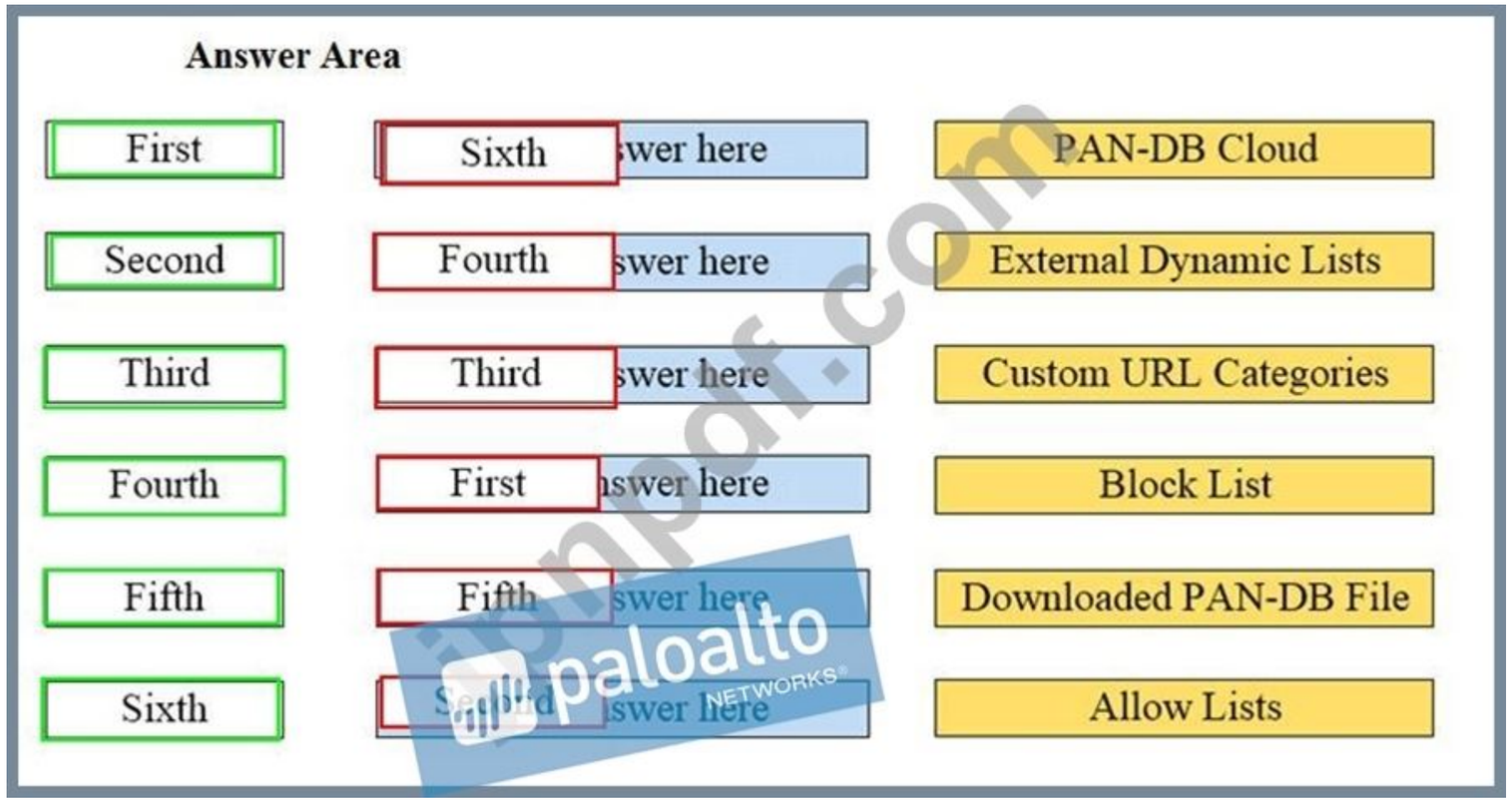
最新問題**: 40**
カスタムURLカテゴリを作成するための正しい手順は何ですか？
A. オブジェクト > セキュリティ プロファイル > URL カテゴリ > 追加
B. オブジェクト > セキュリティ プロファイル > URL フィルタリング > 追加
C. オブジェクト > カスタムオブジェクト > URLフィルタリング > 追加
D. オブジェクト > カスタムオブジェクト > URLカテゴリ > 追加
Answer: (解答を表示する**)**

最新問題**: 41**
システム内でURL分類が処理される正しい順序を設定してください。

Answer Area

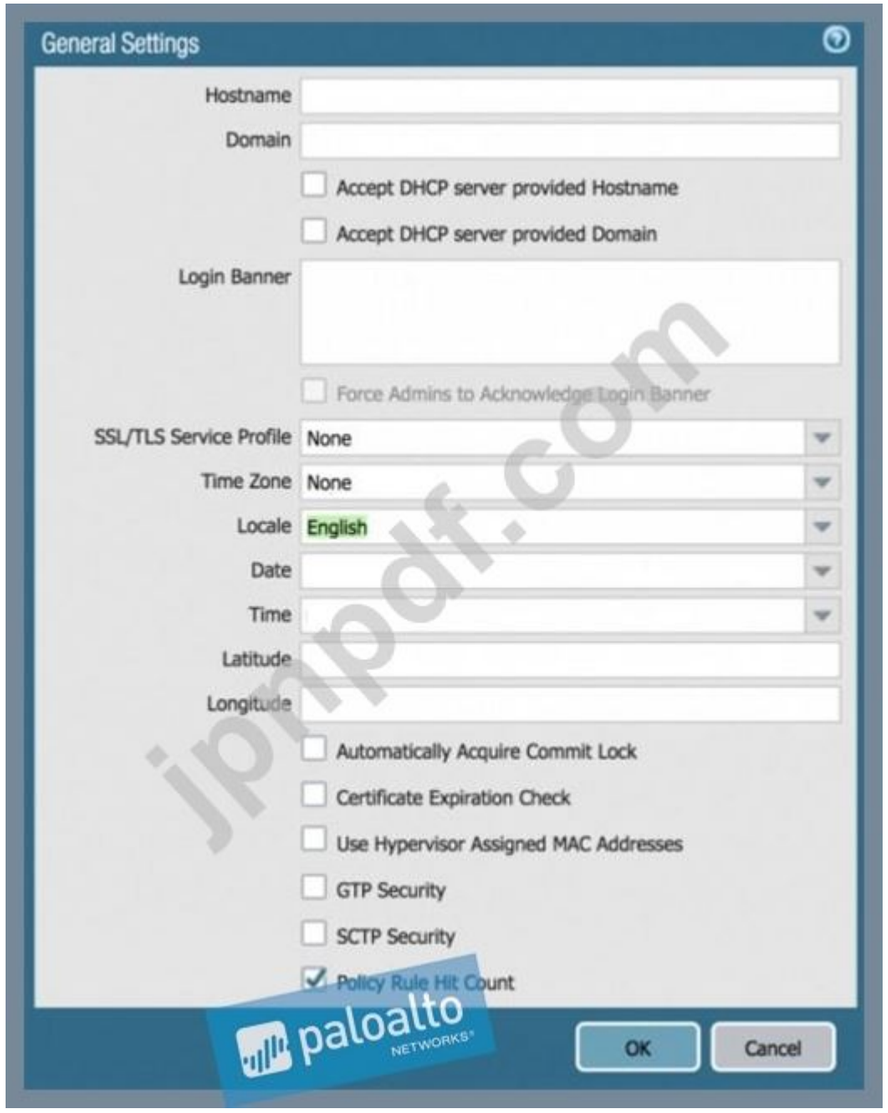
First	Drag answer here	[illegible] Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	Allow Lists

Answer:



最新問題: **42**

図に基づいて、SSL/TLSサービスプロファイル構成オプションの目的は何ですか？

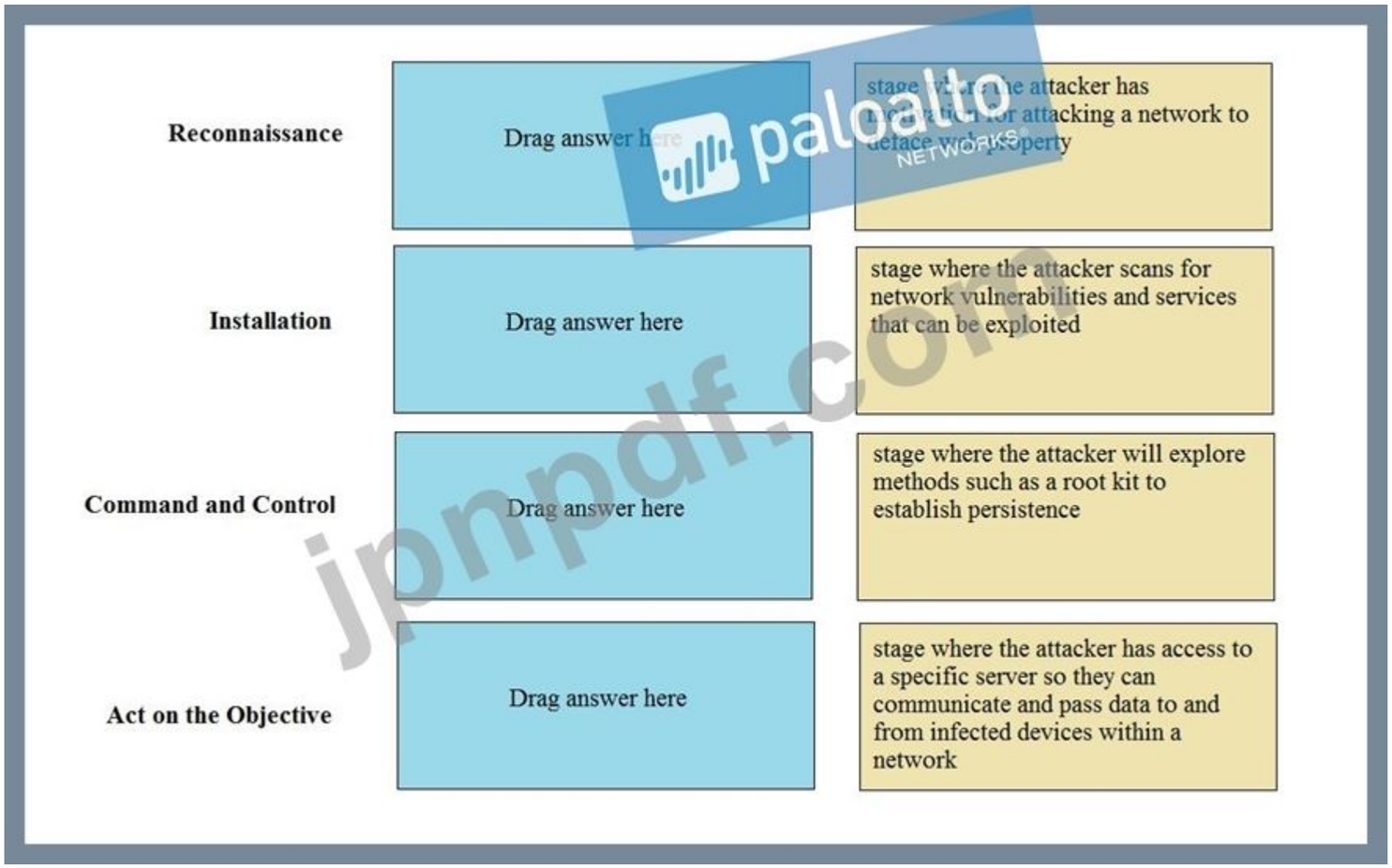


A. クライアントのブラウザを検証するために使用される CA 証明書を定義します。
B. 管理インターフェースからクライアントのブラウザに送信する証明書を定義します。
C. 管理インターフェースを保護するために使用される SSUTLS 暗号化強度を定義します。
D. ファイアウォールのグローバルなSSL/TLSタイムアウト値を定義します。
Answer: (解答を表示する**)**

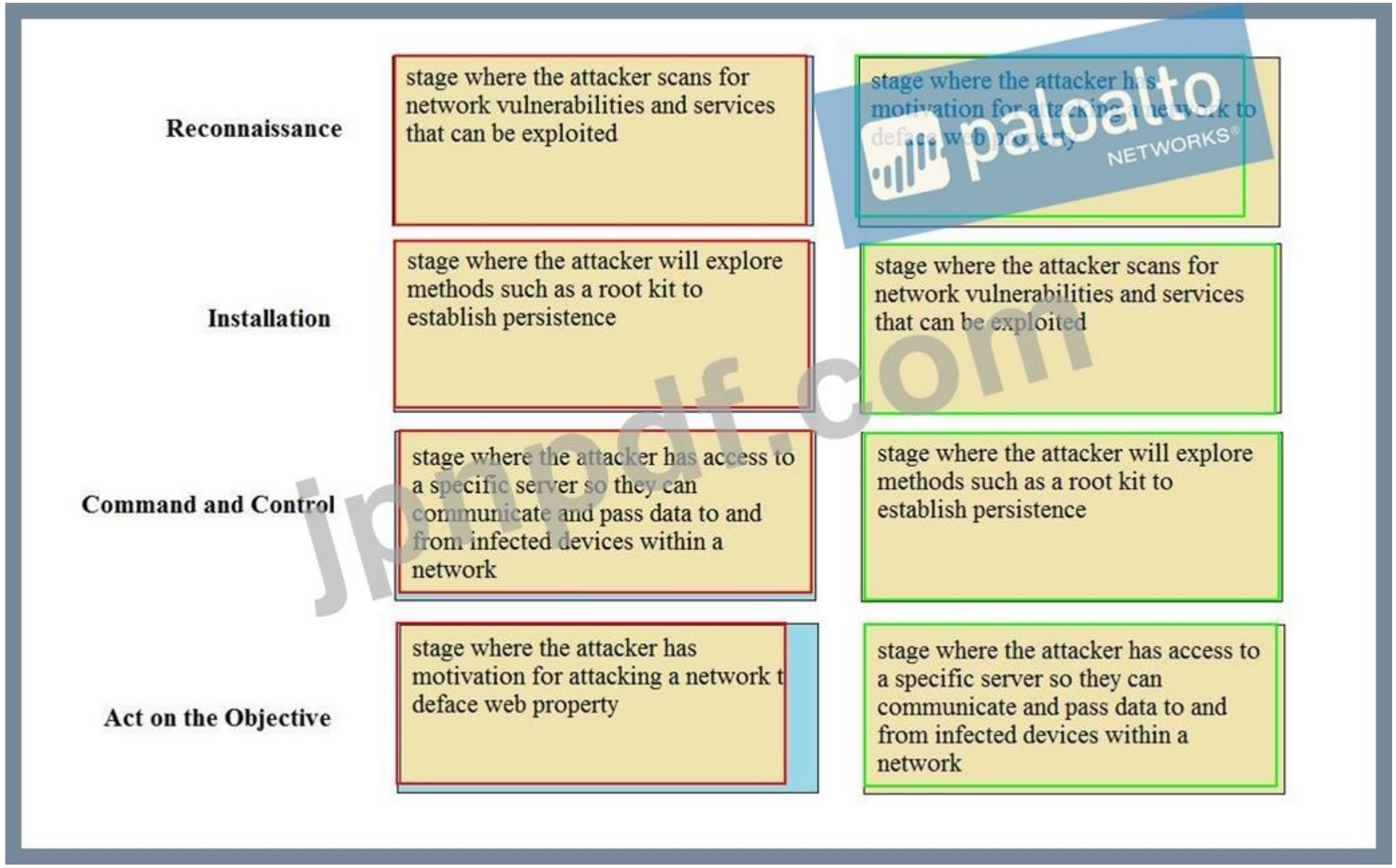
最新問題**: 43**
ドメイン生成アルゴリズムに基づいてマルウェアを作成する際に利用できる3つの要素は何ですか？
（3選択してください。）
A. 時間帯
B. URLカスタムカテゴリ
C. その他の独自の価値
D. 暗号鍵

E. IPアドレス
Answer: A,C,D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection

最新問題**: 44**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。



Answer:



最新問題: **45**
コンテンツに対する制限がほとんどなく、攻撃者が違法または非倫理的なコンテンツを配布するために頻繁に利用するホスティングプロバイダーからのトラフィックを防止するのに役立つ機能はどれでしょうか？
A. パロアルトネットワークスの防弾IPアドレス
B. パロアルトネットワークスのC&C IPアドレス
C. パロアルトネットワークスが認識している悪意のあるIPアドレス
D. パロアルトネットワークスの高リスクIPアドレス
Answer: A (メーッセージを残す**)**
悪意のある、違法な、または非倫理的なコンテンツを提供するために防弾ホストを使用するホストをブロックするには、ポリシーで防弾IPアドレスリストを使用します。
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PM0pCAG

最新問題: **46**
ローカル管理者アカウントに対して、事前定義された役割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. 役割ベース
C. ダイナミック
D. デバイス管理者
Answer: (解答を表示する**)**
動的ロール :これらは、ファイアウォールへのアクセス権限を付与する、組み込みまたは事前定義されたロールです。新機能が追加されると、ファイアウォールは動的ロールの定義を自動的に更新します。手動で更新する必要はありません。

最新問題**: 47**
セキュリティポリシールールに基づいて、内部ゾーンから外部ゾーンへのすべてのFTPトラフィックに一致するルールはありますか？

A. 内部ポータル
B. 外部からの進入
C. インターコーンデフォルト
D. 内部DMZ
Answer: B (メーッセージを残す**)**

最新問題**: 48**
管理者は、ユーザーが特定のメールアプリケーションのみを使用できるように許可する必要があります。
管理者は、ユーザーが特定のメールアプリケーションしか利用できないように、ファイアウォールをどのように設定すればよいでしょうか？
A. アプリケーションフィルターを作成し、コラボレーションカテゴリでフィルタリングします。
B. アプリケーションフィルタを作成し、コラボレーションカテゴリ、メールサブカテゴリでフィルタリングします。

C. アプリケーショングループを作成し、そこにメールアプリケーションを追加します。
D. アプリケーショングループを作成し、そこにメールカテゴリを追加します。
Answer: C (メーッセージを残す)
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**: 49**
SYNフラッド攻撃対策のしきい値を設定できるファイアウォールコンポーネントはどれですか？ 2つ選択）
2つ選択してください。）
A. QoSプロファイル
B. DoS攻撃対策プロファイル
C. ゾーン保護プロファイル
D. DoS攻撃対策ポリシー
Answer: B,C (メーッセージを残す)
洪水攻撃からの保護
ゾーン保護プロファイルは、以下の5種類の洪水から保護します。
* SYN (TCP)
* UDP
* ICMP
* ICMPv6
* その他のIPアドレス

最新問題**: 50**
IPアドレスのブロック機能と同等のアクションを設定できるセキュリティプロファイルはどれですか？ 2つ選択してください。）
A. アンチウイルス
B. URLフィルタリング
C. 脆弱性対策
D. スパイウェア対策
Answer: C,D (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles/actions-in-security-profiles

最新問題**: 51**
バッファオーバーフロー、不正なコード実行、およびシステム上の脆弱性を悪用しようとするその他の試みから保護するために、セキュリティポリシールールにはどのタイプのプロファイルを適用する必要がありますか？
A. URLフィルタリング
B. 脆弱性対策
C. ファイルブロック
D. スパイウェア対策
Answer: B (メーッセージを残す)

脆弱性保護セキュリティプロファイルは、ネットワークに侵入する脅威から保護します。たとえば、脆弱性保護セキュリティプロファイルは、バッファオーバーフロー、不正なコード実行、およびシステム脆弱性を悪用しようとするその他の試みから保護します。デフォルトの脆弱性保護セキュリティプロファイルは、既知のすべての重大度（クリティカル、高、中）の脅威からクライアントとサーバーを保護します。また、特定のシグネチャに対する応答を変更できる例外を作成することもできます。

最新問題: **52**
PAN-OS GUIのどのセクションで、管理者はURLフィルタリングプロファイルを設定しますか？
A. ネットワークab
B. ポリシー
C. オブジェクト
D. デバイス
Answer: C (メーッセージを残す**)**
URL フィルタリング プロファイルは、PAN-OS GUI の [オブジェクト] セクションで構成します。URL フィルタリング プロファイルは、ファイアウォールがさまざまな URL カテゴリに対して実行するアクション (許可、ブロック、警告、続行、オーバーライドなど) を定義します。URL フィルタリング プロファイルでは、認証情報フィッシング防止、URL フィルタリング インライン 機械学習、セーフサーチの強制などの設定も構成できます。URL フィルタリング プロファイルを作成または変更するには、[オブジェクト] > [セキュリティ プロファイル] > [URL フィルタリング] に移動する必要があります。参照: URL フィルタリング プロファイル、[URL フィルタリング プロファイルの作成]、[PAN-OS 10.1 の更新された認定資格]、[Palo Alto Networks 認定ネットワーク セキュリティ管理者 (PAN-OS 10.0)]。

最新問題: **53**
貴社は単一の建物内の1フロアを占有しています。単一のネットワーク上に2台のActive Directoryドメインコントローラーがあります。ファイアウォールの管理プレーンはほとんど利用されていません。
お使いのネットワークでは、どのUser-IDエージェントで十分ですか？
A. 各ドメインコントローラーにWindowsベースのエージェントが展開されます。
B. ファイアウォールにPAN-OS統合エージェントをデプロイする
C. ネットワーク上にCitrixターミナルサーバーエージェントが展開されています
D. ドメインメンバーの内部ネットワークに展開されたWindowsベースのエージェント
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-using-the-windows-user-id-agent/ configure-the-windows-based-user-id-agent-for-user-mapping.html

最新問題: **54**
提示されたセキュリティポリシー規則に基づくと、SSHはどのポートで許可されますか？

	Name	Type	Source Zone	Source Address	Destination Zone	Destination 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. 53

B. 23
C. 22
D. 80
Answer: C (メーッセージを残す**)**

最新問題**: 55**
管理者は、セッションが想定されるNATポリシーと一致しているかどうかを検証するために何を使用しますか？
A. 設定監査
B. テストコマンド
C. 脅威ログ
D. システムログ
Answer: (解答を表示する**)**

最新問題**: 56**
信頼ゾーンのユーザーがDMZゾーン内の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はどのように構成すればよいでしょうか？
A.
Source Zone: Trusted
Destination Zone: DMZ
Services: Application-Default
Applications: SSH
Action: Allow
B.


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: Deny
Answer: (解答を表示する**)**

最新問題**: 57**
Palo Alto NetworksのDNSセキュリティサービスの3つの特徴は何ですか？ 3つ選択してください。）
A. DGA/DNSトンネル検出や機械学習などの技術を使用します
B. 有効な脅威防御ライセンスが必要です。
C. 高度な予測分析を使用して、リアルタイムの保護機能をユーザーに提供します。
D. 有効なURLフィルタリングライセンスが必要です。
E. サードパーティのDNSセキュリティサービスへの有効なサブスクリプションが必要です。

Answer: A,B,C (メーッセージを残す)
DNSセキュリティサブスクリプションを利用することで、高度な予測分析を用いたリアルタイム保護機能を利用できます。DGA/DNSトンネリング検出や機械学習などの技術を用いることで、DNSトラフィックに潜む脅威を事前に特定し、拡張性の高いクラウドサービスを通じて共有することが可能です。DNSシグネチャと保護機能はクラウドベースのアーキテクチャに保存されているため、多様なデータソースから生成された、常に拡大し続けるシグネチャのデータベース全体にアクセスできます。このシグネチャリストにより、DNSを使用して新たに生成される悪意のあるドメインに対する様々な脅威にリアルタイムで対応できます。将来の脅威に対抗するため、DNSセキュリティサービスの分析、検出、および防御機能のアップデートは、コンテンツリリースを通じて提供されます。DNSセキュリティサービスにアクセスするには、脅威防御ライセンスとDNSセキュリティライセンスが必要です。

最新問題**: 58**
Palo Alto Networksのセキュリティ管理ツールの中で、ポリシーの統合作成、集中管理、集中型脅威インテリジェンスを2つ提供するものはどれですか？ 2つ選択してください。）
A. オートフォーカス
B. パノラマ
C. グローバルプロテクト
D. 絞り
Answer: A,B (メーッセージを残す)

最新問題**: 59**
管理者がNATポリシーを作成しています。
住所とゾーンの組み合わせのうち、一致条件として使用されるものはどれですか？ 2つ選択してください。）
A. NAT前のアドレス
B. NAT前ゾーン
C. NAT後のアドレス
D. ポストNATゾーン
Answer: A,B (メーッセージを残す)
NAT ポリシールールは、元の NAT 前の送信元アドレスと宛先アドレス、および NAT 前の宛先ゾーンに基づいてパケットを照合します。これは、NAT 前の送信元アドレスと宛先アドレス、および NAT 後のゾーンに基づいてパケットを照合するセキュリティ ポリシーです。

最新問題**: 60**
ルーティングやスイッチングを必要とせず、許可されたトラフィックを通過させる前にセキュリティポリシーまたはNATポリシーのルールを適用するインターフェースの種類はどれですか？
A. レイヤー3
B. レイヤー2
C. タップ
D. バーチャルワイヤー
Answer: A (メーッセージを残す)

最新問題**: 61**
管理者は、デフォルト設定になっているinterzone-defaultルールに一致するトラフィックに関する問題のトラブルシューティングを行っています。
管理者は何をすべきでしょうか？
A. ルールのログ記録アクションを変更します
B. トラフィックログフィルターを調整して日付を含めるようにします。
C. トラフィックログを更新する

D. システムログを確認する
Answer: A (メーッセージを残す**)**
定義したルールに一致しないトラフィックは、ルールベースの一番下にある事前定義済みのinterzone-defaultルールに一致し、拒否されます。作成したルールに一致しないトラフィックの詳細を確認するには、interzone-defaultルールでログ記録を有効にしてください。

最新問題**: 62**
PAN_OSバージョン9.1以降、セキュリティポリシールールのユーザーフィールド内で使用できる新しいタイプのオブジェクトはどれですか？
A. ダイナミックユーザーグループ
B. 静的ユーザーグループ
C. ローカルユーザー名
D. リモートユーザー名
Answer: A (メーッセージを残す**)**

最新問題**: 63**
Panoramaで 「未使用のアドレスとサービスオブジェクトをデバイスと共有する」設定を無効にすると、どのような効果が得られますか？
A. ファイアウォールにプッシュされるオブジェクトの数を減らす
B. ファイアウォールごとの設定バックアップのバックアップ容量を増やす
C. HAペア間の設定およびセッション同期時間を短縮する
D. アドレスオブジェクトとサービスオブジェクトのファイアウォールごとの容量を増やす
Answer: A (メーッセージを残す**)**

最新問題**: 64**
ローカルファイアウォールのユーザーデータベースに依存する管理者アカウントを有効にする前に必要な前提条件は何ですか？
A. 認証プロファイルの設定
B. 管理インターフェースを専用の管理VLANに分離する
C. 認証ポリシーを設定する
D. 認証シーケンスを設定する
Answer: A (メーッセージを残す**)**

最新問題**: 65**
内部ゾーンのすべてのユーザーは、DMZゾーン内のサーバーへのTelnetアクセスのみを許可される必要があります。このタイプのアクセスのみを許可するセキュリティポリシールールの空欄2つを埋めてください。

2つ選択してください。

A. サービス＝ 任意」

B. アプリケーション = "任意"

C. アプリケーション = "Telnet"

D. サービス - "application-default"

Answer: (解答を表示する)

最新問題**: 66**

トポロジーを考慮すると、ファイアウォールインターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？

A. レイヤー3

B. トンネル

C. タップ

D. バーチャルワイヤー

Answer: (解答を表示する)

最新問題**: 67**

提示されたスクリーンショットに基づいて、どの列に、クリックするとポリシー規則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ていますか？

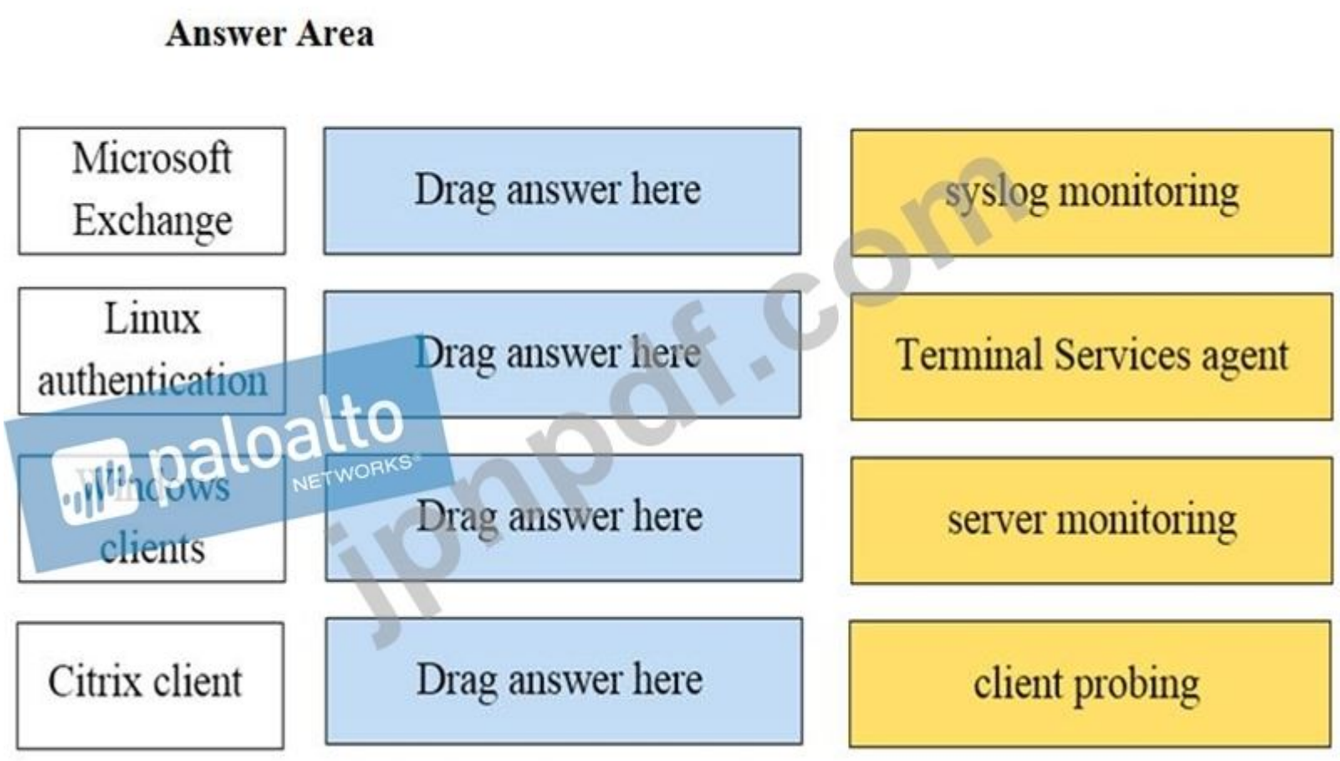
A. 許可されたアプリ

B. 名前

C. サービス
D. 見たアプリ
Answer: D (メーッセージを残す)

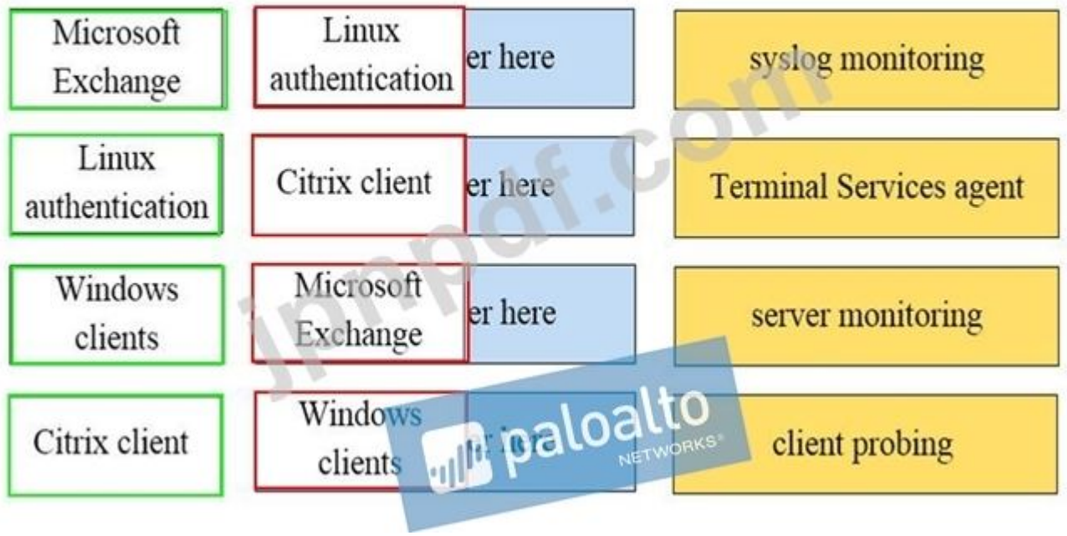
最新問題**: 68**
ファイアウォールが複数の認証プロファイルにアクセスして、ローカルアカウント以外のアカウントを認証できるようにするには、どのような設定が必要ですか？
A. 認証シーケンス
B. LDAPサーバープロファイル
C. 認証サーバーリスト
D. 認証リストプロファイル
Answer: A (メーッセージを残す)
説明／参考資料 :https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/framemaker/pan-os/7-1/pan-os-admin.pdf 144ページ

最新問題**: 69**
ネットワーク機器を適切なユーザーID技術に対応させてください。



Answer:

Answer Area



最新問題: **70**

スクリーンショットに基づいて、ﾅ｢とラベル付けされたユーザー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. 全てのポートでITアプリケーションへのアクセスを可能にします

B. グループ DMZ｢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。

C. DMZゾーン内のサーバーに ﾅ任意の｢ユーザーがアクセスできるようにします。

D. グループ ﾅ｢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。

Answer: D (メーッセージを残す)

最新問題: **71**

外部ゾーンタイプは、どのタイプのオブジェクト間でトラフィックを転送するために使用されますか？

A. レイヤ2インターフェース

B. 仮想ルーター

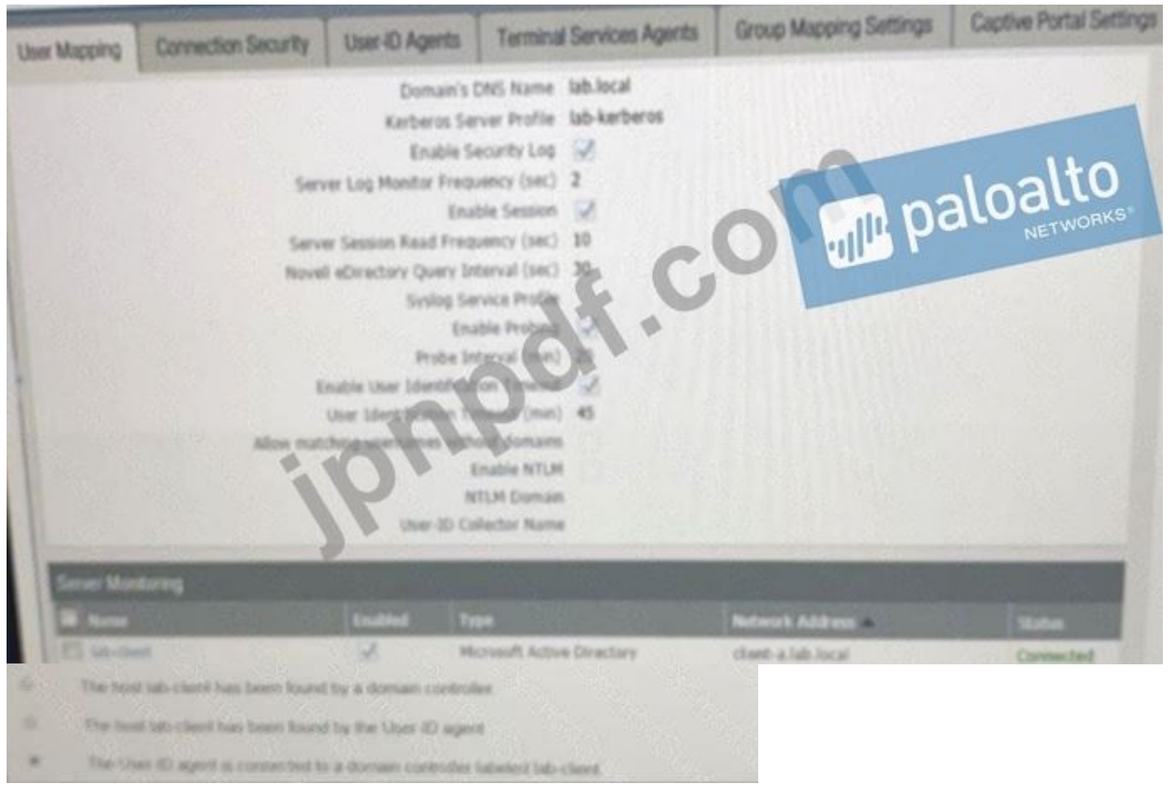
C. レイヤー3インターフェース

D. 仮想システム

Answer: (解答を表示する)

最新問題: **72**

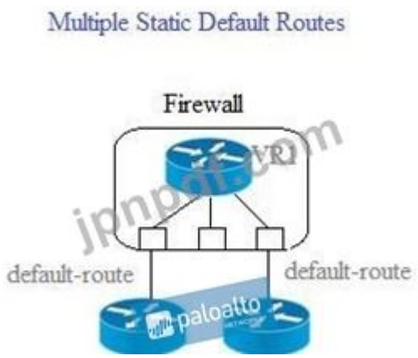
図に基づいて、サーバー監視パネルに表示される出力内容を正確に説明しているのはどの記述ですか？



A. User-IDエージェントは、lab clientというラベルの付いたドメインコントローラーに接続されています。
B. ホスト lab-client は User-ID エージェントによって処理されました。
C. ホスト lab-client がドメイン コントローラによって検出されました。
Answer: A (メーッセージを残す**)**

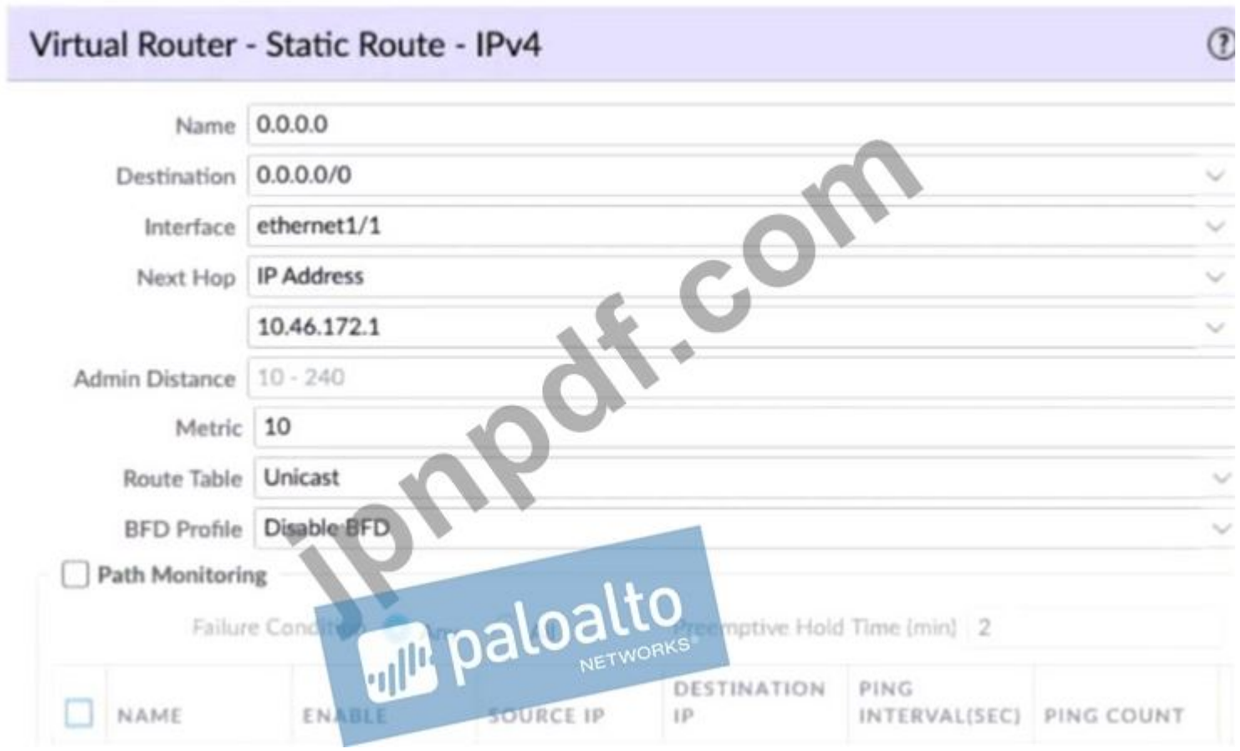
最新問題**: 73**
どのファイアウォールプレーンが、別のプロセッサ上で設定、ログ記録、およびレポート機能を提供しますか？
A. 制御
B. ネットワーク処理
C. データ
D. セキュリティ処理
Answer: A (メーッセージを残す**)**

最新問題**: 74**
このシナリオにおいて、複数の静的デフォルトルートに関して正しい記述はどれですか？ 2つ選択してください。）



A. 経路監視により、経路が使用可能かどうかを判断します。
B. 最も指標値が低いルートが積極的に利用されています
C. 最も高い指標を持つルートが積極的に利用されています
D. 経路監視では、経路が使用可能かどうかは判断されません。
Answer: A,B (メーッセージを残す**)**

最新問題**: 75**
スクリーンショットに示されているように、管理者はどのような2種類のルートを設定していますか？ 2つ選択してください）



A. 静的ルート
B. デフォルトルート
C. BGP
D. OSPF
Answer: B (メーッセージを残す**)**

最新問題: **76**
DNSトラフィックを制御するために利用できる3つのDNSセキュリティカテゴリは何ですか？ 3つ選択してください。）
A. パークドメイン
B. スパイウェアドメイン
C. 脆弱性領域
D. フィッシングドメイン
E. マルウェアドメイン
Answer: A,D,E (メーッセージを残す)
これを表示するには、Ani-Spyware プロファイルの DNS ポリシー > DNS セキュリティに移動してください。
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/dns-security/enable-dns-security

最新問題: **77**
Palo Alto Networksファイアウォールで、ロールベースのアクセス制御における認証と認可をサポートする認証方式はどれですか？ 2つ選択してください。）
A. ケルベロス
B. SAML
C. LDAP
D. TACACS+
Answer: B,D (メーッセージを残す)

最新問題: **78**
ネットワーク図を考慮すると、信頼済みユーザーとゲストユーザーの両方が、SSH、Webブラウジング、SSLアプリケーションを使用して、一般的なインターネットおよびDMZサーバーにアクセスできるようにする必要があります。目的の結果を達成するポリシーはどれですか？
A.


B.

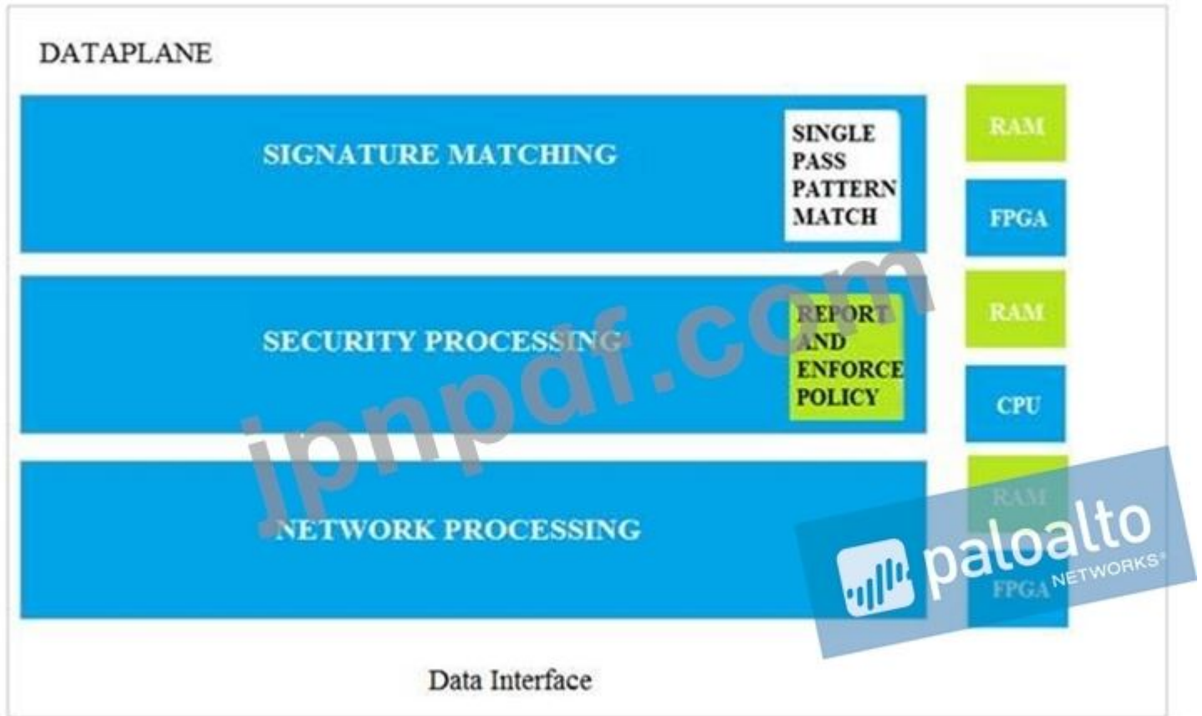

C.

D.

Answer: (解答を表示する)

最新問題: **79**

図に示すデータプレーンプロセッサ層のうち、Palo Alto Networksファイアウォール上でスパイウェアと脆弱性攻撃に対して均一なマッチングを提供する層はどれですか？



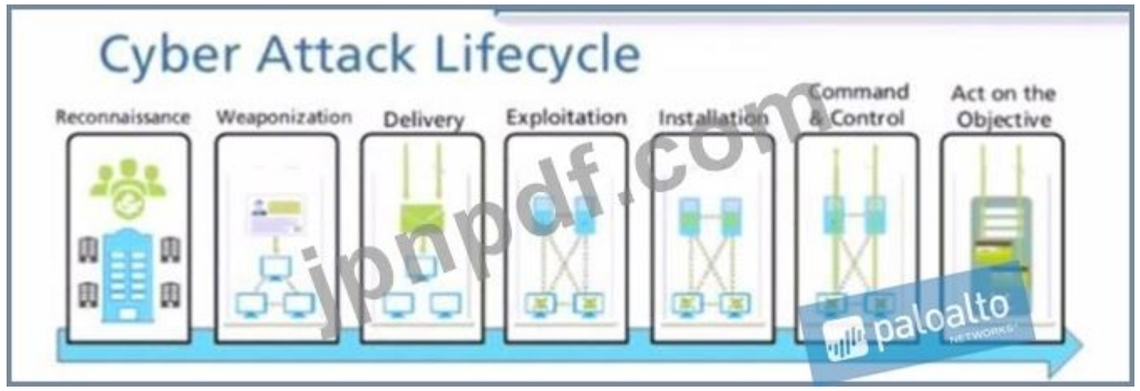
A. ネットワーク処理
B. 署名照合
C. セキュリティ処理
D. セキュリティマッチング
Answer: (解答を表示する)

最新問題: **80**

ファイアウォールで新しいWildFireシグネチャをチェックするために設定できる最小期間はどれくらいですか？

A. 30分ごと
B. 5分ごと
C. 24時間ごとに1回
D. 1分ごと
Answer: (解答を表示する**)**
WildFireの新しいシグネチャは5分ごとに利用可能になるため、ファイアウォールが利用可能になってから1分以内にこれらのシグネチャを取得するようにするには、この設定を使用するのがベストプラクティスです。

最新問題**: 81**
サイバー攻撃のライフサイクルのどの段階で、攻撃者は感染したPDFファイルをメールに添付するのでしょうか？



A. 設置
B. 配送
C. 開発
D. 再保険
E. 指揮統制
Answer: (解答を表示する**)**

最新問題**: 82**
Palo Alto Networksの組み込みIPアドレスEDLを使用するには、どのライセンスが必要ですか？
A. DNSセキュリティ
B. 脅威防止
C. ワイルドファイア
D. SD-WAN
Answer: (解答を表示する**)**
説明／参考資料：
参照：
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**: 83**
ファイアウォールの変更を元に戻すオプションを選択すると、どの設定が置き換えられますか？
A. 別の構成からの設定によるデバイスの状態

B. 実行中の設定から取得した設定を含む候補構成
C. 動的更新スケジューラ設定
D. 候補構成の設定を使用した実行構成
Answer: (解答を表示する**)**

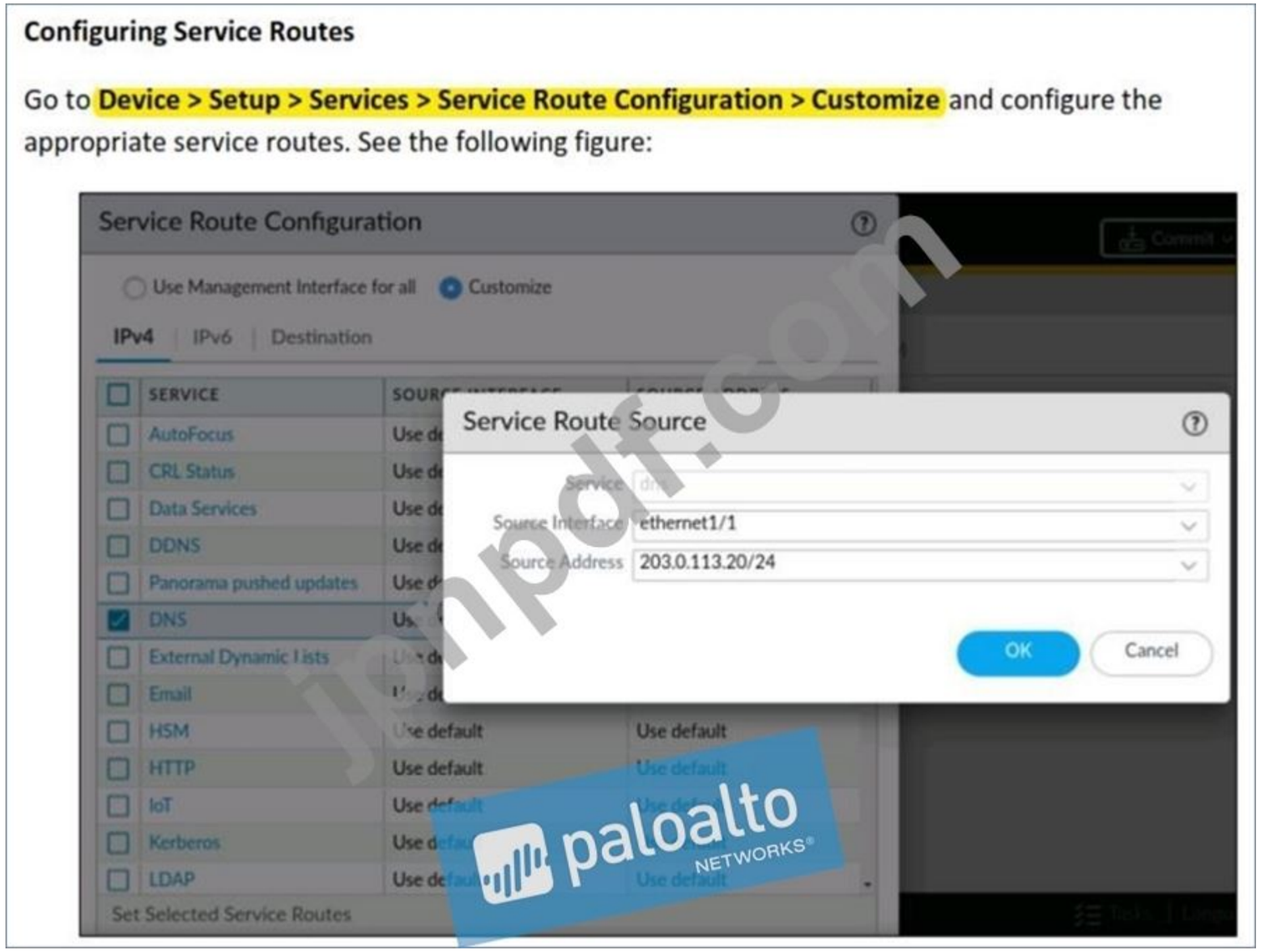
最新問題**: 84**
URLフィルタリングセキュリティプロファイルで設定できるアクションはどれですか？これにより、指定されたパスワードを使用して、特定のカテゴリに属するすべてのWebサイトにユーザーが一時的にアクセスできるようになります。
A. 除外
B. 続ける
C. ホールド
D. オーバーライド
Answer: (解答を表示する**)**
ユーザーには、指定されたカテゴリのウェブサイトへのアクセスを許可するにはパスワードが必要であることを示す応答ページが表示されます。このオプションでは、セキュリティ管理者またはヘルプデスク担当者が、指定されたカテゴリのすべてのウェブサイトへの一時的なアクセスを許可するパスワードを提供します。URLフィルタリングログにログエントリが生成されます。プロキシサーバーを使用するように構成されたクライアントシステムでは、オーバーライドウェブページが正しく表示されません。

最新問題**: 85**
ファイアウォールの候補設定に複数の変更を加えた後、管理者は実行中の設定と一致する候補設定で最初からやり直したいと考えています。デバイス > 設定 > 操作 のどのコマンドを使用すれば、これを最も効率的に実行できますか？
A. 最後に保存した設定に戻す
B. 実行中の設定に戻す
C. 名前付き構成スナップショットをロードします
D. 名前付き設定スナップショットをインポートします
Answer: B (メーッセージを残す**)**

最新問題**: 86**
設定オプションは4つあり、それぞれ特定のURLへのアクセスをブロックするために使用できます。すべてのオプションを同じURLへのアクセスをブロックするように設定した場合、最後にそのURLへのアクセスをブロックするオプションはどれでしょうか？
A. URLフィルタリングプロファイル内のEDL。
B. セキュリティポリシールールのカスタムURLカテゴリ。
C. URLフィルタリングプロファイル内のカスタムURLカテゴリ。
D. URLフィルタリングプロファイル内のPAN-DB URLカテゴリ。
Answer: D (メーッセージを残す**)**
優先順位は上から下へ。最初に一致したものが優先されます: 1) ブロック リスト: 手動で入力されたブロックされた URL オブジェクト - 2) 許可リスト: 手動で入力された許可された URL オブジェクト - 3) カスタム URL カテゴリ - 4) キャッシュ: 外部動的リスト (EDL) から学習された URL - 5) 事前定義カテゴリ: PAN-DB または Brightcloud カテゴリ。

最新問題**: 87**
データプレーンインターフェイスが制御プレーンに代わってDNSクエリを送信できるようにするには、どのファイアウォール機能を設定する必要がありますか？
A. 仮想ルーター

B. 管理者ロールプロファイル
C. DNSプロキシ
D. サービスルート
Answer: D (メーッセージを残す**)**
デフォルトでは、ファイアウォールは管理インターフェイスを使用して、外部動的リスト（EDL）、DNS、電子メール、Palo Alto Networksのアップデートサーバーなど、さまざまなサーバーと通信します。管理インターフェイスは、Panoramaとの通信にも使用されます。ファイアウォールとサーバー間の通信は、データプレーン上のデータポートを経由するようにサービスルートが使用されます。これらのデータポートは、外部サーバーにアクセスする前に、適切なセキュリティポリシールールを設定する必要があります。



最新問題: **88**
どのポリシーセットを使用すれば、ポリシーがデフォルトのセキュリティルールの直前に適用されることを保証できますか？
A. 親デバイスグループのルールベース後
B. 子デバイスグループのルールベース後処理

C. ローカルファイアウォールポリシー
D. ルールベース共有
Answer: (解答を表示する**)**
デフォルトのセキュリティ ルールの直前にポリシーが適用されるようにするために使用するポリシー セットは、共有ポスト ルール ベースです。共有ポスト ルール ベースは、Panorama で定義され、すべてのファイアウォールまたはデバイス グループに適用されるセキュリティ ポリシー ルールのセットです。共有ポスト ルール ベースは、ローカル ファイアウォール ポリシーと子デバイス グループのポスト ルール ベースの後に評価されますが、デフォルトのセキュリティ ルールの前に評価されます。共有ポスト ルール ベースを使用すると、リスクの高いアプリケーションやトラフィックのブロックなど、複数のファイアウォールまたはデバイス グループに共通のセキュリティ ポリシーを適用できます 1。参照: セキュリティ ポリシー ルール階層、セキュリティ ポリシー ルール ベース、認定 - 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**: 89**
管理者は、ユーザーがギャンブル関連のウェブサイトを閲覧した際に、URLフィルタリングのログエントリを作成したいと考えています。セキュリティポリシーとセキュリティプロファイルのアクションの組み合わせとして、どれが適切でしょうか？
A. セキュリティポリシー = 拒否、URLプロファイル内のギャンブルカテゴリ = 許可
B. セキュリティポリシー = 拒否。URLプロファイル内のギャンブルカテゴリ = ブロック
C. セキュリティポリシー = 許可、URLプロファイル内のギャンブルカテゴリ = 警告
D. セキュリティポリシー = 許可。URLプロファイル内のギャンブルカテゴリ = 許可
Answer: (解答を表示する**)**
URLフィルタリングログにログエントリが生成されます。
https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics/url-filtering-profiles

最新問題**: 90**
IPアドレスをユーザー名にマッピングする有効な方法を3つ挙げてください。（3つ選択してください。）
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. ワイルドファイア判決報告
Answer: A,C,D (メッセージを残す**)**
Palo Alto Networksのファイアウォールは、User-IDエージェント、キャプティブポータル、GlobalProtect、XML API、HTTPヘッダーなど、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ピングできます。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。これらの方法の一部を以下に示します。
XML API の使用: XML API を使用すると、外部システムは HTTPS リクエスト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 アドレスの背後にい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にマッピングできます。
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ピングする、認定資格 - Palo Alto Networks、Palo Alto Networks 認定ネットワークセキュリティ管理者 (PAN-OS 10.0) または Palo Alto Networks 認定ネットワークセキュリティ管理者 (PAN-OS 10.0)。

最新問題: **91**
スクリーンショットに基づいて、含まれているグループの目的は何ですか？

			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. これらはRADIUS認証サーバーからインポートされたグループです。
B. ファイアウォールの管理を許可したユーザーのみが含まれます。
C. これらはファイアウォールの認証情報に基づいてのみ表示されるグループです。
D. ユーザー名をグループ名にマッピングするために使用されます。
Answer: D (メーッセージを残す**)**

最新問題: **92**
内部ホストが、ソースNATを使用してインターネット上のサーバーに接続しようとしています。
ファイアウォールでソースNATを有効にするには、どのポリシーが必要ですか？
A. 送信元ゾーンと宛先ゾーンを指定したNATポリシー
B. 外部ソースと任意の宛先アドレスを使用したポストNATポリシー
C. 送信元または宛先ゾーンが選択されていないNATポリシー
D. 外部送信元と任意の宛先アドレスを使用した事前NATポリシー
Answer: A (メーッセージを残す**)**
説明

最新問題: **93**
Active Directoryユニバーサルグループでグループマッピングを使用する場合、ユーザーIDを設定する際に何をする必要がありますか？
A. LDAPサーバープロファイルを作成し、ポート3268またはSSLの場合は3269でグローバルカタログサーバーのルートドメインに接続します。
B. グループマッピングキャッシュをクリアする頻度スケジュールを設定します。
C. ユーザーベースのセキュリティポリシーのプライマリ従業員ID番号を設定します
D. RADIUSサーバープロファイルを作成し、LDAPSを使用してポート636でドメインコントローラーに接続します。
Answer: A (メーッセージを残す**)**

ユニバーサルグループを使用している場合は、まずLDAPサーバープロファイルを作成し、ポート3268（SSLの場合は3269）でグローバルカタログサーバーのルートドメインに接続します。次に、別のLDAPサーバープロファイルを作成し、ポート389でルートドメインコントローラーに接続します。これにより、すべてのドメインとサブドメインでユーザーとグループの情報が確実に利用できるようになります。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-users-to-groups

最新問題: **94**
ベストプラクティス評価に関して、正しい記述はどれですか？
A. ネットワークおよびセキュリティアーキテクチャのあらゆる領域におけるセキュリティリスク防止のギャップを明らかにするのに役立つ一連の質問票を提供します。
B. 経験豊富なセールスエンジニアが指導するこの評価は、予防活動に注力すべき最もリスクの高い領域を特定するのに役立ちます。
C. BPAツールはファイアウォール上でのみ実行可能です
D. 各評価データに対する採用率を示します
Answer: B (メーッセージを残す**)**

最新問題: **95**
Facebookチャットを使用するために、どのApp-IDアプリケーションを許可する必要がありますか？（2つ選択してください。）
A. Facebook
B. facebook-email
C. フェイスブックチャット
D. facebook-base
Answer: C,D (メーッセージを残す**)**

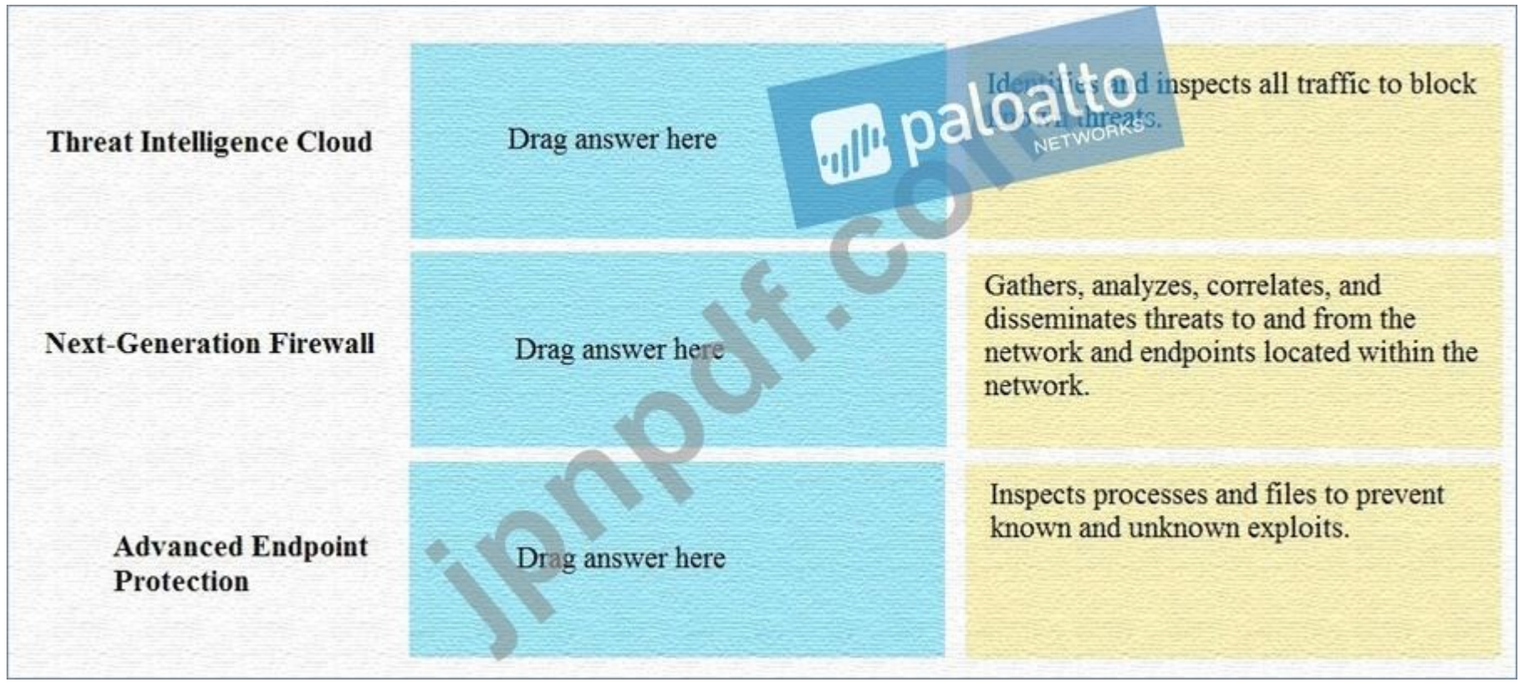
最新問題: **96**
ソースNATポリシーを作成する際、[変換パケット]タブのどの項目に[動的IPとポート]、[動的]、[静的IP]、[なし]のオプションが表示されますか？

A. インターフェース
B. IPアドレス
C. 翻訳タイプ
D. 住所タイプ
Answer: C (メーッセージを残す**)**

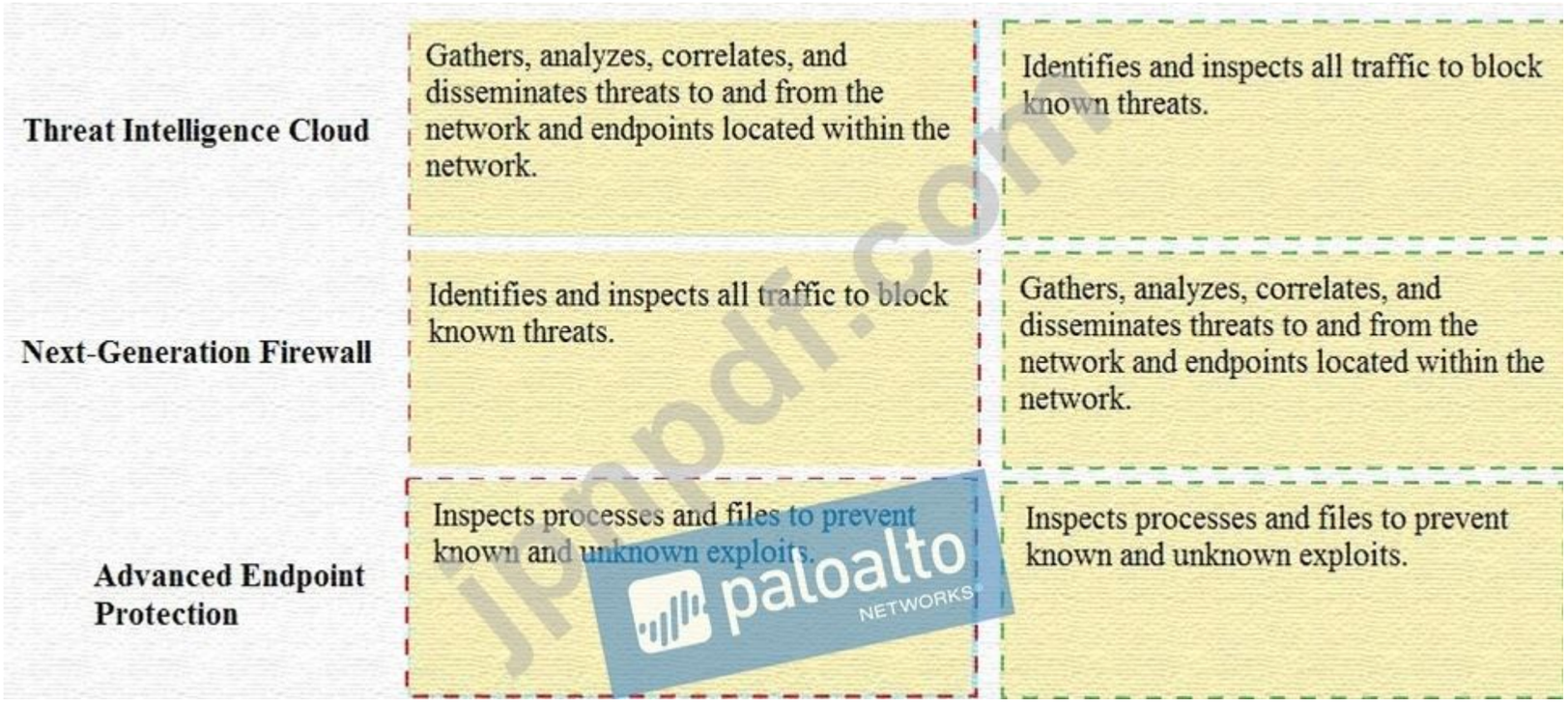
最新問題: **97**

コンテンツに対する制限がほとんどなく、攻撃者が違法または非倫理的なコンテンツを配布するために頻繁に利用するホスティングプロバイダーからのトラフィックを防止するのに役立つ機能はどれでしょうか？
A. パロアルトネットワークスの防弾IPアドレス
B. パロアルトネットワークスのC&C IPアドレス
C. パロアルトネットワークスが認識している悪意のあるIPアドレス
D. パロアルトネットワークスの高リスクIPアドレス
Answer: A (メーッセージを残す**)**
悪意のある、違法な、または非倫理的なコンテンツを提供するために防弾ホストを使用するホストをブロックするには、ポリシーで防弾IPアドレスリストを使用します。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/content-inspection-features/edl-for-bulletproo

最新問題**: 98**
Palo Alto Networks Security Operating Platformのアーキテクチャを、その説明と一致させてください。



Answer:



Explanation:

脅威インテリジェンスクラウド - ネットワークおよびネットワーク内に存在するエンドポイントに対する脅威を収集、分析、関連付け、配信します。

次世代ファイアウォール - すべてのトラフィックを識別および検査し、既知の脅威をブロックします。高度なエンドポイント保護 - プロセスとファイルを検査し、既知および未知のエクスプロイトを防止します。

最新問題**: 99**

ユーザー名をIPアドレスにマッピングする方法を3つ挙げてください。3つ選択してください。）

A. オートフォーカス

B. syslog

C. ポートマッピング

D. ミネメルド

E. サーバー監視

F. トラップ

Answer: B,C,E (メーッセージを残す**)**

最新問題**: 100**

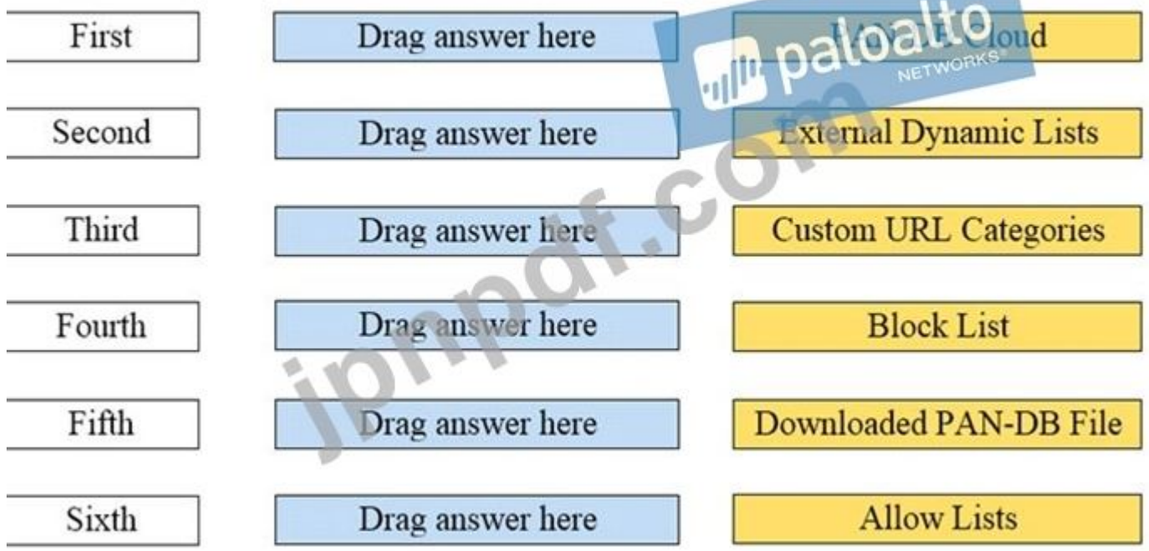
トポロジーを考慮すると、インターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？
A. タップ
B. トンネル
C. レイヤー3
D. バーチャルワイヤー
Answer: (解答を表示する)

最新問題: **101**
ネットワーク管理者は、ネットワーク接続のために動的ルーティングプロトコルを使用する必要があります。
この目的のために、NGFW仮想ルーターはどの3つの動的ルーティングプロトコルをサポートしていますか？ 3つ選択してください。）
A. EIGRP
B. IS-IS
C. BGP
D. OSPF
E. 安らかにお眠りください
Answer: C,D,E (メーッセージを残す)

最新問題: **102**
認証シーケンスを作成するために必要なプロファイルの種類はどれですか？ 2つ選択してください。）
A. サーバープロファイル
B. 認証プロファイル
C. セキュリティプロファイル
D. インターフェース管理プロファイル
Answer: A,B (メーッセージを残す)
ファイアウォールでは、認証プロファイルを指定する認証シーケンスを定義します。認証プロファイルを追加をクリックして、たとえば 『TACACS」という名前のプロファイルを定義すると、その認証プロファイルはTACACS+サー バープロファイルを呼び出します。

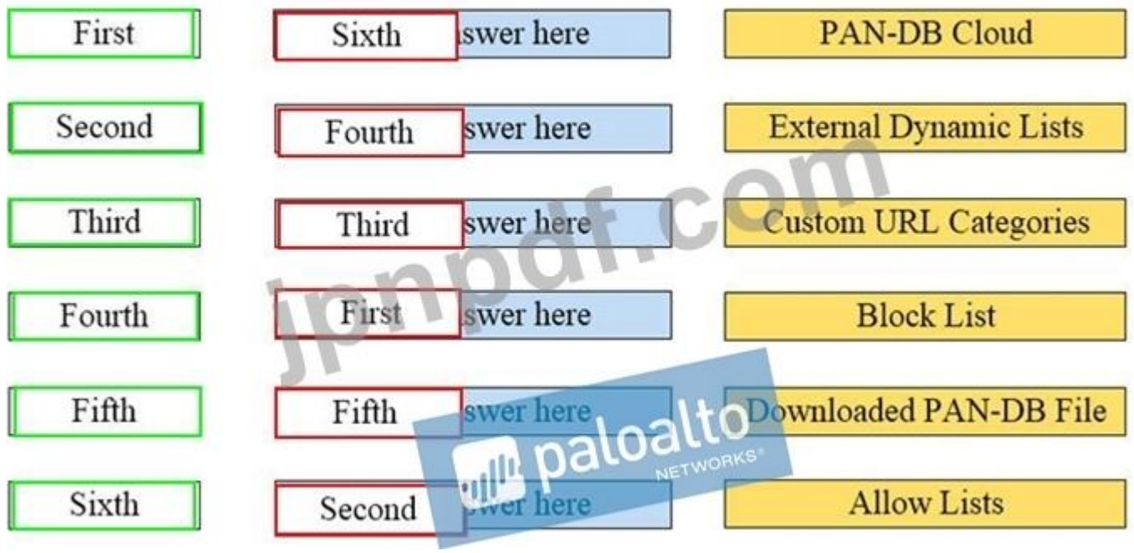
最新問題: **103**
システム内でURL分類が処理される正しい順序を設定してください。

Answer Area



Answer:

Answer Area



最新問題: **104**

管理者は、ユーザーが各自のオフィスアプリケーションを使用できるようにする必要があります。動的な環境で複数のアプリケーションを許可するには、管理者はファイアウォールをどのように設定すればよいでしょうか？

A. アプリケーションフィルタを作成し、 オフィス プログラム」という名前を付け、ビジネス システム カテゴリのオフィス プログラム サブカテゴリでフィルタを設定します。

B. アプリケーショングループを作成し、そこにビジネスシステムを追加します。

C. アプリケーションフィルタを作成し、 オフィス プログラム」という名前を付け、次に ビジネス システム」カテゴリでフィルタリングします。

D. アプリケーショングループを作成し、Office 365、Evernote、Google Docs、Libre Officeを追加します。

Answer: (解答を表示する**)**

説明
アプリケーションフィルタは、カテゴリ、サブカテゴリ、テクノロジー、リスク要因、特性など、ユーザーが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するオブジェクトです。これは、明示的に承認していないアプリケーションへのアクセスを安全に有効にしたいが、ユーザーがアクセスできるようにしたい場合に便利です。たとえば、従業員が業務で使用するオフィスプログラム（Evernote、Google Docs、Microsoft Office 365など）を自由に選択できるようにしたい場合などが考えられます。このようなアプリケーションを安全に有効にするには、カテゴリ「ビジネスシステム」とサブカテゴリ「オフィスプログラム」に一致するアプリケーションフィルタを作成します。新しいアプリケーション「オフィスプログラム」が登場し、新しいアプリIDが作成されると、これらの新しいアプリケーションは定義したフィルタに自動的に一致します。フィルタに定義した属性に一致するアプリケーションを安全に有効にするために、ポリシールールベースに追加の変更を加える必要はありません。
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: **105**
ミッションクリティカルなデバイスに関するベストプラクティスによると、ウイルス対策ソフトのアップデート推奨間隔はどのくらいですか？
A. 毎時
B. 分単位
C. 毎日
D. 毎週
Answer: (解答を表示する**)**

最新問題: **106**
ファイアウォールが新しい Wildfire アンチウイルス シグネチャをチェックするように設定できる最小頻度はどれくらいですか？
A. 5分ごと
B. 1分ごと
C. 24時間ごと
D. 30分ごと
Answer: B (メーッセージを残す**)**

WildFire	Provides near real-time malware and antivirus sig[illegible]eated as a result of the analysis done by the WildFire public cloud. **WildFire signature updates are made available every five minutes. You can set the firewall to check for new updates as frequently as every minute to ensure that the firewall retrieves the latest WildFire signatures within a minute of availability.** Without the WildFire subscription, you must wait at least 24 hours for the signatures to be provided in the Antivirus update.

最新問題: **107**
PAN-OSバージョン10.0で導入されたDNSセキュリティサービスに関して、正しい記述は次のうちどれですか？ 2つ選択）
A. PAN-DBと同様の機能を持ち、アプリポータル経由でのアクティベーションが必要です。

B. 動的DNS更新の必要性を排除します。
C. ITは自動的に有効化され、設定されます。
D. ダウンロードした DNS アップデートの DNS エントリの 100K 制限を解除します。
Answer: A,D (メーッセージを残す)

最新問題: **108**
管理者は、LAN ゾーンまたは VPN ゾーンから発信され、DMZ ゾーンまたは Untrust ゾーン宛ての DNS トラフィックに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ます。
管理者は、送信元ゾーンと宛先ゾーンがLANであるトラフィックを照合したくないし、送信元ゾーンと宛先ゾーンがVPNであるトラフィックも照合したくない。
どのセキュリティポリシー規則タイプを使用すべきでしょうか？
A. イントラゾーン
B. デフォルト
C. インターゾーン
D. ユニバーサル
Answer: (解答を表示する)

最新問題: **109**
セキュリティポリシールールに基づいて、内部ゾーンから外部ゾーンへのすべてのFTPトラフィックに一致するルールはありますか？

A. インターコーンデフォルト
B. インサイドポータル
C. 内部DMZ
D. 外部からの進入
Answer: A (メーッセージを残す)

最新問題: **110**
管理者がアドレスオブジェクトを作成するには、どのタブをクリックすればよいですか？
A. モニター
B. 物体
C. ポリシー
D. デバイス
Answer: B (メーッセージを残す)

最新問題: **111**
管理者は、アプリケーションと脅威の動的アップデートをスケジュールする際に、アップデートのインストールを一定期間遅延させるにはどうすればよいですか？

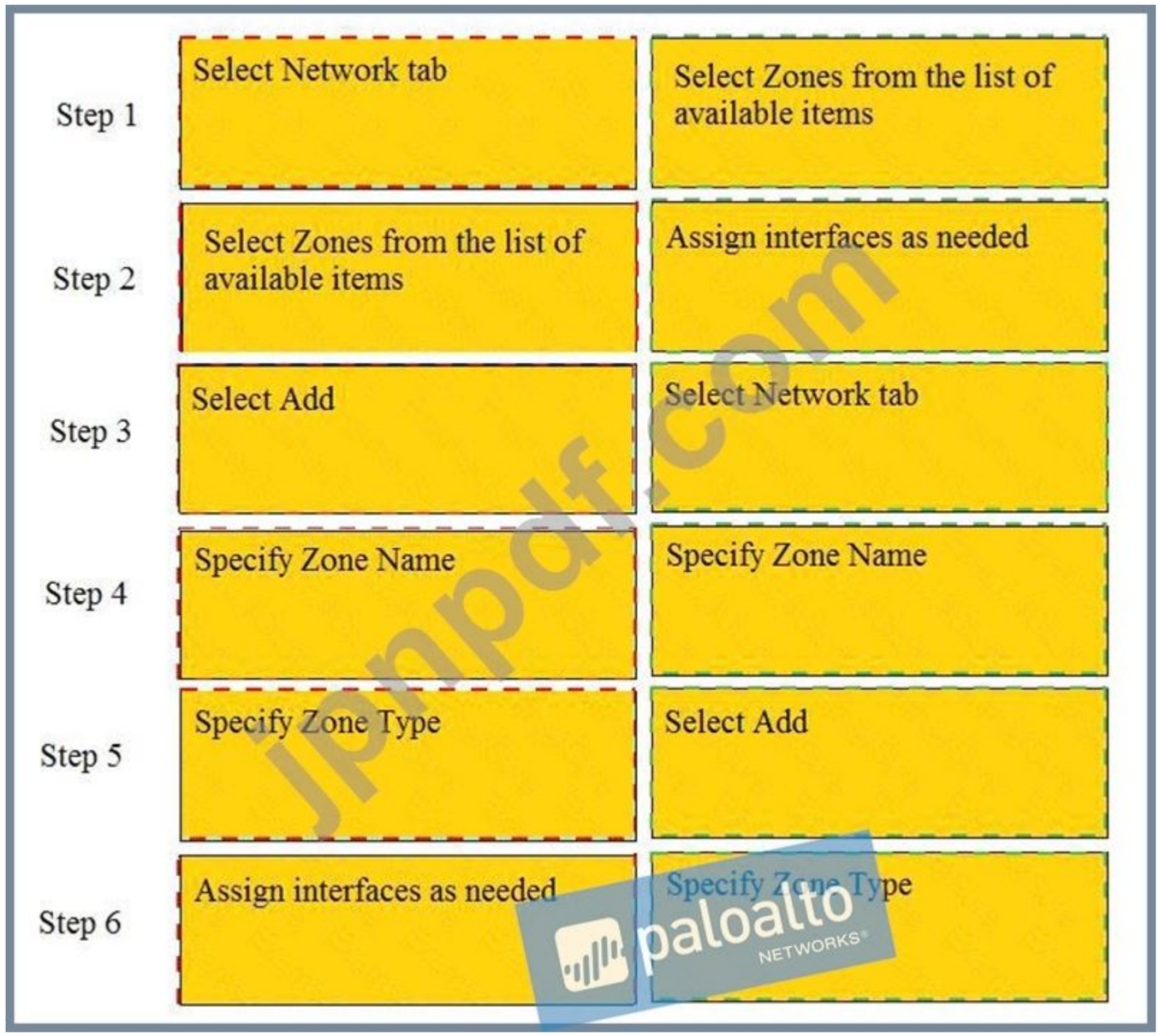
A. 平日は自動更新を無効にする
B. ﾚしきい値」のオプションを設定します
C. 新規アプリケーションを無効にする」オプションを使用して自動的に ﾀウンロードしてインストール」します
D. 管理者がアップデートを承認した後、アプリケーションと脅威を自動的に ﾀウンロードのみ」し、後でインストールします。
Answer: B (メーッセージを残す**)**

最新問題**: 112**
ポリシーオプティマイザの主な機能は何ですか？
A. 組み合わせ可能なセキュリティルールを強調表示することで、管理プレーンの負荷を軽減します。
B. 他のファイアウォールベンダーのセキュリティルールをPalo Alto Networksの設定に移行する
C. ｾッション開始時にログを記録する」セキュリティルールを削除する
D. ポートベースのセキュリティルールをアプリケーションベースのセキュリティルールに変換する
Answer: D (メーッセージを残す**)**
説明／参考資料：参考資料https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html

最新問題**: 113**
Palo Alto Networks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順番に説明します。

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 - 利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
ステップ4 - ゾーン名を指定する
ステップ5 - ゾーンタイプの指定
ステップ6 - 必要に応じてインターフェースを割り当てる

最新問題: **114**
パケット数に基づく攻撃を防ぐには、どの防御技術が有効でしょうか？
A. ゾーン保護プロファイル

B. URLフィルタリングプロファイル
C. ウイルス対策プロファイル
D. 脆弱性プロファイル
Answer: A (メーッセージを残す**)**
DoS保護機能は、個々のデバイスに対する攻撃に対する防御層をさらに強化するものであり、ゾーン保護プロファイルのしきい値がデバイスへの攻撃のCPSレートを上回っている場合に有効となる。

最新問題**: 115**
セキュリティポリシールールに基づいて、内部ゾーンから外部ゾーンへのすべてのFTPトラフィックに一致するルールはありますか？

A. 内部DMZ
B. インターコーンデフォルト
C. 外部からの進入
D. インサイドポータル
Answer: B (メーッセージを残す**)**

最新問題**: 116**
スクリーンショットに基づいて、 ft」とラベル付けされたユーザーグループの目的は何ですか？

A. 全てのポートでITアプリケーションへのアクセスを可能にします
B. グループ DMZ」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。
C. グループ ft」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. DMZゾーン内のサーバーに 任意の」ユーザーがアクセスできるようにします。
Answer: C (メーッセージを残す**)**

最新問題**: 117**
管理者が外部の動的リストに対して例外を手動で適用しようとしています。一部のエントリは赤線で下線が引かれて表示されています。
このエラーの原因は何でしょうか？
A. 項目には記号が含まれています。
B. エントリはワイルドカードです。

C. エントリには正規表現が含まれています。
D. エントリが重複しています。
Answer: (解答を表示する**)**
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**
提示されたセキュリティポリシー規則に基づくと、SSHはどのポートで許可されますか？

			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. 任意の港
B. デフォルトポート
C. 一時的な港のみ
D. SSLおよびSNMPv3と同じポート
Answer: B (メーッセージを残す**)**

最新問題**: 119**
管理者が、デフォルトのNATルールから特定のフローを除外する 『NATなし」ルールを作成したいと考えています。これを行うための最適な方法はありますか？
A. アプリケーションオーバーライド付きの静的NATルールを作成します。
B. 正しいパラメータで新しいNATルールを作成し、翻訳タイプを 『なし」のままにします。
C. セキュリティ ポリシー ルールを作成して、トラフィックを許可します。
D. 宛先インターフェースに変換する静的NATルールを作成します。
Answer: (解答を表示する**)**

最新問題**: 120**
管理者は、ホストへの攻撃に使用されている新しいマルウェアに関する通知を受け取ります。
このマルウェアは、一般的なアプリケーションのソフトウェア上の脆弱性を悪用する。
管理者がファイアウォールの脅威シグネチャデータベースを更新した後、どのセキュリティプロファイルがこの脅威を検出し、アクセスをブロックしますか？
A. 送信セキュリティポリシールールに適用されるデータフィルタリングプロファイル
B. 送信セキュリティポリシールールに適用されるウイルス対策プロファイル
C. 受信セキュリティポリシールールに適用される脆弱性プロファイル
D. 受信セキュリティポリシールールに適用されるデータフィルタリングプロファイル
Answer: (解答を表示する**)**

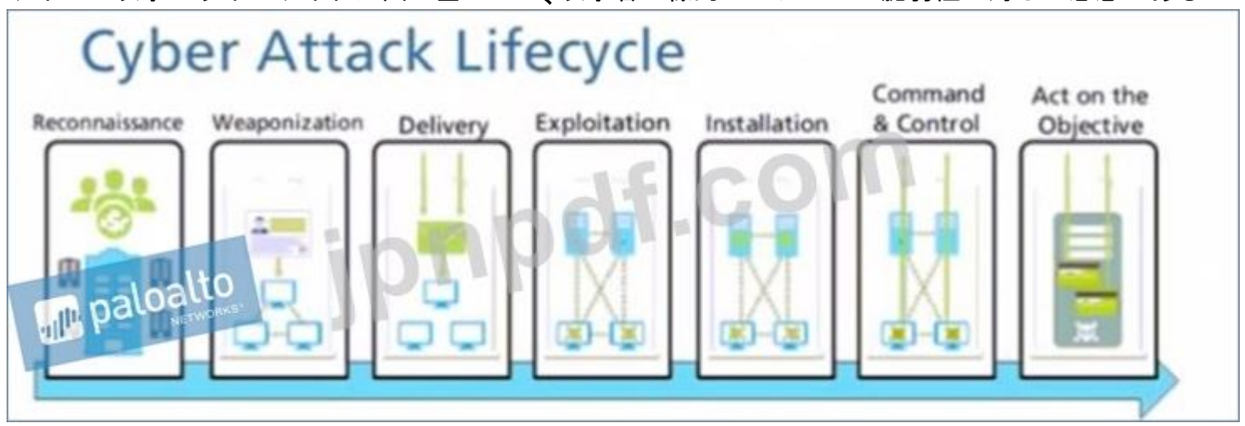
最新問題: **121**
ウイルス対策プロファイル内で有効な選択肢を2つ挙げてください。2つ選択してください。）
A. ドロップ
B. ブロックIP
C. 拒否
D. デフォルト
Answer: A,D (メーッセージを残す**)**

最新問題: **122**
ファイアウォールを通過するトラフィックをログに記録するためのベストプラクティスは何ですか？
A. セッション開始時とセッション終了時の両方のログ記録を有効にします。
B. セッション開始時のみログを有効にする。
C. セッション終了時のみログを有効にする。
D. すべてのログ記録オプションを無効にします。
Answer: (解答を表示する**)**
ファイアウォールを通過するトラフィックをログに記録するベストプラクティスは、 "セッション終了時のみログ記録を有効にする」ことです。このオプションを有効にすると、ファイアウォールはセッションが終了したときにのみログエントリを生成するため、ファイアウォールとログストレージへの負荷が軽減されます。ログエントリには、送信元および宛先IPアドレス、ポート、ゾーン、アプリケーション、ユーザー、バイト数、パケット数、セッションの継続時間などの情報が含まれます。 "セッション終了時のみログ記録」オプションでは、最終的なアプリケーションとユーザー、合計バイト数とパケット数、セッション終了理由1など、セッションに関するより正確な情報も提供されます。 "セッション終了時のみログ記録を有効にする」には、次の手順を実行する必要があります。
ログに記録したいトラフィックに一致するセキュリティポリシールールを作成または変更します。
ポリシールールの "アクション」タブを選択し、 "セッション終了時にログを記録する」オプションをオンにします。
変更内容をファイアウォールまたはPanoramaと管理対象ファイアウォールにコミットします。

最新問題: **123**
最近、ファイアウォールのポリシーを最適化するために変更が加えられましたが、セキュリティチームはこれらの変更が効果を発揮してい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のヒットカウンター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キーを押してください。
B. ルールをハイライトし、各ルールに対して "ルールヒットカウンターのリセット」> "選択したルール」を使用します。
C. ファイアウォールを再起動してください
D. [ルールヒットカウンターのリセット] > [すべてのルール] オプションを使用する
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: **124**
管理者は、ファイアウォールを通過するトラフィックのログ記録に関するベストプラクティスに従いたいと考えている。
どのログ設定が正しいですか？
A. セッション開始時にログを有効にする
B. すべてのログ記録を無効にする
C. セッション開始時と終了時の両方でログを有効にする
D. セッション終了時にログを有効にする
Answer: (解答を表示する**)**

最新問題: **125**
サイバー攻撃のライフサイクル図に基づいて、攻撃者が標的のマシン上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てください。



A. 搾取
B. 目標に向かって行動する
C. インストール
D. 偵察
Answer: A (メーッセージを残す**)**

最新問題: **126**
サイバー攻撃ライフサイクル図に基づいて、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てください。

A. 偵察

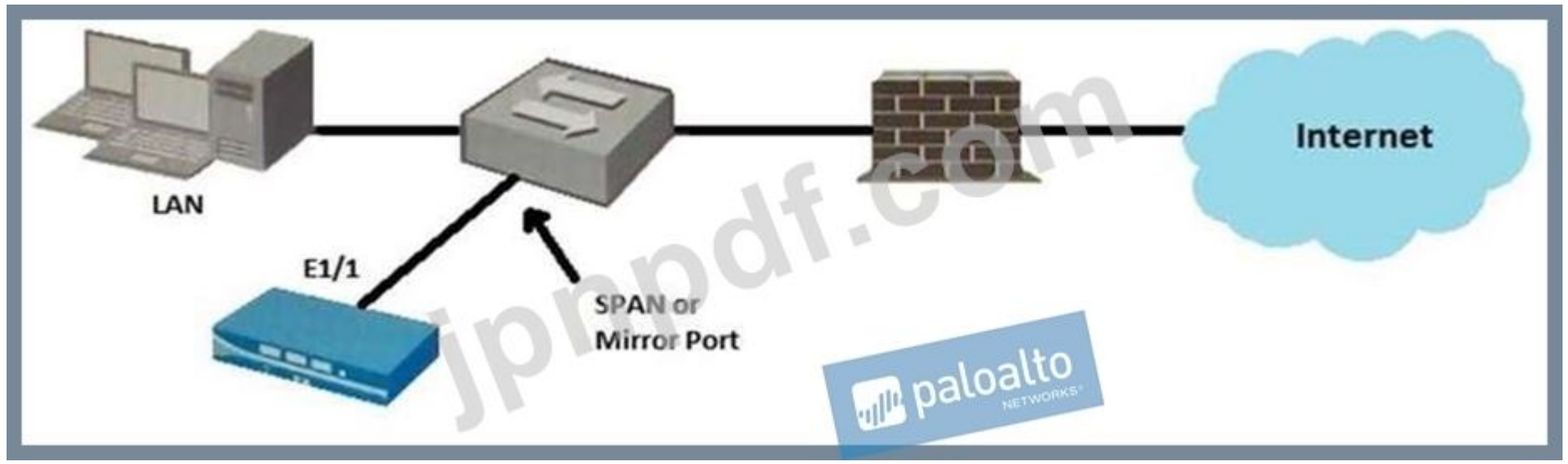
B. 目標に向かって行動する
C. 搾取
D. インストール
Answer: C (メーッセージを残す**)**

最新問題**: 127**
DNSトラフィックを使用して保護されたネットワーク上の感染ホストを特定するには、どのセキュリティプロファイルを適用しますか？
A. URLトラフィック
B. 脆弱性対策
C. スパイウェア対策
D. ウイルス対策
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**: 128**
管理者が、一致条件に単一のアプリケーションが含まれ、アクションが拒否となるセキュリティポリシーを設定しました。
アプリケーションのデフォルトの拒否アクションがreset-bothの場合、ファイアウォールはどのようなアクションを実行しますか？
A. トラフィックをサイレントに破棄し、ICMP到達不能コードを送信します。
B. クライアント側とサーバー側のデバイスにTCPリセットを送信します
C. 静かにトラフィックを遮断します
D. サーバー側のデバイスにTCPリセットを送信します
Answer: B (メーッセージを残す**)**

最新問題**: 129**
『0 5 1 1/0 127 248 2」はどのタイプのアドレスオブジェクトですか？
A. IPワイルドカードマスク
B. IPサブネット
C. IP範囲
D. IPネットマスク
Answer: A (メーッセージを残す**)**

最新問題**: 130**



トポロジーを考慮すると、ファイアウォールインターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？

A. タップ

B. トンネル

C. バーチャルワイヤー

D. レイヤー3

Answer: (解答を表示する**)**

説明／参考資料：

最新問題**: 131**

管理者が、ベストプラクティスに沿うようセキュリティポリシーを更新しています。

以下のスクリーンショットに表示されているのは、ポリシーオプティマイザーのどの機能ですか？

A. 未使用アプリ

B. 新しいアプリビューアー

C. ルール使用法

D. アプリ制御なしのルール

Answer: (解答を表示する**)**

最新問題**: 132**

ファイアウォールが新しい Wildfire アンチウイルス シグネチャをチェックするように設定できる最小頻度はどれくらいですか？

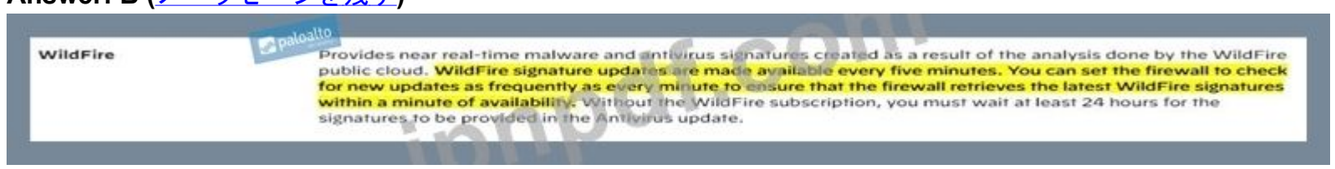
A. 5分ごと

B. 1分ごと

C. 24時間ごと

D. 30分ごと

Answer: B (メーッセージを残す**)**



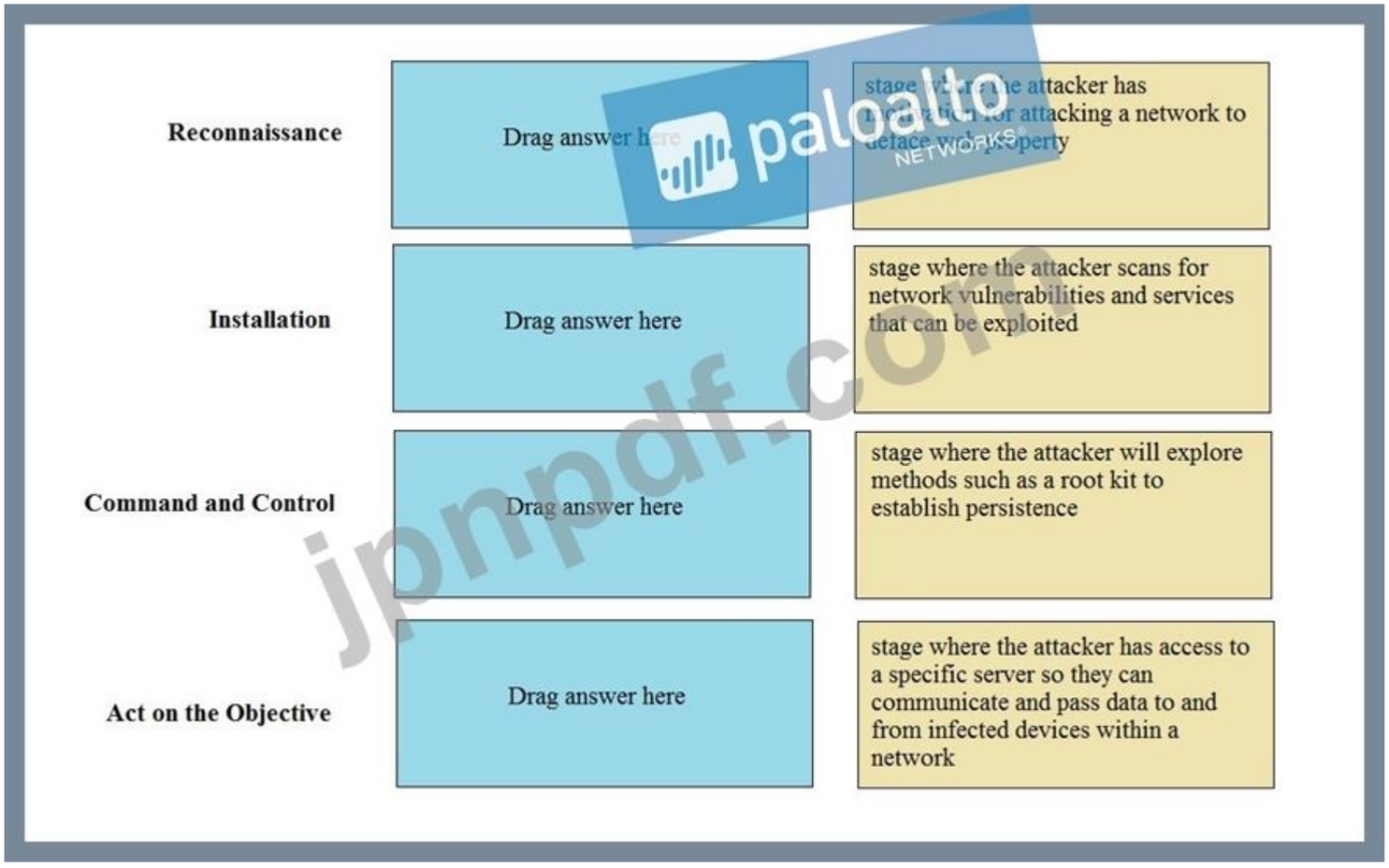
最新問題: **133**
ドメイン生成アルゴリズムで使用できる3つの要素は何ですか？ 3つ選択してください。）
A. 暗号鍵
B. 時刻
C. その他の固有値
D. URLカスタムカテゴリ
E. IPアドレス
Answer: A,B,C (メーッセージを残す)
ドメイン生成アルゴリズム（DGA）は、悪意のあるコマンド＆コントロール（C2）通信チャネルを確立する際に、通常、多数のドメインを自動生成するために使用されます。DGAベースのマルウェア（Pushdo、BankPatch、CryptoLockerなど）は、多数の候補ドメインの中にアクティブなC2サーバーの場所を隠すことで、ブロックされるドメインの数を制限します。また、時間帯、暗号鍵、その他の固有の値などの要素に基づいてアルゴリズム的に生成することができます。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-al

最新問題: **134**
セキュリティポリシーの適用状況と使用状況を監視するために何が使用されますか？
A. セキュリティプロファイル
B. アプリID
C. ポリシーベース転送
D. ポリシーオプティマイザ
Answer: (解答を表示する)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/policies/policies-security/applications-and-usage

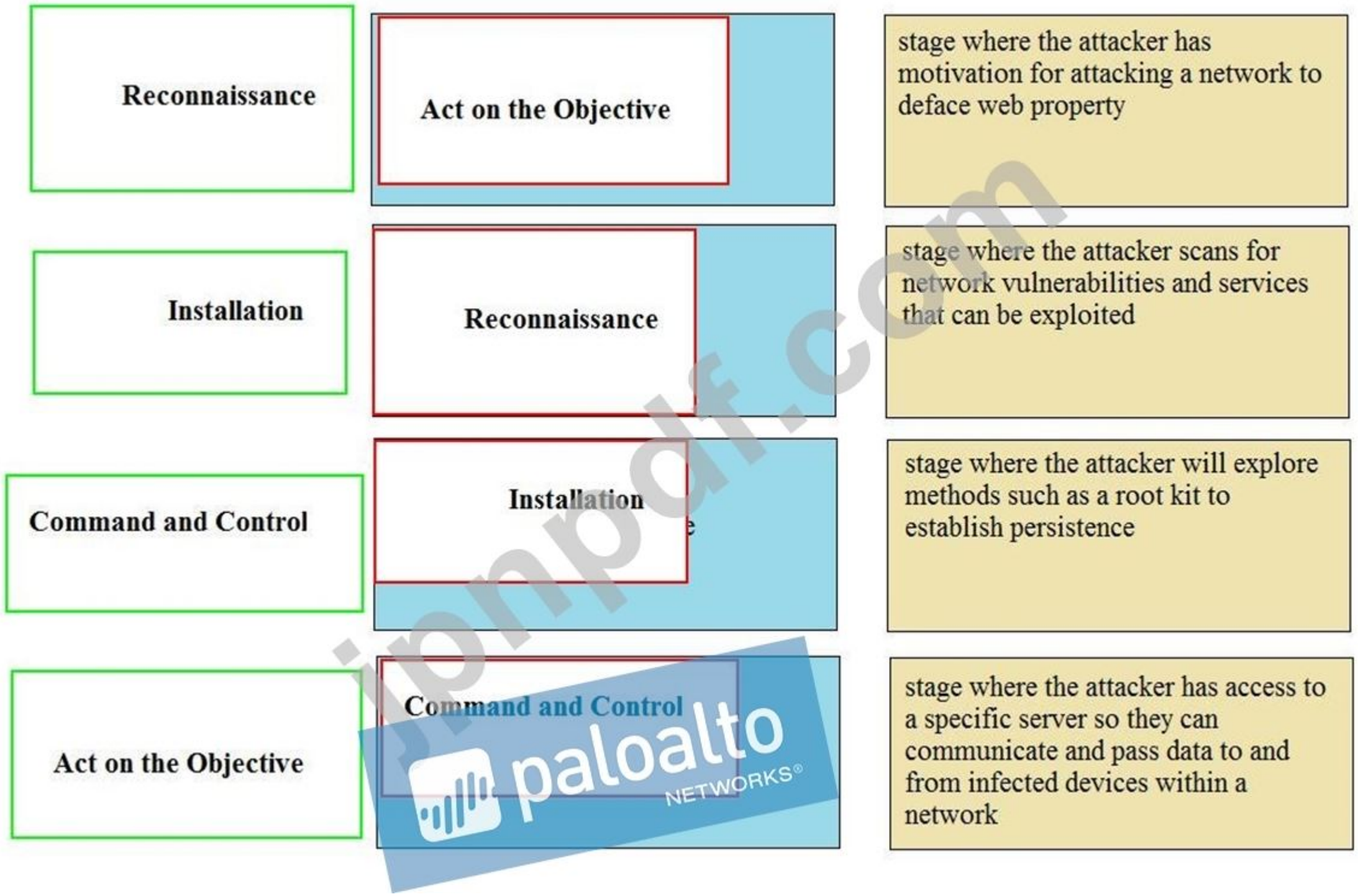
最新問題: **135**
管理者がNATルールを設定しています
最低限必要な情報は次のうちどれですか？ 3つ選択してください。）
A. 発生源ゾーン
B. 名前
C. 目的地ゾーン
D. 宛先インターフェース
E. 宛先住所
Answer: A,C,E (メーッセージを残す)

最新問題: **136**
DNSシンクホール設定でシンクホールIPアドレスを構成するために使用できるセキュリティプロファイルはどれですか？
A. 脆弱性対策
B. アンチスパイウェア
C. アンチウイルス
D. URLフィルタリング
Answer: B (メーッセージを残す)
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

最新問題: **137**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。



Answer:



最新問題: **138**
インターネットコンテンツへのアクセスが制限された場合、エンドユーザーに通知するにはどのような措置を講じるべきでしょうか？
A. 通知が有効になっているカスタム「URLカテゴリ」オブジェクトを作成します。
B. セキュリティポリシー拒否ログの監視データを公開します。
C. すべてのURLサイトの「サイトアクセス」設定が「警告」に設定されていることを確認してください。
D. インターネットアクセスを提供するインターフェースで「応答ページ」を有効にします。
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/device/device-response-pages.html

最新問題: **139**
どの管理者が、ホストに感染する新しいマルウェアに関するグローバル通知を受け取りますか？感染すると、感染したホストはコマンド＆コントロール (C2) サーバーへの接続を試みます。
ファイアウォールのシグネチャデータベースが更新された後、どのセキュリティプロファイルコンポーネントがこの脅威を検知し、防止するのでしょうか？
A. 送信セキュリティポリシーに適用されるウイルス対策プロファイル
B. 受信セキュリティポリシーに適用されるデータフィルタリングプロファイル
C. 送信セキュリティポリシーに適用されるデータフィルタリングプロファイル
D. 受信セキュリティポリシーに適用される脆弱性プロファイル
Answer: C (メーッセージを残す**)**
説明

最新問題: **140**
管理者は、10個のデバイスグループと5つのテンプレートにまたがる、100台のPanorama管理ファイアウォール上のセキュリティポリシーで、同じアドレスオブジェクトを参照したいと考えています。
管理者はアドレスオブジェクトを作成する際に、どの設定操作を行うべきですか？
A. アドレスオブジェクトにグローバルタグを付ける。
B. オーバーライド無効化が解除されていることを確認してください。
C. 共有」オプションがチェックされていることを確認してください。
D. 共有」オプションがオフになっていることを確認してください。
Answer: (解答を表示する**)**
10 台の Panorama 管理ファイアウォール上のセキュリティ ポリシーで、10 のデバイス グループと 5 つのテンプレートにわたって同じアドレス オブジェクトを参照するには、管理者はアドレス オブジェクトの作成時に [共有] オプションがチェックされていることを確認する必要があります。このオプションを使用すると、管理者は Panorama 上のすべてのデバイス グループとテンプレートで使用できる共有アドレス オブジェクトを作成できます。共有アドレス オブジェクトは、複数のファイアウォール ポリシー ルール、フィルタ、およびその他の機能で使用できます 1。これにより、複数のファイアウォールにわたるアドレス オブジェクトの管理の複雑さと重複が軽減されます 2。参照: アドレス オブジェクト、共有アドレス オブジェクトの作成、認定 - Palo Alto Networks、Palo Alto Networks 認定ネットワーク セキュリティ アドミニストレーター (PAN-OS 10.0) または [Palo Alto Networks 認定ネットワーク セキュリティ アドミニストレーター (PAN-OS 10.0)]。

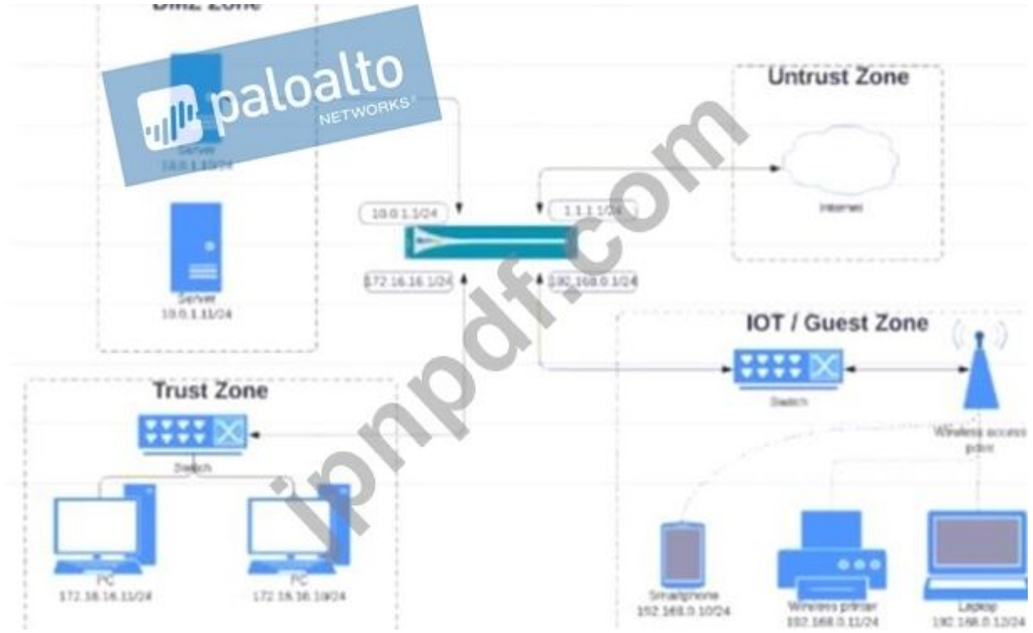
最新問題: **141**
貴社は、新たなコンプライアンス要件に対応するため、無線機器が使用するすべてのIPアドレスについて、ユーザー名との関連付けを必須としています。無線機器自体へのダウンタイムや設定変更を最小限に抑えつつ、IPアドレスとユーザーのマッピング情報をできるだけ早く収集する必要があります。なお、無線機器は様々なメーカーの製品です。
このシナリオを踏まえ、IPアドレスとユーザーのマッピング情報をNGFWに送信するオプションを選択してください。
A. 半径
B. XFFヘッダー
C. syslog
D. UID再配布
Answer: C (メーッセージを残す**)**

最新問題: **142**
スクリーンショットに基づいて、ログに記録されたトラフィックに関する正しい記述を2つ選びなさい。2つ選択してください。）

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. ウェブセッションが復号化されました。
B. セキュリティプロファイルによりトラフィックが拒否されました。
C. URLフィルタリングによりトラフィックが拒否されました。
D. ウェブセッションの復号化に失敗しました。
Answer: A (メーッセージを残す**)**

最新問題**: 143**



ネットワーク図を考慮すると、信頼済みユーザーとゲストユーザーの両方が、SSH、Webブラウジング、SSLアプリケーションを使用して、一般的なインターネットおよびDMZサーバーにアクセスできるようにする必要があります。目的の結果を達成するポリシーはどれですか？

A)

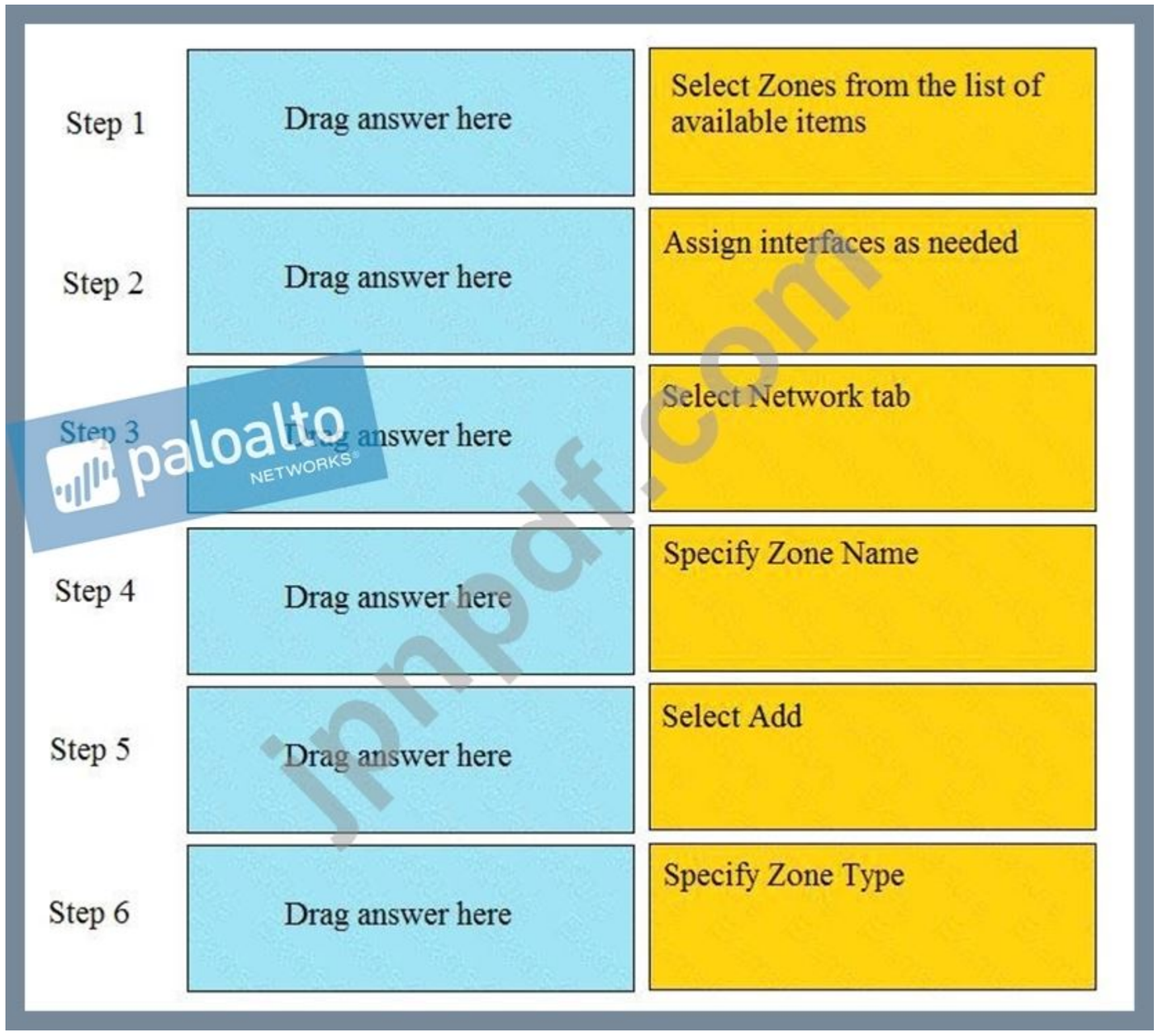
B)

C)

D)

A. オプション
B. オプション
C. オプション
D. オプション
Answer: (解答を表示する**)**

最新問題**: 144**
Palo Alto Networks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順番に説明します。


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 - 利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
ステップ4 - ゾーン名を指定する
ステップ5 - ゾーンタイプの指定
ステップ6 - 必要に応じてインターフェースを割り当てる

最新問題: **145**
セキュリティポリシーに添付できるセキュリティプロファイルの種類はどれですか？ 2つ選択してください。）
A. ウイルス対策

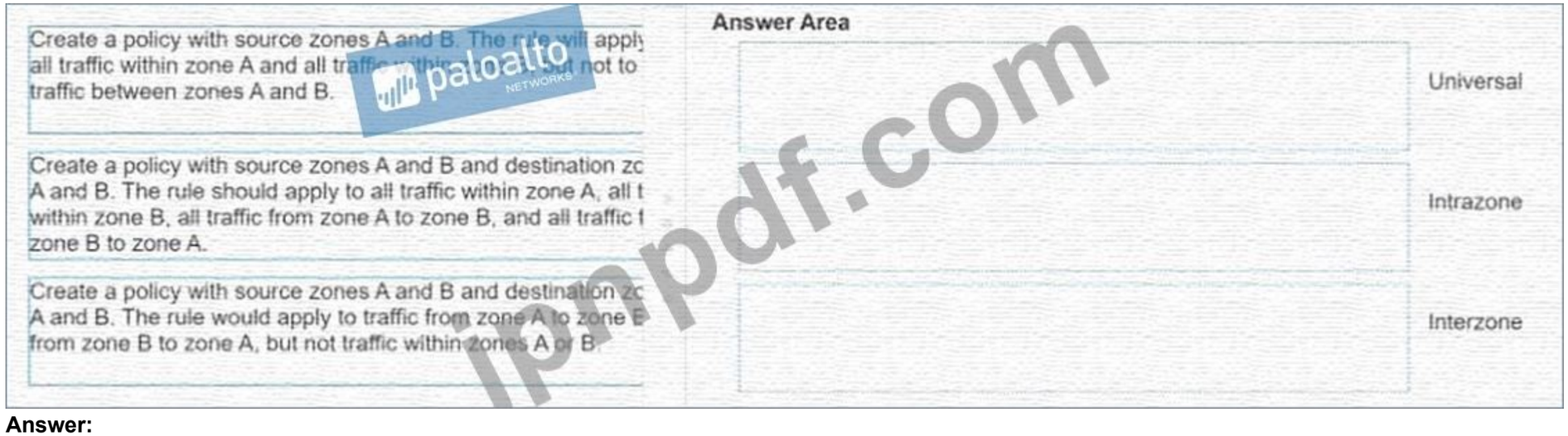
B. DDoS攻撃対策
C. 脅威
D. 脆弱性
Answer: A,D (メーッセージを残す**)**
参考文献：

最新問題**: 146**
提供された画像に基づいて、セキュリティポリシー規則に当てはまる記述を2つ選択してください。

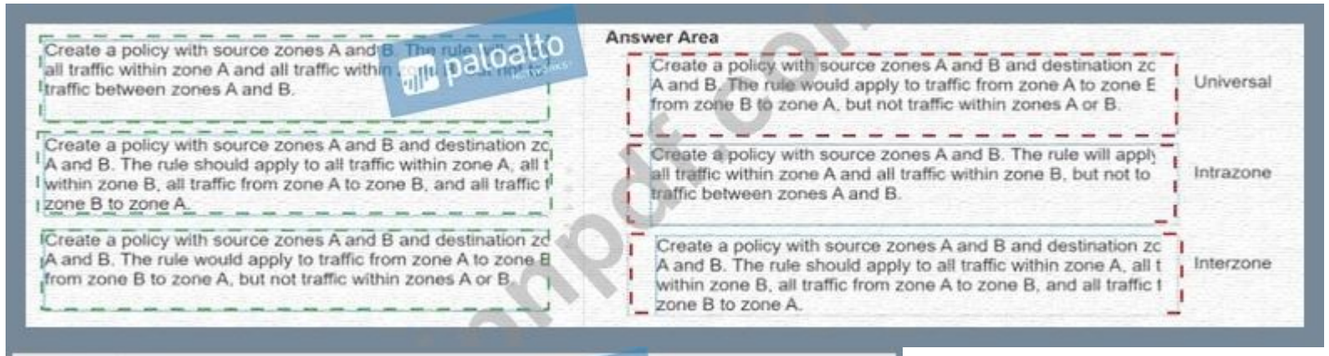
				Source			Destination						
	NAME	TAGS	TYPE	ZONE	ADDRESS	DEVICE	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
19	Allow-Office-Programs	none	universal	Internal	any	any	External	any	office-programs	application-defa...	Allow		
20	Allow-FTP	none	universal	Internal	any	any	External	FTP Server	any	FTP	Allow		
21	Allow-Social-Media	none	universal	Internal	any	any	External	any	facebook	application-defa...	Allow		
22	intrazone-default	none	intrazone	any	any	any	(intrazone)	any	any	any	Allow	none	
23	interzone-default	none	interzone	any	any	any	any	any	any	any	Deny	none	

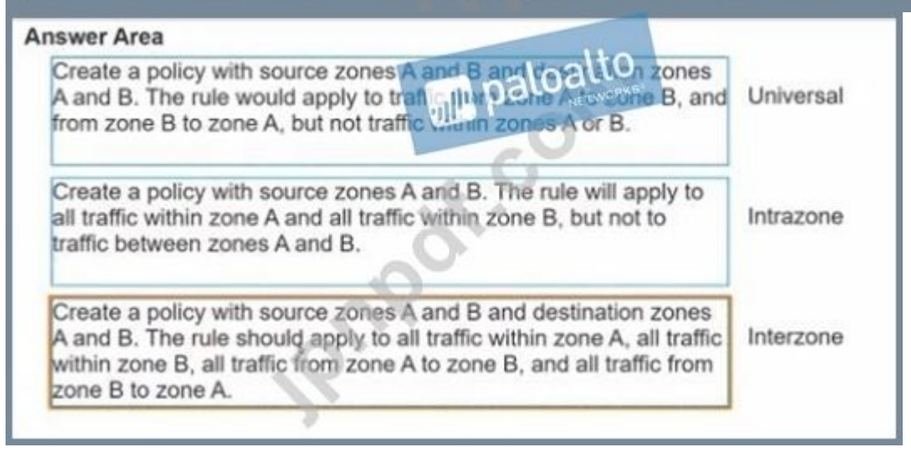
A. Allow-FTP ポリシーでは、App-ID を使用して FTP が許可されます。
B. Allow-Office-Programs ルールはアプリケーションフィルタを使用しています。
C. Allow-Social-Mediaルールは、すべてのFacebook機能を許可します。
D. Allow-Office-Programs ルールはアプリケーション グループを使用しています。
Answer: B,C (メーッセージを残す**)**

最新問題**: 147**
各ルールタイプと例を一致させてください。



Answer:





最新問題: **148**
App-IDアプリケーションタグを操作する際に許可される操作はどれですか？
A. 定義済みのタグは削除できます。
B. 定義済みのタグは、WildFireの動的更新によって更新される場合があります。
C. 定義済みのタグは変更可能です。
D. 定義済みのタグにカスタムタグを追加できます。
Answer: C (メーッセージを残す)

最新問題: **149**
管理者は、www.paloaltonetworks.comへのアクセスを許可しつつ、同じカテゴリに属する他のすべてのサイトへのアクセスを拒否したいと考えています。
管理者は、www.paloaltonetworks.comへのアクセスを許可するセキュリティポリシールールのマッチング条件として使用するために、どのオブジェクトを作成する必要がありますか？
A. アプリケーショングループ
B. アドレス ab
C. URLカテゴリ
D. サービス
Answer: C (メーッセージを残す)
URL カテゴリ オブジェクトは、管理者が作成して、www.paloaltonetworks.com へのアクセスを許可しつつ、同じカテゴリ内の他のすべてのサイトへのアクセスを拒否するセキュリティ ポリシー ルールの一致条件として使用するオブジェクトです。URL カテゴリ オブジェクトを使用すると、管理者は、ビジネスや経済などの特定のカテゴリに属する URL のカスタム リストを定義できます。管理者は、このオブジェクトをセキュリティ ポリシー ルールで使用して、カテゴリに基づいて URL へのアクセスを許可または拒否できます 1。たとえば、管理者は、www.paloaltonetworks.com を含む URL カテゴリ オブジェクトを作成し、それをビジネスや経済カテゴリに割り当てることができます。次に、管理者は、この URL カテゴリ オブジェクトへのアクセスを許可し、定義済みのビ

ジネスや経済カテゴリへのアクセスを拒否するセキュリティ ポリシー ルールを作成できます 2。参考資料: カスタム URL カテゴリの作成、カスタム URL カテゴリへのアクセスを許可または拒否するセキュリティ ポリシー ルールの作成、認定資格 - Palo Alto Networks、Palo Alto Networks 認定ネットワーク セキュリティ管理者 (PAN-OS 10.0) または [Palo Alto Networks 認定ネットワーク セキュリティ管理者 (PAN-OS 10.0)]。

最新問題: **150**
URLカテゴリは、どの2種類のポリシータイプにおいてマッチング条件として使用できますか？ 2つ選択してください。）
A. 認証
B. 復号化
C. アプリケーションオーバーライド
D. 夜
Answer: A,B (メーッセージを残す**)**
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: **151**
予防姿勢評価に関して、正しい記述はどれですか？
A. セキュリティポリシー採用ヒートマップコンポーネントは、デバイスグループ、シリアル番号、ゾーン、アーキテクチャ領域、その他のカテゴリで情報をフィルタリングします。
B. ネットワークおよびセキュリティアーキテクチャのあらゆる領域におけるセキュリティリスク防止のギャップを明らかにするのに役立つ一連の質問票を提供します。
C. 各評価領域における採用率をパーセンテージで示します。
D. 評価のためにPanorama/ファイアウォールに対して200以上のセキュリティチェックを実行します
Answer: (解答を表示する**)**
説明／参考資料 :https://docs.paloaltonetworks.com/best-practices/8-1/data-center-best-practices/data-center-best-practice-security-policy/use-palo-alto-networks-assessment-and-review-tools

最新問題: **152**
デフォルトでは、interzone-default ルールにはどのアクションが割り当てられますか？
A. 許可する
B. サーバーリセット
C. 否定する
D. Reset-client
Answer: C (メーッセージを残す**)**

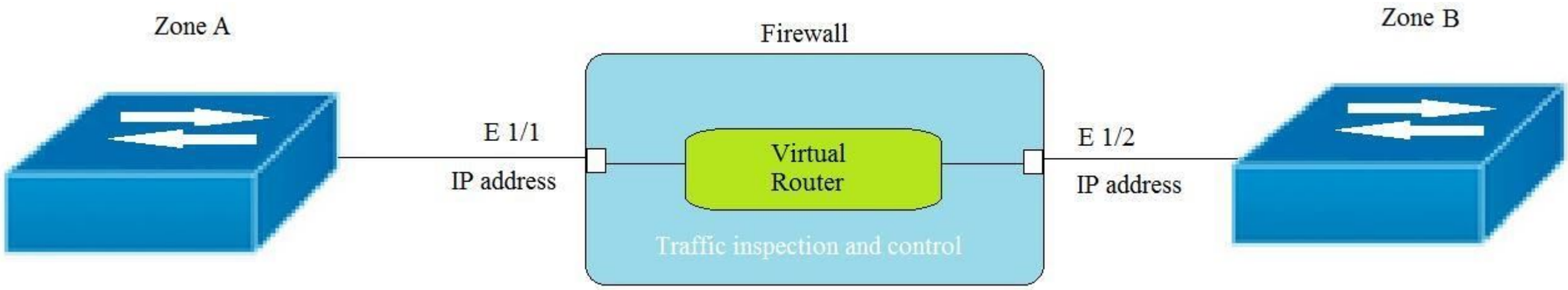
最新問題: **153**
ウイルス対策セキュリティプロファイルの 「アクション」タブで編集できるアクション列はどれですか？
A. ウイルス
B. 署名

C. スパイウェア
D. トロイの木馬
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-web-interface-help/objects/objects-security-profiles-antivirus

最新問題**: 154**
管理者は、危険なメディアコンテンツサイトへのアクセスを制限したいと考えています。この目的を達成するには、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べきでしょうか？ 2つ選択してください）
A. 高リスク
B. レクリエーションと趣味
C. ストリーミングメディア
D. 既知のリスク
Answer: B,C (メーッセージを残す**)**

最新問題**: 155**
管理者は、複数の送信元IPアドレスを同じパブリックIPアドレスに変換できるようにするNATポリシーを作成したいと考えています。これを実現するのに最も適切なNATポリシーはどれでしょうか？
A. 動的IP
B. 動的IPアドレスとポート番号
C. 目的地
D. 固定IPアドレス
Answer: B (メーッセージを残す**)**

最新問題**: 156**
トポロジーを考慮すると、ゾーンAとゾーンBにはどのゾーンタイプを設定すべきでしょうか？



A. レイヤー2
B. バーチャルワイヤー
C. レイヤー3
D. タップ
Answer: (解答を表示する**)**

最新問題**: 157**
ローカルデータベースのユーザーアカウントを追加し、そのユーザーを割り当てる新しいグループを作成するために必要な手順の順序を適切に定義しているのは、どの操作リストですか？
A. 1. デバイス > ローカル ユーザー データベース > ユーザーに移動し、[追加] をクリックします。2. ユーザーの名前を入力します。3. パスワードまたはハッシュを入力して確認します。4. アカウントを有効にして、[OK] をクリックします。5. デバイス > ローカル ユーザー データベース > ユーザー グループに移動し、[追加] をクリックします。6. グループの名前を入力します。7. ユーザーをグループに追加して、「OK」をクリックします。
B. 1. デバイス > 認証プロファイル > ユーザーに移動し、「追加」をクリックします。2. ユーザーの名前を入力します。3. パスワードまたはハッシュを入力して確認します。4. アカウントを有効にして「OK」をクリックします。5. デバイス > ローカルユーザーデータベース > ユーザーグループに移動し、「追加」をクリックします。6. グループの名前を入力します。7. ユーザーをグループに追加して、「OK」をクリックします。
C. 1. デバイス > ユーザーに移動し、「追加」をクリックします。2. ユーザーの名前を入力します。3. パスワードまたはハッシュを入力して確認します。4. アカウントを有効にして「OK」をクリックします。5. デバイス > ユーザー グループに移動し、「追加」をクリックします。6. グループの名前を入力します。7. ユーザーをグループに追加して「OK」をクリックします。
D. 1. デバイス > 管理者 に移動し、「追加」をクリックします。2. ユーザーの名前を入力します。3. パスワードまたはハッシュを入力して確認します。4. アカウントを有効にして、「OK」をクリックします。5. デバイス > ユーザー グループ に移動し、「追加」をクリックします。6. グループの名前を入力します。7. ユーザーをグループに追加して、「OK」をクリックします。
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClHcCAK

最新問題**: 158**
最高財務責任者（CFO）は駐車場でUSBメモリを見つけ、会社のノートパソコンに接続してみることにした。そのUSBメモリにはマルウェアが仕込まれており、それがCFOのパソコンに侵入すると、既知のコマンド＆コントロール（C&C）サーバーに接続し、感染したパソコンにノートパソコンからのデータ漏洩を開始するよう指示を出した。
どのセキュリティプロファイル機能が、C&Cサーバーとの通信を阻止するために使用された可能性がありますか？
A. スパイウェア対策プロファイルを作成し、DNSシンクホールを有効にする
B. アンチウイルスプロファイルを作成し、DNSシンクホールを有効にする
C. URLフィルタリングプロファイルを作成し、DNSシンクホールカテゴリをブロックします。
D. セキュリティポリシーを作成し、DNSシンクホールを有効にする
Answer: A (メーッセージを残す**)**
参考文献：

最新問題**: 159**
最近、ファイアウォールのポリシーを最適化するために変更が加えられましたが、セキュリティチームはこれらの変更が効果を発揮してい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におけるヒットカウンターをゼロにリセットする最も迅速な方法は何ですか？
A. CLIでコマンド「reset rules」を入力し、Enterキーを押してください。
B. [ルールヒットカウンターのリセット] > [すべてのルール] オプションを使用する
C. ファイアウォールを再起動してください
D. ルールをハイライトし、各ルールに対して「ルールヒットカウンターのリセット」>「選択したルール」を使用します。
Answer: (解答を表示する**)**

最新問題**: 160**
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、どのような設定が必要ですか？
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**)**
サービス層＝第4層、アプリケーション層＝第7層

最新問題**: 161**
ポリシーオプティマイザの主な機能は何ですか？
A. 組み合わせ可能なセキュリティルールを強調表示することで、管理プレーンの負荷を軽減します。
B. 他のファイアウォールベンダーのセキュリティルールをPalo Alto Networksの設定に移行する
C. 「セッション開始時にログを記録する」セキュリティルールを削除する
D. ポートベースのセキュリティルールをアプリケーションベースのセキュリティルールに変換する
Answer: D (メーッセージを残す**)**
参考資料 :https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html

最新問題**: 162**
管理者は、NGFWトラフィックログをどの属性列でフィルタリングして、エントリがセッションの開始または終了に関するものかを判断する必要がありますか？
A. 受信時間
B. タイプ
C. 目的地
D. ソース
Answer: B (メーッセージを残す**)**
NGFWトラフィックログの「タイプ」属性列は、ログエントリがセッションの開始または終了のどちらに関するものかを示します。可能な値は、START、END、DROP、DENY、およびINVALIDです。STARTの値はログエントリがセッションの開始に関するものであることを意味し、ENDの値はログエントリがセッションの終了に関するものであることを意味します。その他の値は、さまざまな理由でファイアウォールによってセッションが終了されたことを示します12。参照 :トラフィックログフィールド、セッションログのベストプラクティス

最新問題**: 163**
スクリーンショットに基づいて、含まれているグループの目的は何ですか？

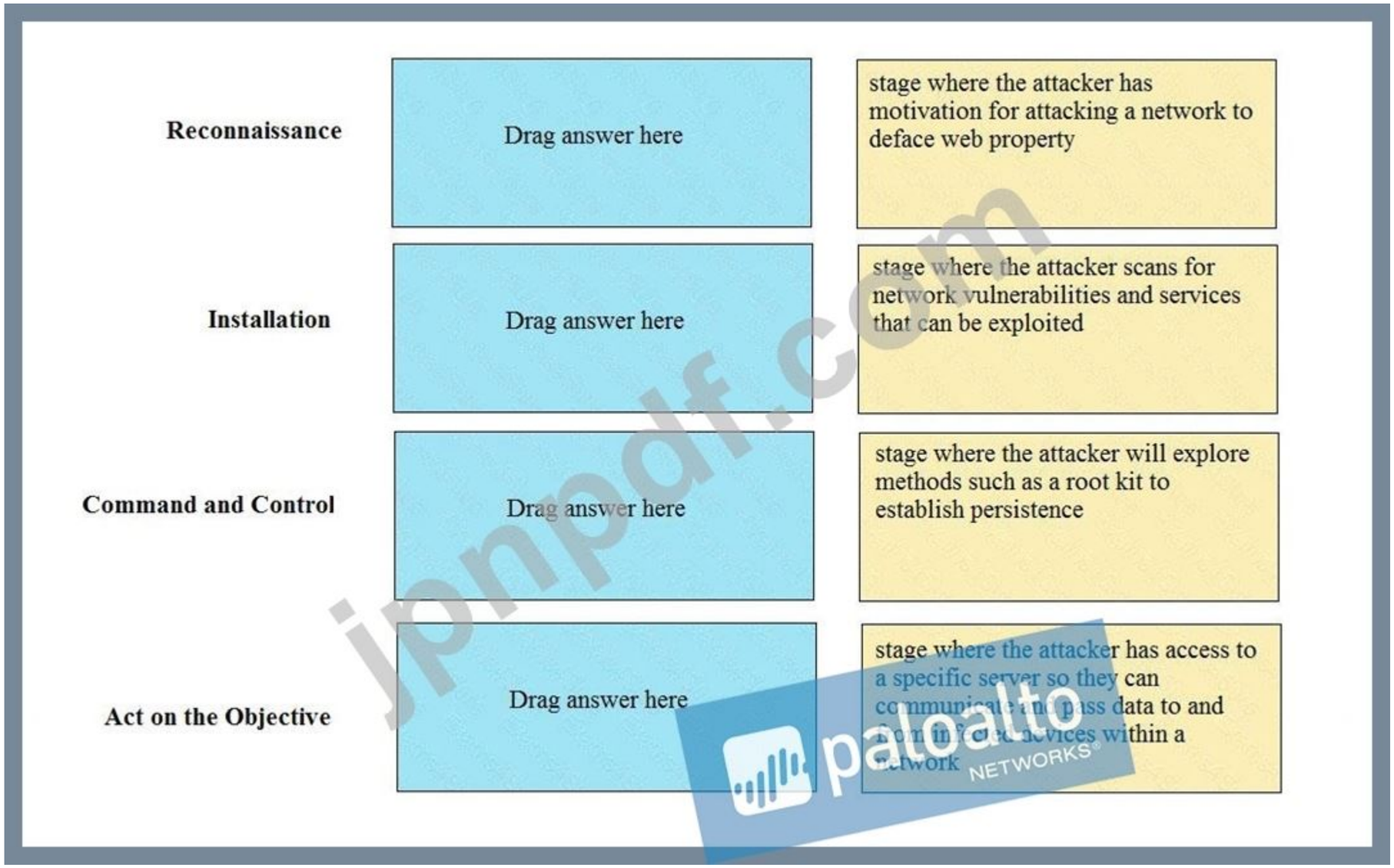

A. これらはRADIUS認証サーバーからインポートされたグループです。
B. ファイアウォールの管理を許可したユーザーのみが含まれます。
C. これらはユーザー名をグループ名にマッピングするために使用されます。
D. これらはファイアウォールの認証情報に基づいてのみ表示されるグループです。
Answer: (解答を表示する**)**

最新問題**: 164**
PAN-OS 11.0 Nova リリースでは、新しいインライン深層学習分析エンジンが検知・防止できる攻撃オプションはどれですか？（2つ選択してください。）
A. コマンドインジェクション攻撃

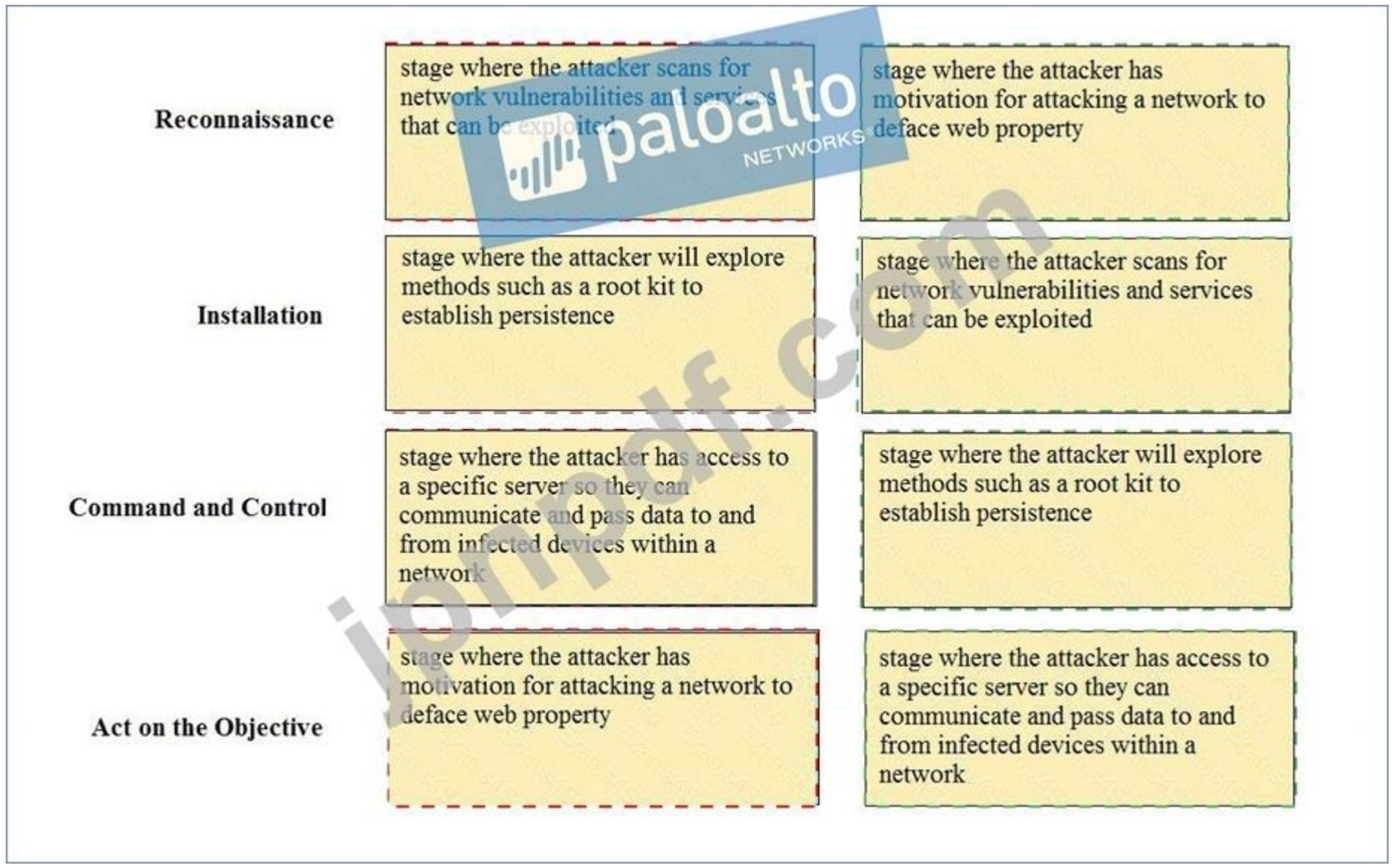
B. SSL攻撃
C. SQLインジェクション攻撃
D. HTTP攻撃
Answer: A,C (メーッセージを残す**)**
Palo Alto Networksは、Advanced Threat Preventionクラウドに新しいインライン型ディープラーニング検出エンジンを導入し、コマンドインジェクションやSQLインジェクションの脆弱性をリアルタイムでトラフィック分析することで、ゼロデイ脅威からユーザーを保護します。
(https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/content-inspection-features/vuln-protection-inline-cloud-analysis)

最新問題**: 165**
管理者は、ホストを感染させる新しいマルウェアに関するグローバル通知を受け取ります。感染したホストは、コマンド＆コントロール（C2）サーバーへの接続を試みます。ファイアウォールのシグネチャデータベースが更新された後、この脅威を検出して防止するセキュリティプロファイルコンポーネントはどれですか？（2つ選択）
（2つ選択してください。）
A. アウトバウンドセキュリティポリシーに適用される脆弱性保護プロファイル
B. 送信セキュリティポリシーに適用されるアンチスパイウェアプロファイル
C. 送信セキュリティポリシーに適用されるウイルス対策プロファイル
D. 発信セキュリティポリシーに適用されるURLフィルタリングプロファイル
Answer: (解答を表示する**)**
説明/参考資料：https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/policy/create-best-practice-security-profiles

最新問題**: 166**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。

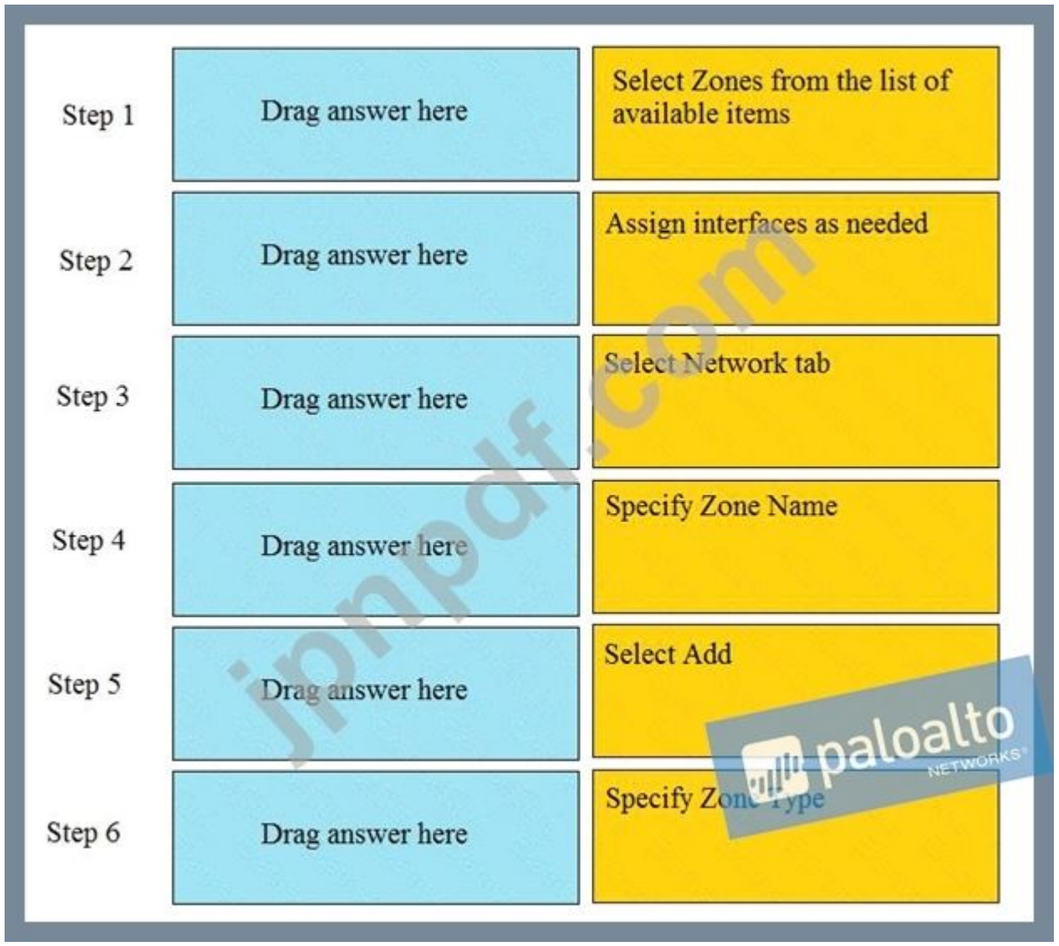

Reconnaissance
Drag answer here
stage where the attacker has motivation for attacking a network to deface web property
Installation
Drag answer here
stage where the attacker scans for network vulnerabilities and services that can be exploited
Command and Control
Drag answer here
stage where the attacker will explore methods such as a root kit to establish persistence
Act on the Objective
Drag answer here
stage where the attacker has access to a specific server so they can
data to and
within a
network

Answer:



説明
偵察 - 攻撃者がネットワークの脆弱性や悪用可能なサービスをスキャンする段階。
インストール - 攻撃者がルートキットなどの方法を試して永続性を確立する段階。コマンドとコントロール - 攻撃者が特定のサーバーにアクセスして、ネットワーク内の感染したデバイスとの間で通信やデータの送受信を行える段階。
目的実行段階 - 攻撃者がWeb資産を改ざんするためにネットワークを攻撃する動機を持つ段階

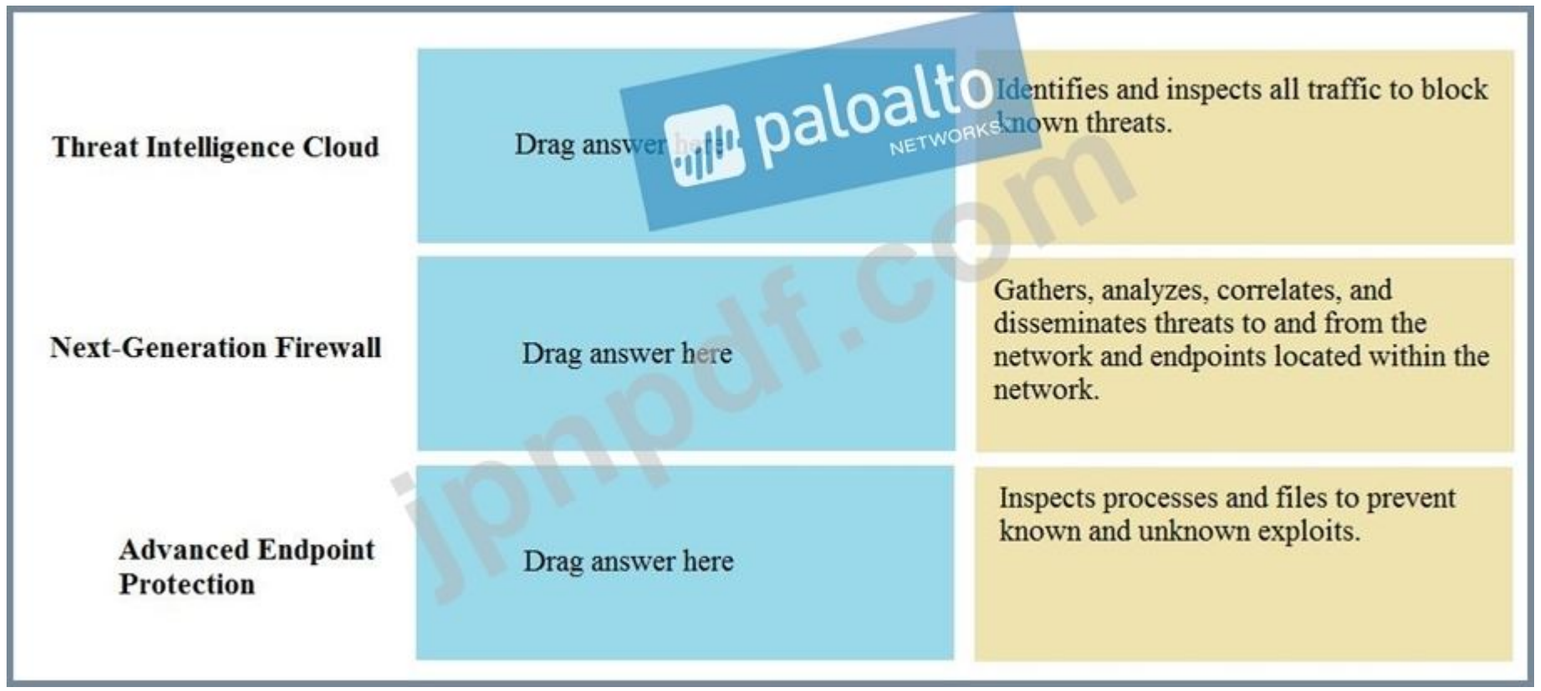
最新問題: **167**
Palo Alto Networksファイアウォールを使用して新しいセキュリティゾーンを作成するために必要な手順を順番に説明します。


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

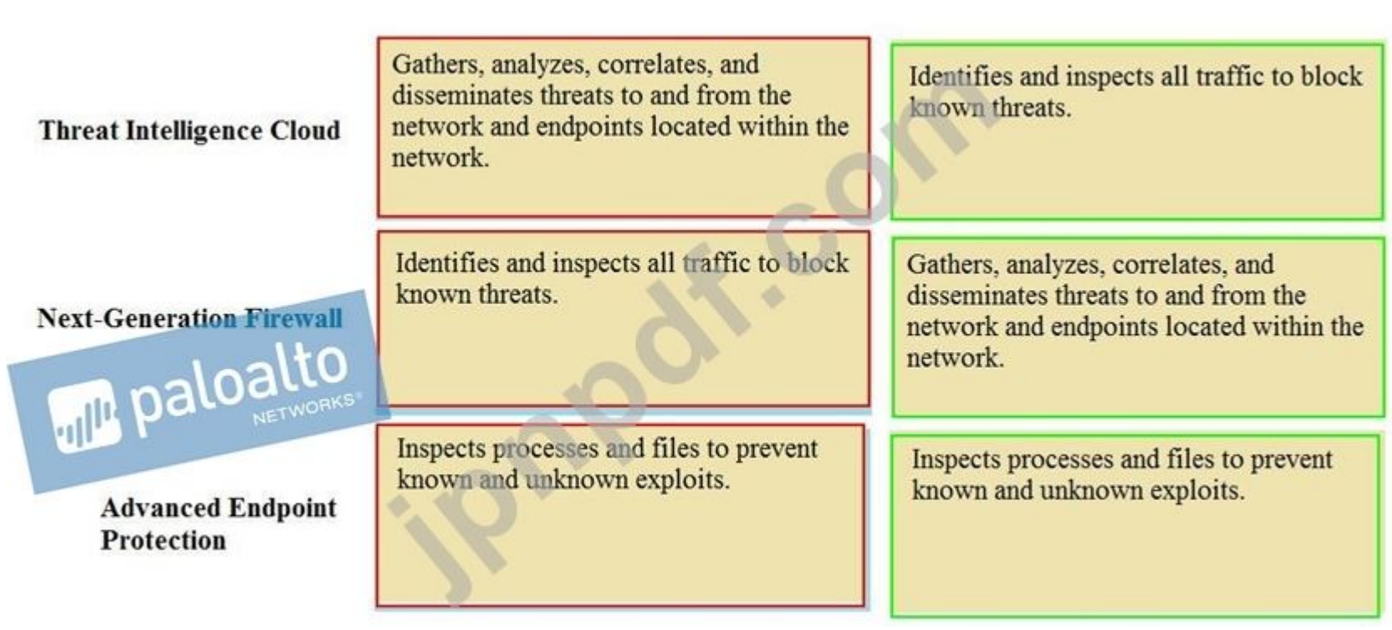
Answer:

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 - 利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
ステップ4 - ゾーン名を指定する
ステップ5 - ゾーンタイプの指定
ステップ6 - 必要に応じてインターフェースを割り当てる

最新問題: **168**
Palo Alto Networks Security Operating Platformのアーキテクチャを、その説明と一致させてください。



Answer:



最新問題: **169**

管理者プロファイル PCNSA Admin」には認証プロファイルが設定されています。

認証シーケンス PCNSA」

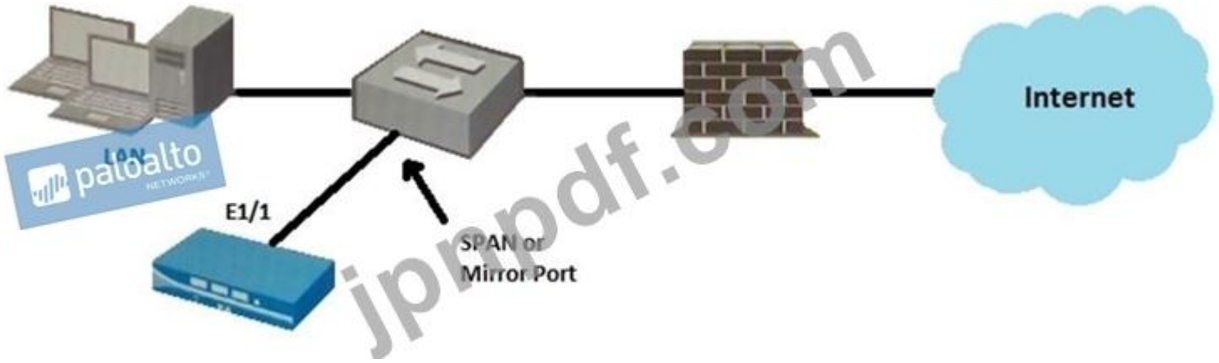
認証シーケンスPCNSAには、4つの認証プロファイルを含むプロファイルリストがあります。

認証プロファイルLDAP

認証プロファイル半径

認証プロファイルローカル
認証プロファイル TACACS
ネットワーク障害発生後、LDAPサーバーにアクセスできなくなりました。RADIUSサーバーには引き続きアクセスできますが、 PCNSA Admin」のユーザー名とパスワードが失われています。
障害発生後の PCNSA管理者」ログイン機能について説明しているのは、どのオプションですか？
A. LDAPサーバーに接続できないため、認証が失敗しました
B. 認証プロファイルがローカルのため認証OK
C. RADIUSサーバーがPCNSA管理者のユーザー名とパスワードを紛失したため、認証が失敗しました。
D. 認証プロファイルTACACSにより認証OK
Answer: B (メーッセージを残す**)**

最新問題**: 170**
トポロジーを考慮すると、インターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？



A. バーチャルワイヤー
B. タップ
C. レイヤー3
D. トンネル
Answer: (解答を表示する**)**

最新問題**: 171**
DNSシンクホーリングを有効にするために予約すべきアドレスはどれですか？ 2つ選択してください。）
A. IPv6
B. メール
C. IPv4
D. MAC
Answer: A,C (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

最新問題**: 172**
管理者は、ホストを感染させる新しいマルウェアに関するグローバル通知を受け取ります。感染したホストは、コマンド＆コントロール (C2)サーバーへの接続を試みます。ファイアウォールのシグネチャデータベースが更新された後、この脅威を検出して防止するセキュリティプロファイルコンポーネントはどれですか？ 2つ選択してください。）
A. 送信セキュリティポリシーに適用されるウイルス対策プロファイル

B. 送信セキュリティポリシーに適用されるアンチスパイウェアプロファイル
C. 発信セキュリティポリシーに適用されるURLフィルタリングプロファイル
D. アウトバウンドセキュリティポリシーに適用される脆弱性保護プロファイル
Answer: B,C (メーッセージを残す)

最新問題**: 173**
図に基づいて、サーバー監視パネルに表示される出力内容を正確に説明しているのは、次のうちどれですか？

A. User-IDエージェントは、lab-clientというラベルの付いたドメインコントローラに接続されています。
B. ホスト lab-client がユーザー ID エージェントによって検出されました。
C. ホスト lab-client がドメイン コントローラによって検出されました。
D. ユーザーIDエージェントは、lab-clientというラベルの付いたファイアウォールに接続されています。
Answer: (解答を表示する)
lab-clientはホストではなく、指定されたドメインコントローラー（Active Directory）に接続するエージェントに付ける名前です。

最新問題**: 174**
ポリシーオプティマイザの使用方法を最も適切に説明しているのは、次のうちどれですか？
A. ポリシーオプティマイザは、選択された各セキュリティポリシーに対してログ転送プロファイルを追加または変更できます。
B. ポリシーオプティマイザーは、過去90日間使用されていないセキュリティポリシーを表示できます。
C. Policy Optimizer を使用すると、スケジュールに基づいて、存在するすべてのレイヤー 4 ポリシーに対して、無効化されたレイヤー 7 App-ID セキュリティ ポリシーを自動的に作成できます。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。
D. VM-50ファイアウォールのポリシーオプティマイザは、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。

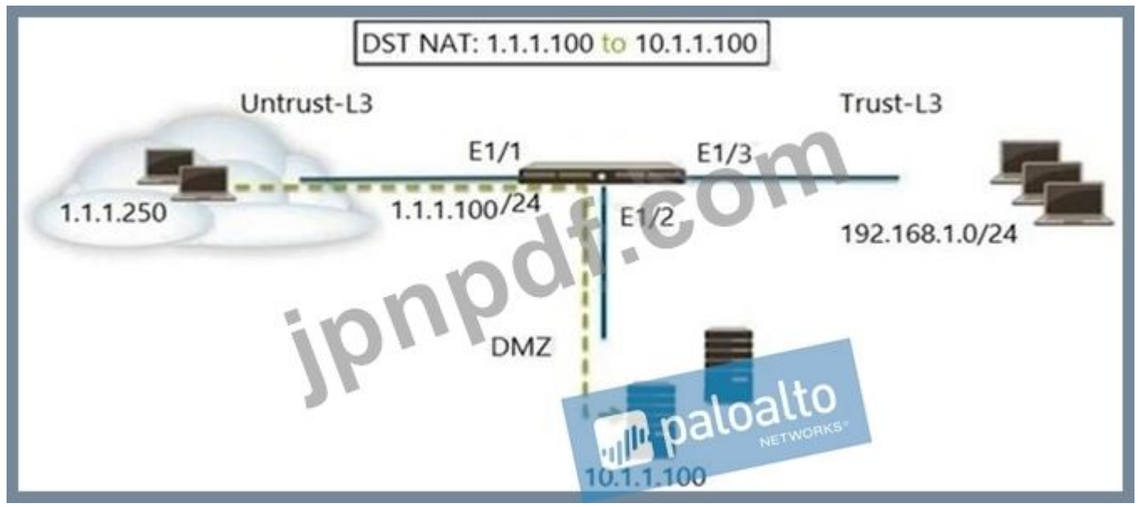
Answer: (解答を表示する)

最新問題**: 175**
管理者がスクリーンショットに表示されているセキュリティポリシールールを確認しています。

セキュリティポリシーのEDL-Denyの2つのフィールドが赤色で強調表示されているのはなぜですか？
A. 宛先ゾーン、アドレス、デバイスがすべて「任意」であるため
B. アクションが拒否であるため
C. このポリシーではウイルス対策検査が有効になっているため
D. Security-EDLタグには赤色が割り当てられているため
Answer: D (メーッセージを残す)

最新問題**: 176**
Facebookチャットを使用するために、どのApp-IDアプリケーションを許可する必要がありますか？（2つ選択してください。）
A. フェイスブック
B. Facebookチャット
C. facebook-base
D. facebook-email
Answer: B,C (メーッセージを残す)
説明／参考資料：
参考資料：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClV0CAK

最新問題**: 177**
図を参照してください。DMZ内のWebサーバーが、DNATによってパブリックアドレスにマッピングされています。



どのセキュリティポリシールールで、Webサーバーへのトラフィックが許可されますか？

A. Untrust (any) から Untrust (10.1.1.100)、Web ブラウジング - 許可

B. 信頼しない (任意) から信頼しない (1.1.1.100)、ウェブブラウジング - 許可

C. DMZ (10.1.1.100) への不信 (任意)、ウェブブラウジング - 許可

D. DMZ (1.1.1.100) への不信 (任意)、ウェブブラウジング - 許可

Answer: (解答を表示する**)**

最新問題**: 178**

システム内でログの閲覧権限を持つ管理者に対して、ログの全体像をどのように表示できますか？

A. サイドメニューから統合ログエントリを選択します。

B. ページに表示される列数を変更する

C. 各ページに表示されるログの数を変更します。

D. サイドメニューからシステムログのエントリを選択します。

Answer: (解答を表示する**)**

ログの全体像を把握するには、サイドメニューから統合ログを選択するのが最適です。統合ログは、トラフィック、脅威、URLフィルタリング、データフィルタリング、WildFireログ1など、ファイアウォールによって生成されたすべてのログを表示する単一のビューです。統合ログを使用すると、管理者は時間範囲、重要度、送信元、宛先、アプリケーション、アクション1などのさまざまな基準に基づいてログをフィルタリング、並べ替え、エクスポートできます。

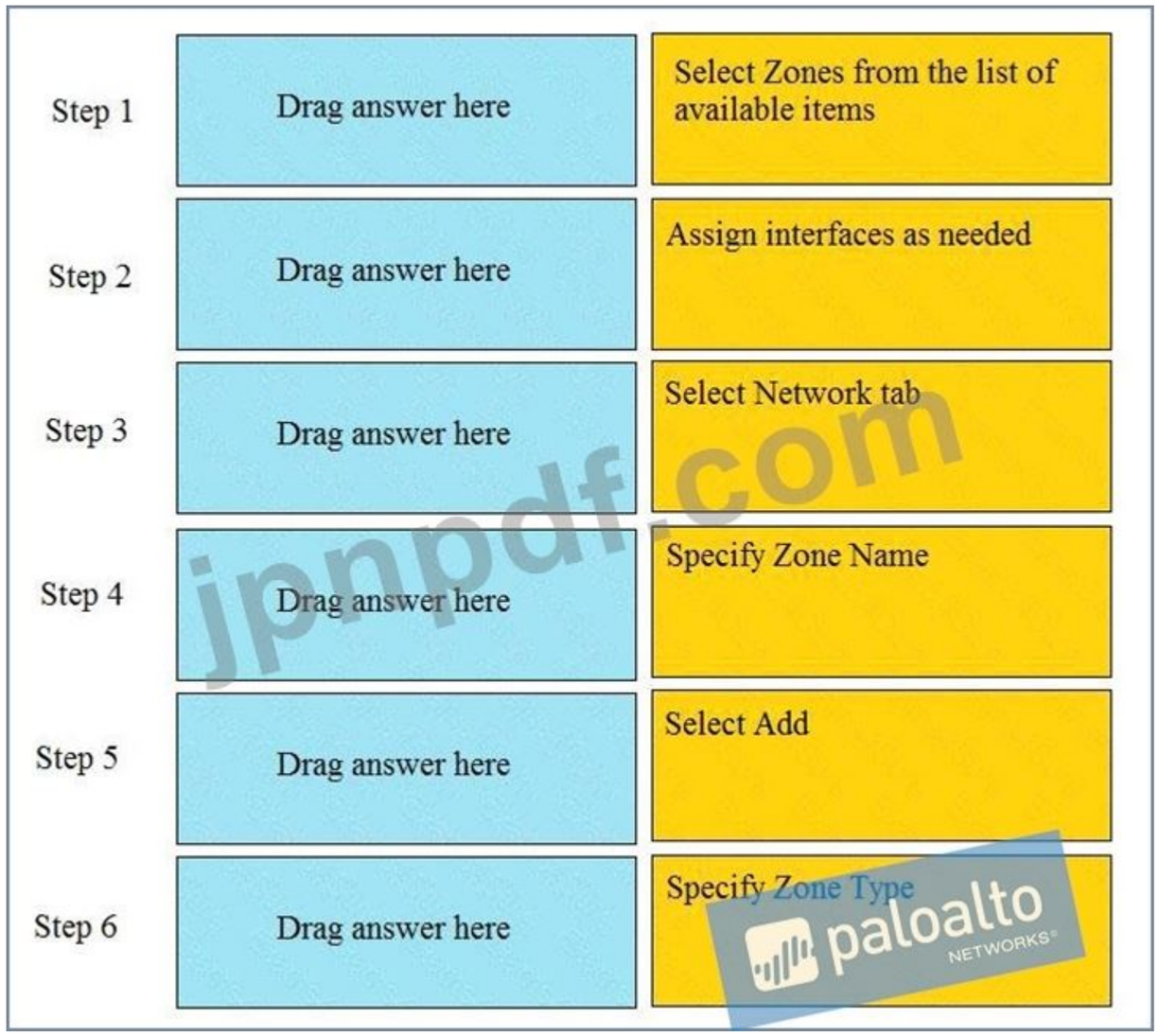
ページに表示される列数や各ページに表示されるログ数を変更しても、ログの全体像を把握できるわけではなく、現在のログビューの表示設定が変更されるだけです。サイドメニューの「システムログ」を選択しても、ファイアウォールによって生成されたすべてのログが表示されるわけではなく、構成変更、システムアラート、HAステータス2などのシステムイベントに関連するログのみが表示されます。

参考文献：

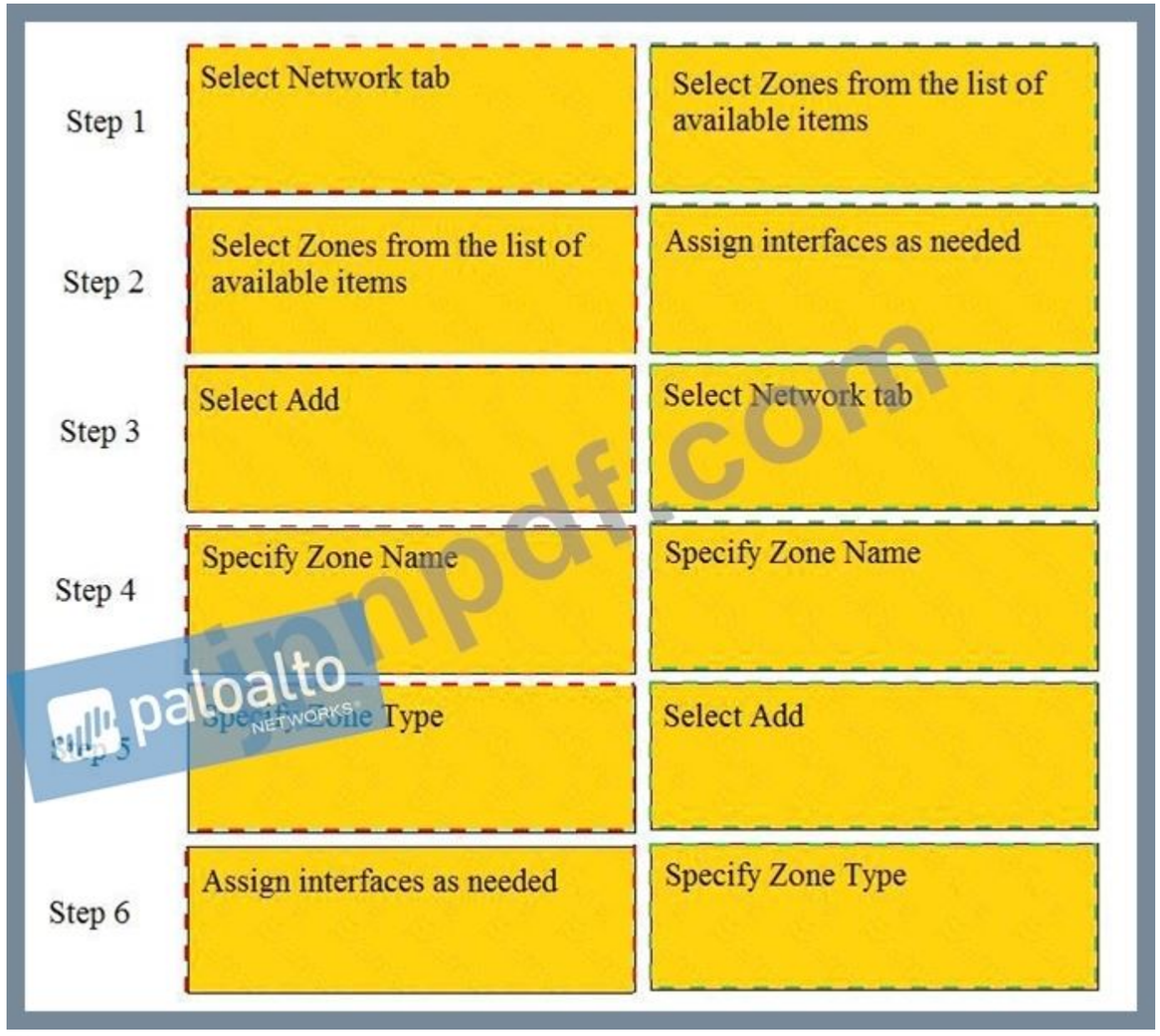
1 :ログの表示 - Palo Alto Networks 2 :ログの表示と管理 - Palo Alto Networks

最新問題**: 179**

Palo Alto Networks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順番に説明します。



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 - 利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
ステップ4 - ゾーン名を指定する
ステップ5 - ゾーンタイプの指定
ステップ6 - 必要に応じてインターフェースを割り当てる

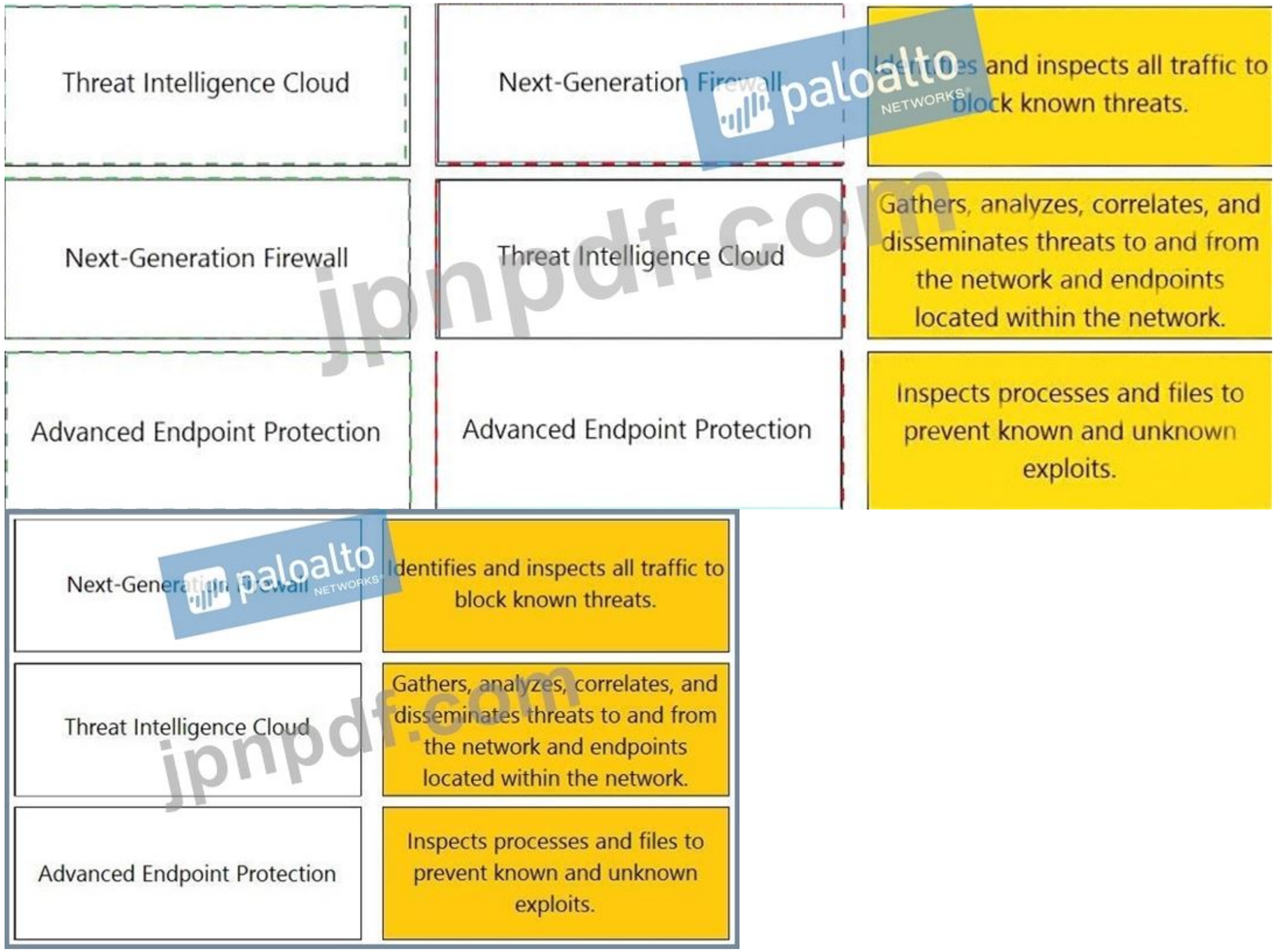
最新問題: **180**
分類ミスにより、ウェブサイトが予期せず許可されました。
この問題を適切に解決するための2つの方法は何ですか？ 2つ選択してください。）
A. https://urlfiltering paloaltonetworks.com のウェブサイトのカテゴリを確認してください。
適切な分類を指定して 「変更依頼」を送信し、確認が取れるまで待ってから再度テストを行ってください。
B. ウェブサイトに割り当てられている URL カテゴリを特定します。
有効なURLフィルタリングプロファイルを編集し、そのカテゴリのサイトアクセス設定をブロックするように更新してください。

C. URLカテゴリを作成し、影響を受けるURLを割り当てます。
元のポリシーの下に、カスタム URL カテゴリを URL カテゴリ修飾子として指定したセキュリティ ポリシーを追加します。
ポリシーアクションを 拒否」に設定します。
D. URLカテゴリを作成し、影響を受けるURLを割り当てます。
ブロックするカスタムURLカテゴリの、アクティブなURLフィルタリングプロファイルのサイトアクセス設定を更新します。
Answer: (解答を表示する**)**

最新問題**: 181**
設定オプションは4つあり、それぞれ特定のURLへのアクセスをブロックするために使用できます。すべてのオプションを同じURLへのアクセスをブロックするように設定した場合、最後にそのURLへのアクセスをブロックするオプションはどれでしょうか？
A. セキュリティポリシールールのカスタムURLカテゴリ
B. URLフィルタリングプロファイルのカスタムURLカテゴリ
C. URLフィルタリングプロファイルにおけるPAN-DB URLカテゴリ
D. URLフィルタリングプロファイルにおけるEDL
Answer: A (メーッセージを残す**)**

最新問題**: 182**
各機能をDoS攻撃対策ポリシーまたはDoS攻撃対策プロファイルに一致させてください。

Answer:



最新問題**: 183**
管理者は、デフォルト設定になっている「intrazone-default」ルールに一致するトラフィックに関する問題のトラブルシューティングを行っています。
管理者は何をすべきでしょうか？
A. ルールのログ記録アクションを変更する
B. システムログを確認する
C. トラフィックログフィルターを調整して日付を含めるようにします

D. トラフィックログを更新する
Answer: A (メーッセージを残す**)**

最新問題**: 184**
管理者が宛先ゾーンを変更できるルールタイプはどれですか？ 2つ選択してください。）
A. インターゾーン
B. 影付き
C. イントラゾーン
D. ユニバーサル
Answer: A,D (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClomCAC

最新問題**: 185**
提示されたスクリーンショットに基づくと、どの列に、クリックするとポリシー規則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ていますか？

A. 見たアプリ
B. サービス
C. 名前
D. 許可されたアプリ
Answer: A (メーッセージを残す**)**

最新問題**: 186**
Panoramaで管理されているデバイスについて、正しい記述はどれですか？
A. Panorama は、Panorama からのコミット後にローカル構成ロックを自動的に削除します。
B. ローカル構成ロックにより、Panorama管理対象デバイスのセキュリティポリシーの変更が禁止されます。
C. ローカルファイアウォールで設定されたセキュリティポリシールールが常に優先されます
D. ローカル設定ロックはPanoramaから手動で解除できます
Answer: C (メーッセージを残す**)**
説明
参照：
<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/administer-panorama/manage-locks-forrestricting-configuration-changes.html>

最新問題: 187

ユーザーがURL管理者パスワードを入力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すればよいでしょうか？

A. オーバーライド

B. 認証

C. 認証

D. 続ける

Answer: B (メーッセージを残す**)**

説明／参考資料：

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**: 188**
ポリシーオプティマイザーのポリシービューは、セキュリティポリシーの動作とどのような点で異なりますか？
A. セキュリティプロファイルの設定が不足しているルールを表示します。
B. これは、ポートベースとして構成されていないApp-IDを持つルールを示します。
C. ソースゾーンと宛先ゾーンが同じルールを表示します。
D. より具体的なルールよりも、基準に一致するより広範なルールが設定されていることを示します。
Answer: (解答を表示する**)**
Policy Optimizer のポリシー ビューは、セキュリティ ポリシー ビューとはいくつかの点で異なります。その 1 つは、ポート ベースとして構成されていない App-ID を持つルールを示すことです。これらは、特定のアプリケーションまたはアプリケーション グループではなく、 &any」に設定されているアプリケーションを持つルールです。これらのルールは過度に寛容であり、指定されたポート上のすべてのアプリケーション トラフィックを許可するため、セキュリティ ギャップが生じる可能性があります。Policy Optimizer は、これらのルールを最小権限アクセスの原則 12 に従うアプリケーション ベースのルールに変換するのに役立ちます。Policy Optimizer を使用して、ポート ベースのルールを検出してアプリケーション ベースのルールに変換したり、使用されていないアプリケーションを削除したり、使用されていないルールを削除したり、ポリシー基準に一致する新しいアプリケーションを検出したりできます 3。参照:
ポリシーオプティマイザのベストプラクティス - パロアルトネットワークス
管理: ポリシーオプティマイザー - パロアルトネットワークス | テクニカルドキュメント
セキュリティポリシーオプティマイザーを使用する理由と、そのメリットは何ですか？

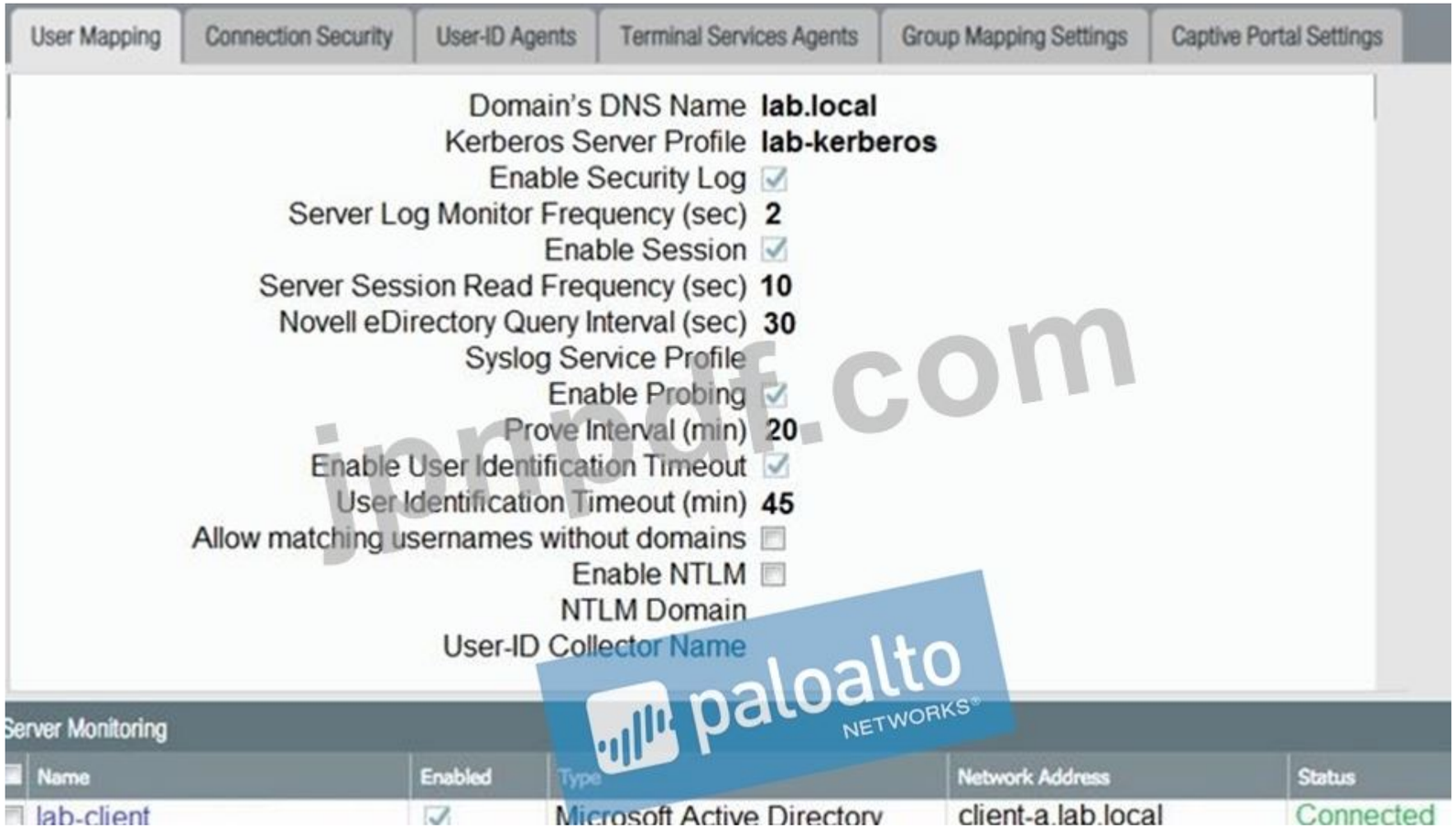
最新問題**: 189**
管理者は、アクティブな構成と、コミットされた場合に変更される可能性のある内容との違いを確認するために、どの2つの構成を比較する必要がありますか？ 2つ選択してください。）
A. 候補者
B. アクティブ
C. デバイスの状態
D. ランニング
Answer: A,D (メーッセージを残す**)**

最新問題**: 190**

WildFire分析プロファイル内で、分析のためにサンプルを転送するためのマッチング基準として、どのような条件を定義できますか？
A. アプリケーションカテゴリ
B. ソース
C. ファイルサイズ
D. 方向
Answer: (解答を表示する**)**
WildFire分析プロファイルを使用すると、アプリケーション、ファイルの種類、トラフィックの送信方向（アップロードまたはダウンロード）に基づいて、WildFire分析のために転送するファイルまたは電子メールリンクを指定できます。方向一致基準は、ファイルまたは電子メールリンクが送信元ゾーンから宛先ゾーンに送信されたか（アップロード）、宛先ゾーンから送信元ゾーンに送信されたか（ダウンロード）を決定します。トラフィックの方向に関係なくファイルまたは電子メールリンクを転送するために、両方の方向を選択することもできます。参照 :セキュリティプロファイル：WildFire分析、オブジェクト > セキュリティプロファイル > WildFire分析

最新問題**: 191**
デバイスグループの階層構造において、共有レベルの下にいくつのレベルが存在する可能性がありますか？
A. 2
B. 3
C. 4
D. 5
Answer: (解答を表示する**)**
デバイスグループ階層を作成すると、デバイスグループを最大4レベルのツリー階層にネストできます。下位レベルのグループは、上位レベルのグループの設定（ポリシー規則とオブジェクト）を継承します。
https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy

最新問題**: 192**
図に基づいて、サーバー監視パネルに表示される出力内容を正確に説明しているのはどの記述ですか？



A. ホスト lab-client がドメイン コントローラによって検出されました。
B. ユーザーIDエージェントは、lab-clientというラベルの付いたファイアウォールに接続されています。
C. ホスト lab-client がユーザー ID エージェントによって検出されました。
D. User-IDエージェントは、lab-clientというラベルの付いたドメインコントローラに接続されています。
Answer: (解答を表示する**)**

最新問題**: 193**
最高財務責任者 (CFO)が駐車場でマルウェアに感染したUSBドライブを発見し、それを会社のノートパソコンに挿入したところ、マルウェアが感染し、既知のコマンド&コントロールサーバーに接続して企業データを不正に持ち出した。
どのセキュリティプロファイル機能を使用して、コマンド&コントロールサーバーとの通信を阻止できた可能性がありますか？
A. データフィルタリングプロファイルを作成し、そのDNSシンクホール機能を有効にします。
B. URLフィルタリングプロファイルを作成し、DNSシンクホールURLカテゴリをブロックします。
C. アンチスパイウェアプロファイルを作成し、DNSシンクホール機能を有効にします。
D. ウイルス対策プロファイルを作成し、DNSシンクホール機能を有効にします。
Answer: (解答を表示する**)**

最新問題**: 194**
どの管理サービスが管理インターフェースにアクセスするように構成できますか？

A. HTTP、CLI、SNMP、HTTPS
B. HTTPS、SSH、Telnet、SNMP
C. SSH: telnet HTTP、HTTPS
D. HTTPS、HTTP、CLI、API
Answer: D (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/management-interfaces Palo Alto Networks ファイアウォールを管理するには、以下のユーザー インターフェイスを使用できます。
ウェブインターフェースを使用すると、設定や監視作業を比較的簡単に実行できます。このグラフィカルインターフェースでは、HTTPS（推奨またはHTTPを使用してファイアウォールにアクセスでき、管理作業を行うのに最適な方法です。
コマンドラインインターフェイス （CLI）を使用すると、SSH（推奨）Telnet、またはコンソールポート経由でコマンドを連続して入力することで、一連のタスクを実行できます。CLIはシンプルなインターフェイスで、操作モードと設定モードの2つのコマンドモードをサポートしており、それぞれに明確なコマンドとステートメントの階層構造があります。コマンドのネスト構造と構文に慣れると、CLIは迅速な応答時間と管理効率を提供します。
XML API を利用することで、業務を効率化し、既存の社内開発アプリケーションやリポジトリとの統合を実現できます。XML API は、HTTP/HTTPS リクエストとレスポンスを使用して実装された Web サービスです。
Panoramaを使用すると、複数のファイアウォールに対してWebベースの管理、レポート作成、およびログ収集を実行できます。
PanoramaのWebインターフェースはファイアウォールのWebインターフェースに似ていますが、集中管理のための追加機能が備わっています。

最新問題**: 195**
提示されたセキュリティポリシー規則に基づくと、SSHはどのポートで許可されますか？

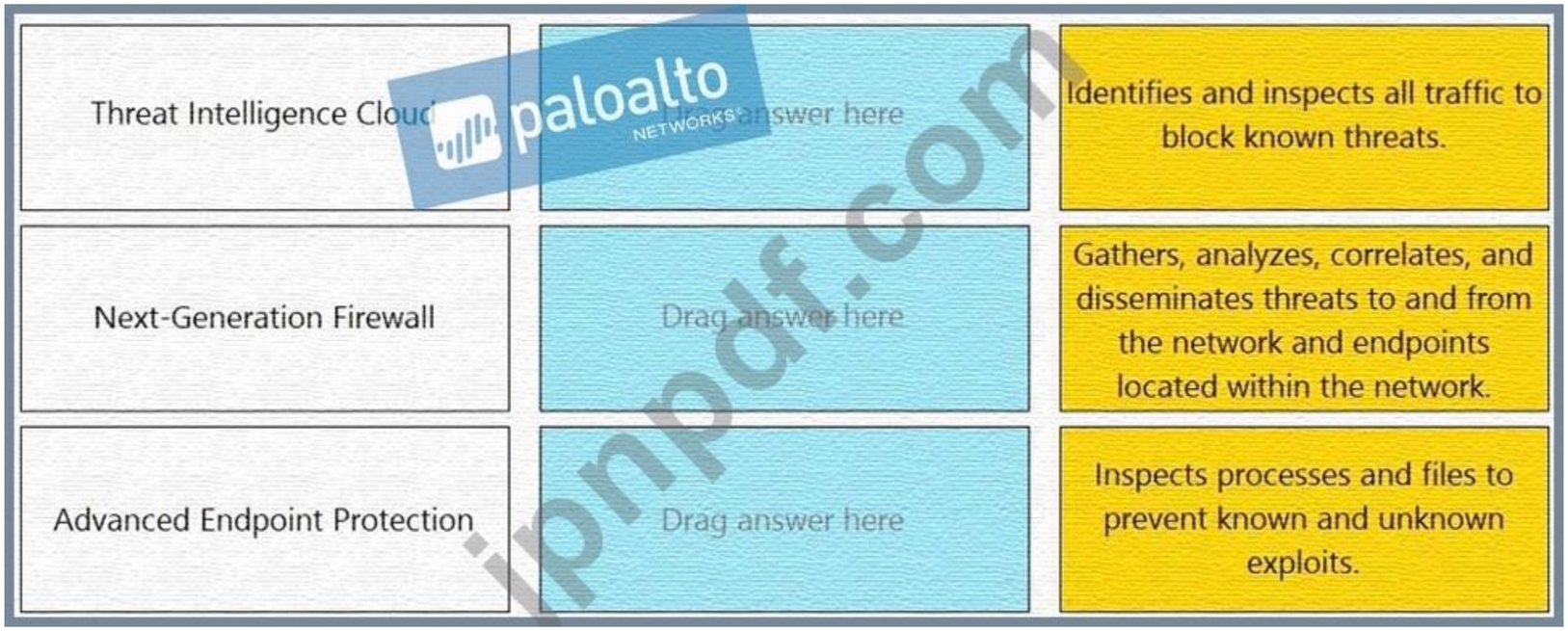
			Source		Destination						
	Name	**Type**	**Zone**	**Address**	**Zone**	**Address**	**Application**	**Service**	**URL Category**	**Action**	**Profile**
1	Deny Google	Universal	Inside	Any	Outside	Any	Google-docs-base	Application-d	Any	Deny	None
2	Allowed-security serv...	Universal	Inside	Any	Outside	Any	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. 22
B. 53
C. 80
D. 23
Answer: (解答を表示する)

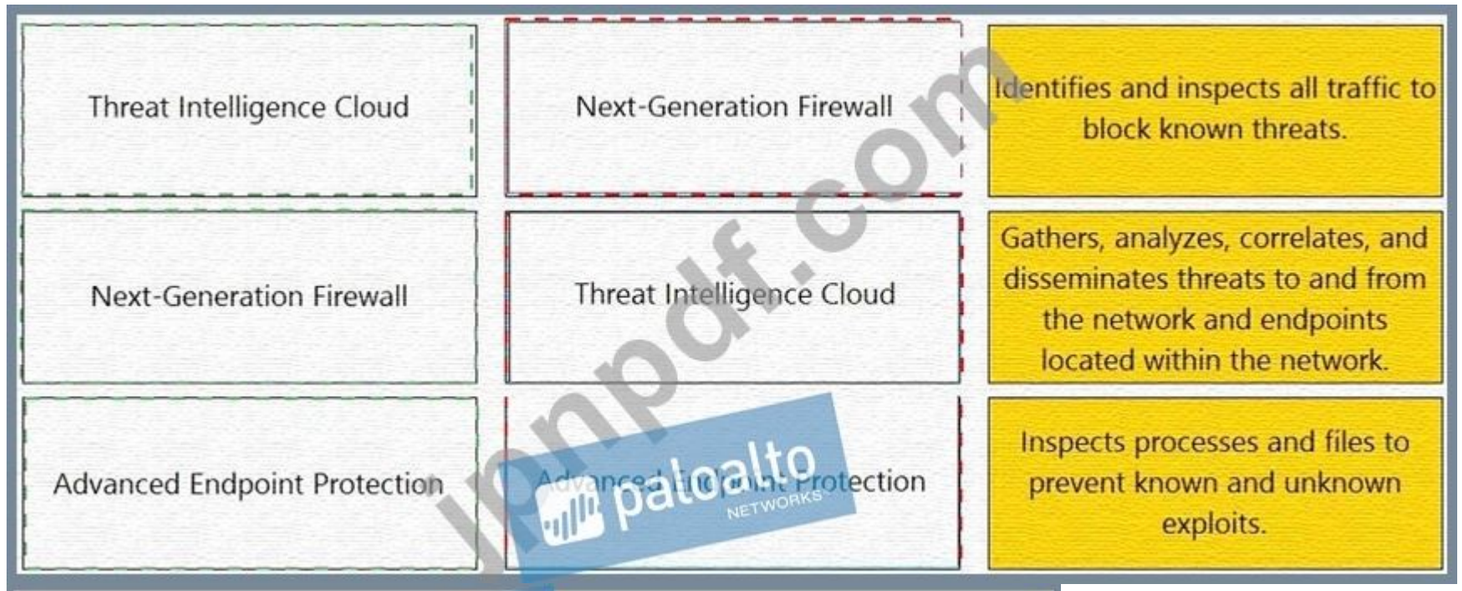
最新問題**: 196**
管理者は、既知のマルウェアドメインをすべてブロックまたはシンクホールするために、リアルタイムのシグネチャ検索を実行する機能を追加する必要があります。
この結果を得るには、どのタイプの単一統合エンジンを使用すればよいでしょうか？
A. ユーザーID
B. アプリID

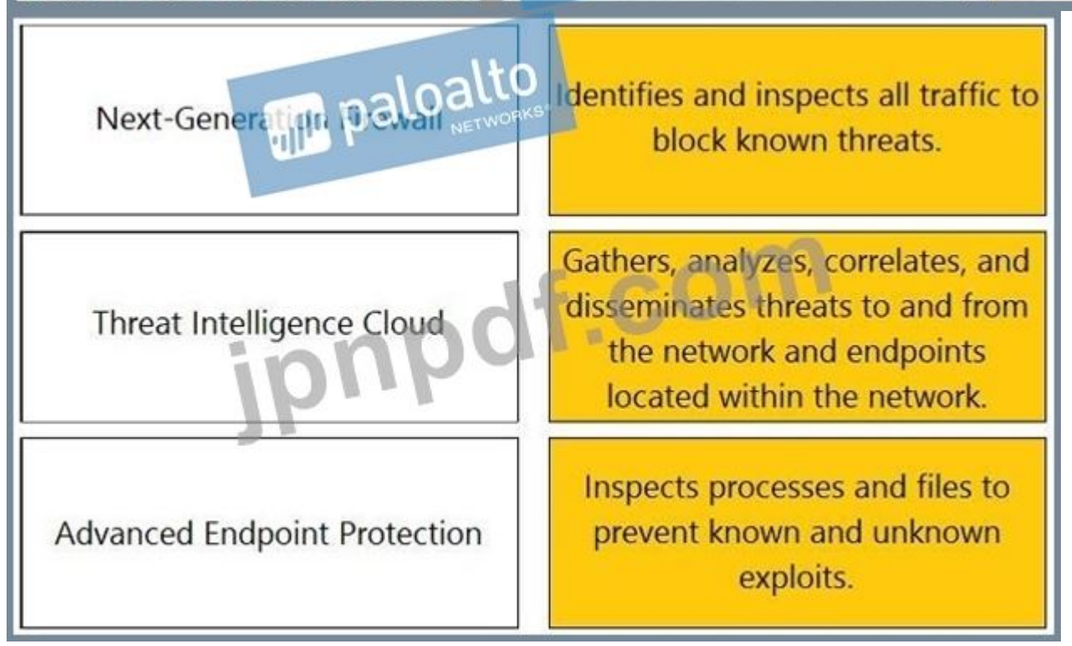
C. セキュリティ処理エンジン
D. コンテンツID
Answer: D (メーッセージを残す**)**
Content-ID™は、リアルタイムの脅威防御エンジンと包括的なURLデータベース、およびアプリケーション識別要素を組み合わせることで、不正なデータやファイルの転送を制限し、広範囲にわたるエクスプロイト、マルウェア、危険なウェブ閲覧、標的型攻撃、未知の脅威を検出してブロックします。
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/techbrief-content-id.pdf

最新問題: **197**
各機能をDoS攻撃対策ポリシーまたはDoS攻撃対策プロファイルに一致させてください。



Answer:





最新問題: **198**
ファイアウォールを通過するトラフィックをログに記録するためのベストプラクティスは何ですか？
A. セッション開始時とセッション終了時の両方のログ記録を有効にします。
B. セッション開始時のみログを有効にする。
C. セッション終了時のみログを有効にする。
D. すべてのログ記録オプションを無効にします。
Answer: C (メーッセージを残す**)**
ファイアウォールを通過するトラフィックをログに記録するためのベストプラクティスは、セッション終了時のみログを有効にすることです。

このオプションを使用すると、ファイアウォールはセッション終了時にのみログエントリを生成するため、ファイアウォールとログストレージへの負荷が軽減されます。ログエントリには、送信元および宛先IPアドレス、ポート、ゾーン、アプリケーション、ユーザー、バイト数、パケット数、セッションの継続時間などの情報が含まれます。セッション終了時のログオプションでは、最終的なアプリケーションとユーザー、合計バイト数とパケット数、セッション終了理由1など、セッションに関するより正確な情報も提供されます。セッション終了時のみのログを有効にするには、次の手順を実行する必要があります。
ログに記録したいトラフィックに一致するセキュリティポリシールールを作成または変更します。
ポリシールールの「アクション」タブを選択し、「セッション終了時にログを記録する」オプションをオンにします。
変更内容をファイアウォールまたはPanoramaと管理対象ファイアウォールにコミットします。
参考資料: ログの表示と管理、セッション終了時のログ、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**: 199**
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. 脅威防止ライセンス
B. 脅威実装ライセンス
C. 脅威保護ライセンス
D. 脅威環境ライセンス
Answer: A (メーッセージを残す**)**

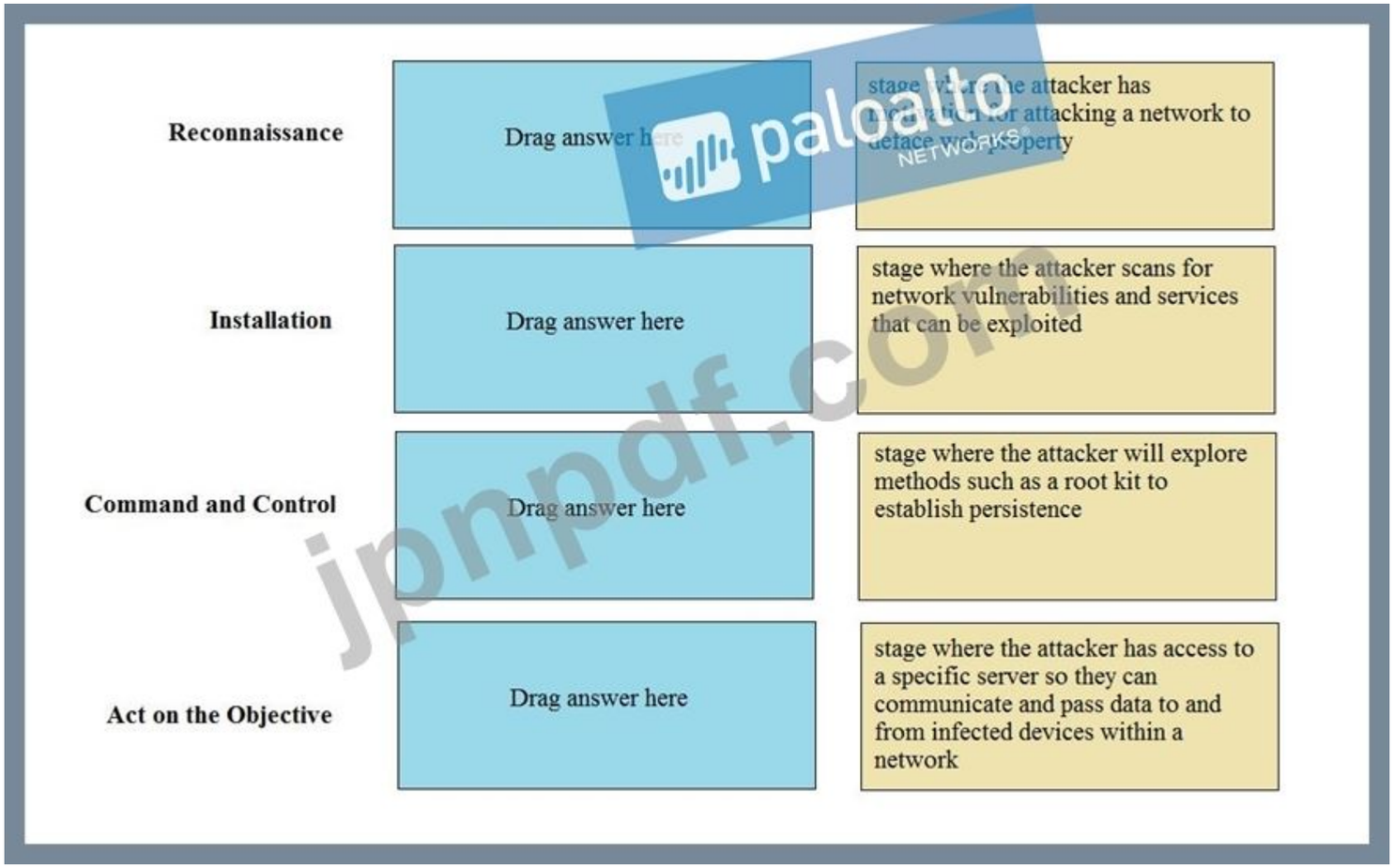
最新問題**: 200**
セキュリティポリシールールの構成要素となるコンポーネントはどれですか？
A. 復号プロファイル
B. 宛先インターフェース
C. タイムアウト（分）
D. アプリケーション
Answer: D (メーッセージを残す**)**
説明／参考資料：
参照：
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html

最新問題**: 201**
App-IDの更新プロセス中に、既存のポリシールールがApp-IDの更新によって影響を受けるかどうかを確認するには、どこをクリックすればよいですか？
A. ダウンロード
B. レビューポリシー
C. テストポリシーの一致
D. 今すぐチェック
Answer: (解答を表示する**)**

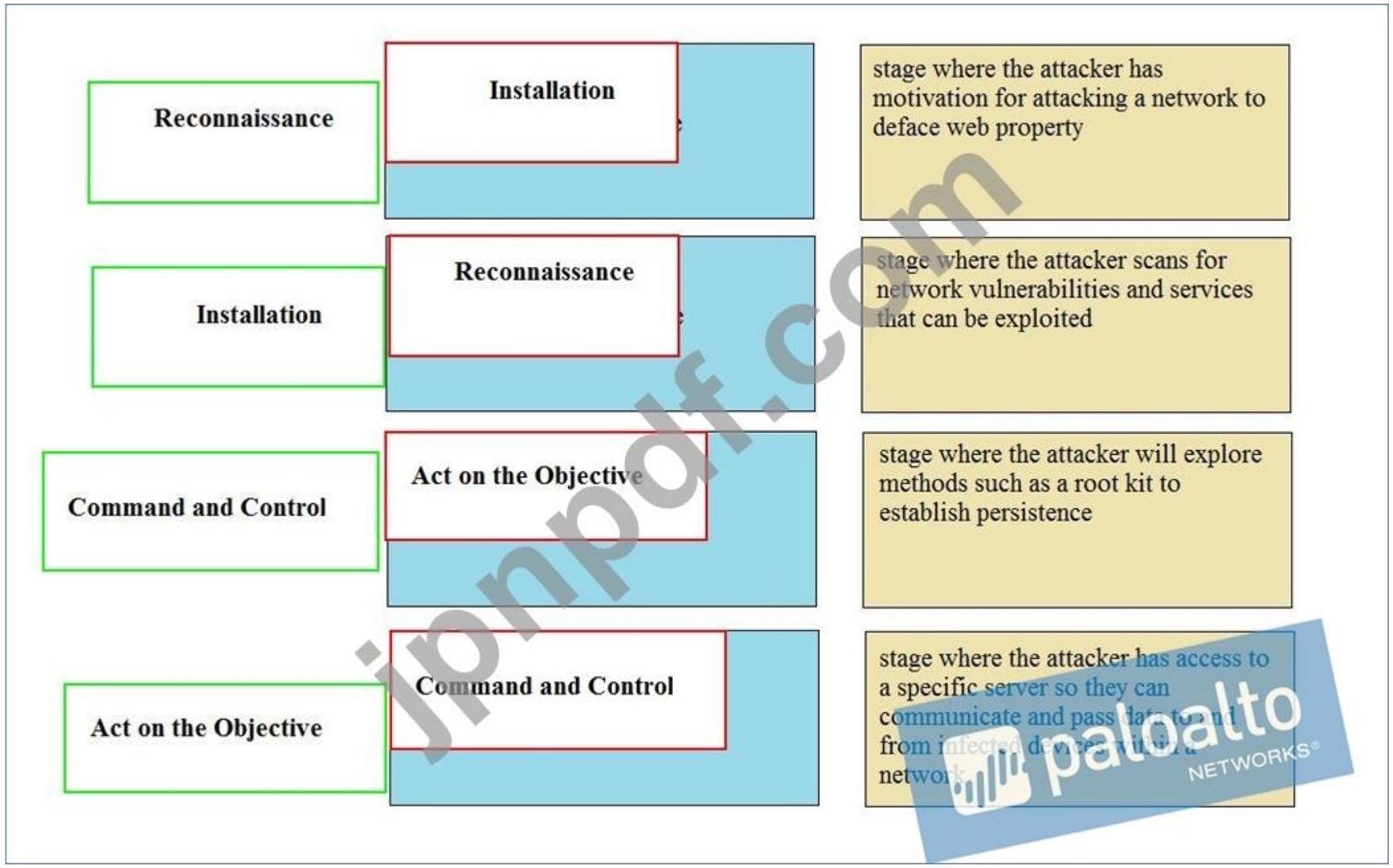
最新問題**: 202**
IPワイルドカードマスク型のアドレスオブジェクトは、設定のどの部分で参照できますか？
A. セキュリティポリシールール

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: (解答を表示する**)**
IPワイルドカードマスク型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
--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）が続く形式でIPワイルドカードアドレスを入力してください。例：
10.182.1.1/0.127.248.0。ワイルドカードマスクでは、ゼロ ０）ビットは、比較対象のビットが、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。マスクの1 １）ビットはワイルドカードビットであり、比較対象のビットが、1でカバーされるIPアドレスのビットと一致する必要はありません。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。一致の例として、バイナリスニペット0011では、ワイルドカードマスク1010によって4つの一致 ０001、0011、1001、および1011）が得られます。

最新問題**: 203**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。



Answer:



最新問題: **204**

示されているセキュリティポリシーの例では、どの2つのウェブサイトがブロックされますか？ 2つ選択してください。）

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

最新問題: **205**
FTPで転送された悪意のあるファイルを介してホストに感染する、新たなマルウェアに関する通知を受け取ります。
ファイアウォールの脅威シグネチャデータベースを更新した後、どのセキュリティプロファイルがこの脅威を検知し、内部ネットワークを保護しますか？
A. URLフィルタリングプロファイルが受信セキュリティポリシールールに適用されます。
B. 送信セキュリティポリシールールに適用されるデータフィルタリングプロファイル。
C. 受信セキュリティポリシールールにアンチウイルスプロファイルが適用されます。
D. 脆弱性対策
Answer: C (メーッセージを残す**)**
送信セキュリティポリシールールに適用されるアクションプロファイル。
参照：
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

最新問題: **206**
ユーザー名を動的ユーザーグループに含めるためにタグ付けするには、どの2つの機能を利用できますか？ 2つ選択してください）
A. XML API
B. ログ転送の自動タグ付け
C. GlobalProtectエージェント
D. ユーザーID Windowsベースエージェント
Answer: A,D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

最新問題: **207**
ゼロトラストファイアウォール環境では保護されるが、境界防御のみのファイアウォール環境では保護されないデータフローの方向はどれですか？
A. アウトバウンド
B. 受信
C. 東西
D. 北南
Answer: (解答を表示する**)**

最新問題: **208**
貴社は単一の建物内の1フロアを占有しています。単一のネットワーク上に2台のActive Directoryドメインコントローラーがあります。ファイアウォールの管理プレーンはほとんど利用されていません。
お使いのネットワークでは、どのUser-IDエージェントで十分ですか？
A. 各ドメインコントローラーにWindowsベースのエージェントが展開されます。
B. ファイアウォールにPAN-OS統合エージェントをデプロイする
C. ネットワーク上にCitrixターミナルサーバーエージェントが展開されています
D. ドメインメンバーの内部ネットワークに展開されたWindowsベースのエージェント
Answer: A (メーッセージを残す**)**

説明/参考資料: https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/map-ip-addresses-to-users/ configure-user-mapping-using-the-windows-user-id-agent/configure-the-windows-based-user-id-agent-for-user-mapping.html

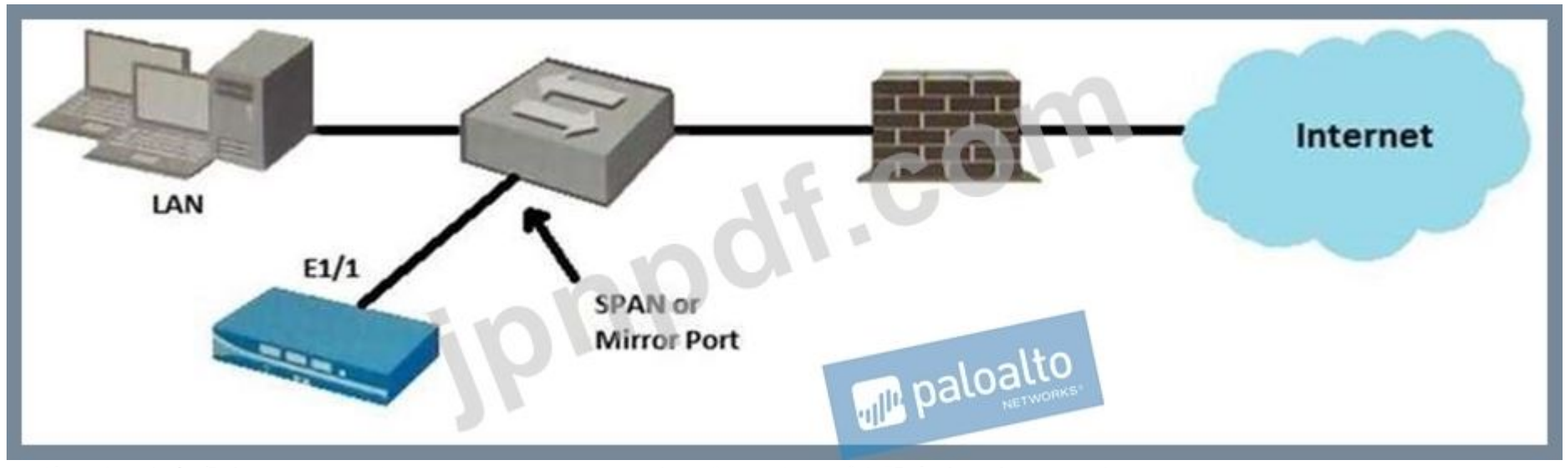
最新問題: **209**

提示されたセキュリティポリシー規則に基づくと、SSHはどのポートで許可されますか？

			Source		Destination						
	Name	Type	Zone	Address	Zone	Address	User	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. 一時的な港のみ
B. 任意のポート
C. デフォルトポート
D. SSLおよびSNMPv3と同じポート
Answer: C (メーッセージを残す)

最新問題: **210**



トポロジーを考慮すると、インターフェースE1/1にはどのゾーンタイプを設定すべきでしょうか？
A. トンネル
B. レイヤー3
C. タップ
D. バーチャルワイヤー
Answer: C (メーッセージを残す)

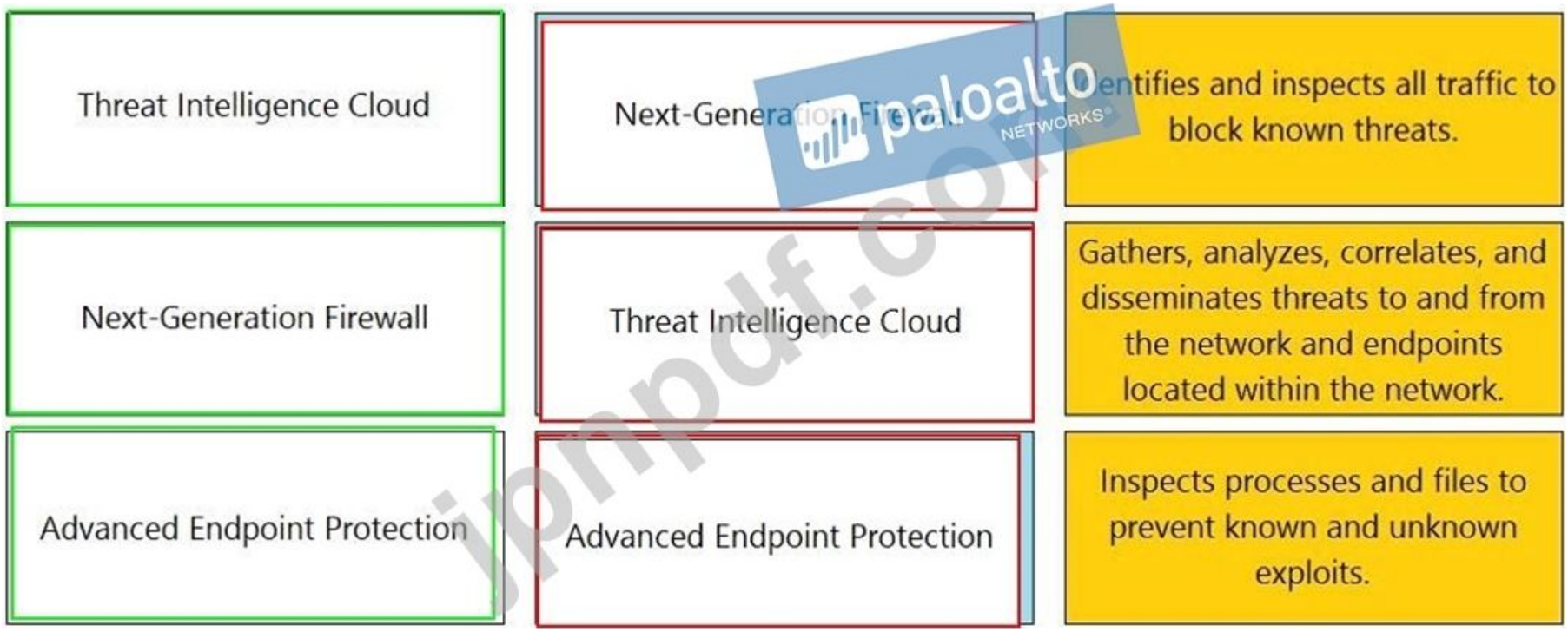
最新問題: **211**

管理者は、特定のアプリケーションに対するデフォルトの拒否アクションを上書きし、代わりにトラフィックをブロックしてICMPコードを送信したいと考えています。

目的地との通信は行政上禁止されています。」
どのセキュリティポリシーアクションがこれを引き起こしているのでしょうか？
A. ドロップ
B. ICMP到達不能を破棄して送信
C. 両方をリセット
D. サーバーをリセット
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-policy/security-policy-actions.html

最新問題: **212**
各機能をDoS攻撃対策ポリシーまたはDoS攻撃対策プロファイルに一致させてください。

Answer:



最新問題: **213**

ユーザーは、URLフィルタリングのセキュリティプロファイル内のどこで、認証情報の送信を防止するアクションを設定する必要がありますか？

A. URLフィルタリング > カテゴリ

B. URLフィルタリング > URLフィルタリング設定

C. URLフィルタリング > インラインカテゴリ分類

D. URLフィルタリング > HTTPヘッダー挿入

Answer: A (メーッセージを残す**)**

https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention/set-up-credential-phishing-prevention#idfd42ebad-d0fc-415a-aadc-e222fc2beb80

最新問題: **214**

上記の詳細なログ情報を踏まえて、ファイアウォールのトラフィック検査の結果はどうでしたか？

A. 脆弱性保護プロファイルのアクションによってブロックされました。
B. アンチスパイウェアプロファイルアクションによってブロックされました。
C. セキュリティポリシーのアクションによりブロックされました。
D. ウイルス対策セキュリティプロファイルのアクションによってブロックされました。
Answer: B (メーッセージを残す**)**

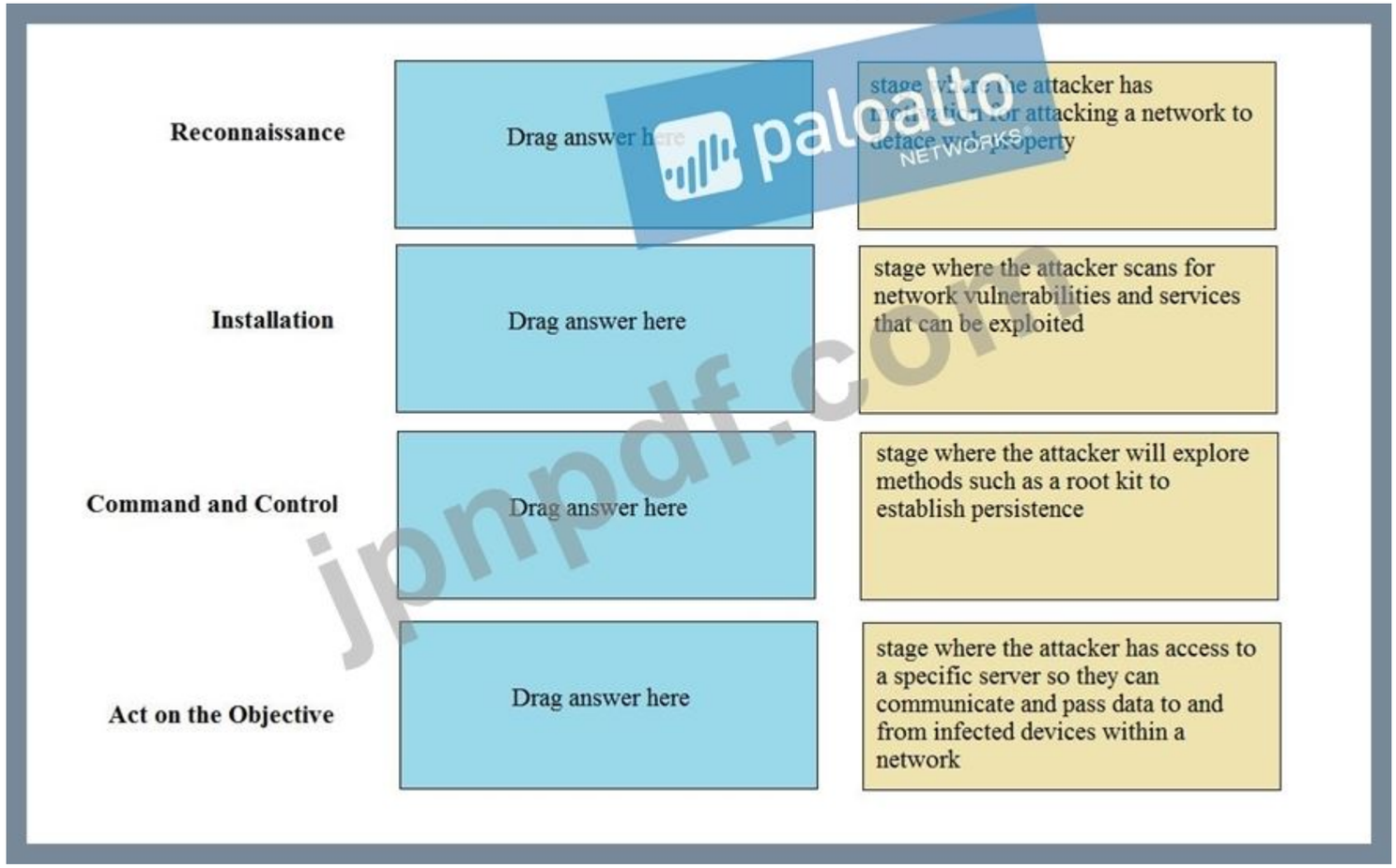
最新問題**: 215**
管理者が、外部の動的リストに例外処理を適用するため、手動でエントリを追加しています。管理者は変更を保存しようとしていますが、「OK」ボタンがグレー表示になっていて選択できません。「OK」ボタンがグレー表示される理由として考えられるものを2つ挙げてください。（2つ選択してください。）
A. エントリが重複しています。
B. エントリがリストのエントリと一致します。
C. 入力されたエントリはリストのエントリと一致しません。
D. このエントリにはワイルドカードが含まれています。
Answer: A,C (メーッセージを残す**)**

最新問題**: 216**
ポリシーオプティマイザのポリシービューは、セキュリティポリシービューとどのように異なりますか？
A. ルールの順序に影響を与えない並べ替えオプションを提供します。
B. ルールの利用状況を表示します。
C. 関連するゾーンの詳細を示します。
D. ルールによって認識されるアプリケーションを指定します。
Answer: A (メーッセージを残す**)**

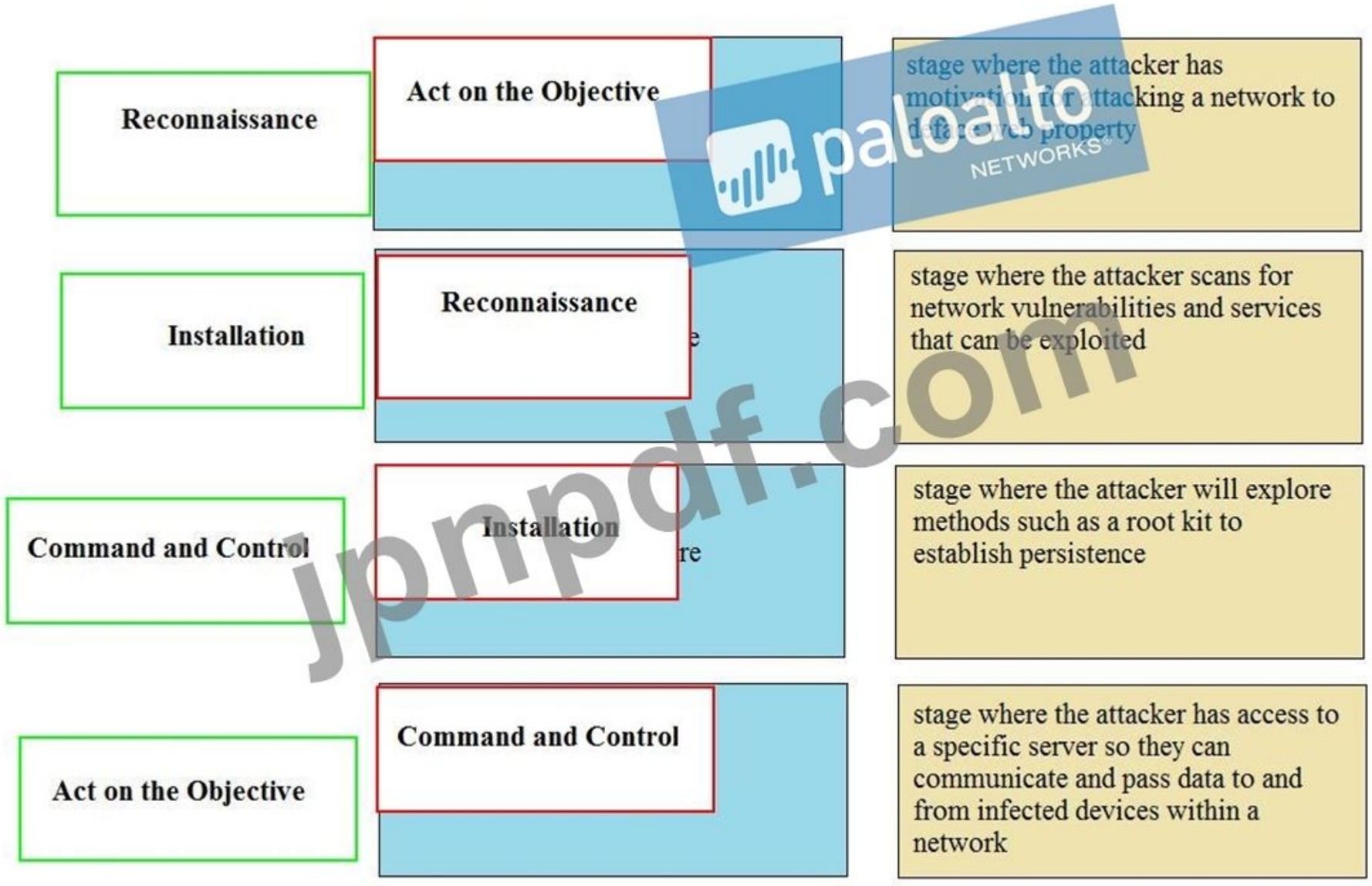
PoliciesSecurity では、ルールのフィルタリングや並べ替えを行うことはできません。これは、ルールベース内のポリシー ルールの順序が変更されるためです。PoliciesSecurityPolicy OptimizerNo App Specified、PoliciesSecurityPolicy OptimizerUnused Apps、および PoliciesSecurityPolicy OptimizerNew App Viewer (SaaS Inline Security サブスクリプションをお持ちの場合) をフィルタリングおよび並べ替えても、ルールベース内のルールの順序は変更されません。
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/app-id/security-policy-rule-optimization/policy-op

最新問題: **217**
今週、パワーボール宝くじの当選金額が異例の高値に達しました。貴社は社員の士気を高めるため、今週限定でパワーボール宝くじのウェブサイト（www.powerball.com）へのアクセスを許可することにしました。ただし、URLフィルタリングの「ギャンブル」カテゴリに登録されている他のウェブサイトへのアクセスは禁止されています。
従業員がPowerBall宝くじのウェブサイトにアクセスできる一方で、「ギャンブル」URLカテゴリへのアクセスをブロックしない方法はどれですか？
A. カスタム URL カテゴリを作成し、*.powerball.com を追加して、セキュリティ プロファイルで許可します。
B. URLフィルタリングの許可リストに*.powerball.comを追加します。
C. powerball.com をギャンブル URL カテゴリから手動で削除します。
D. セキュリティ ポリシーの許可ルールに URL www.powerball.com だけを追加します。
Answer: (解答を表示する**)**

最新問題: **218**
サイバー攻撃ライフサイクルの各段階を、正しい説明と一致させてください。

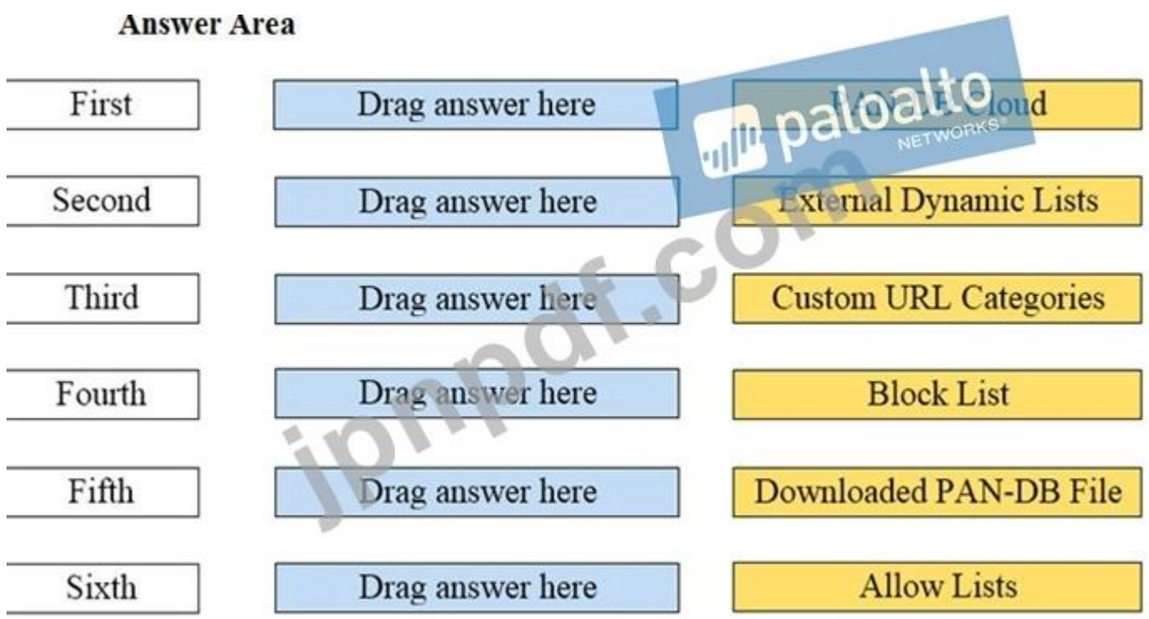


Answer:

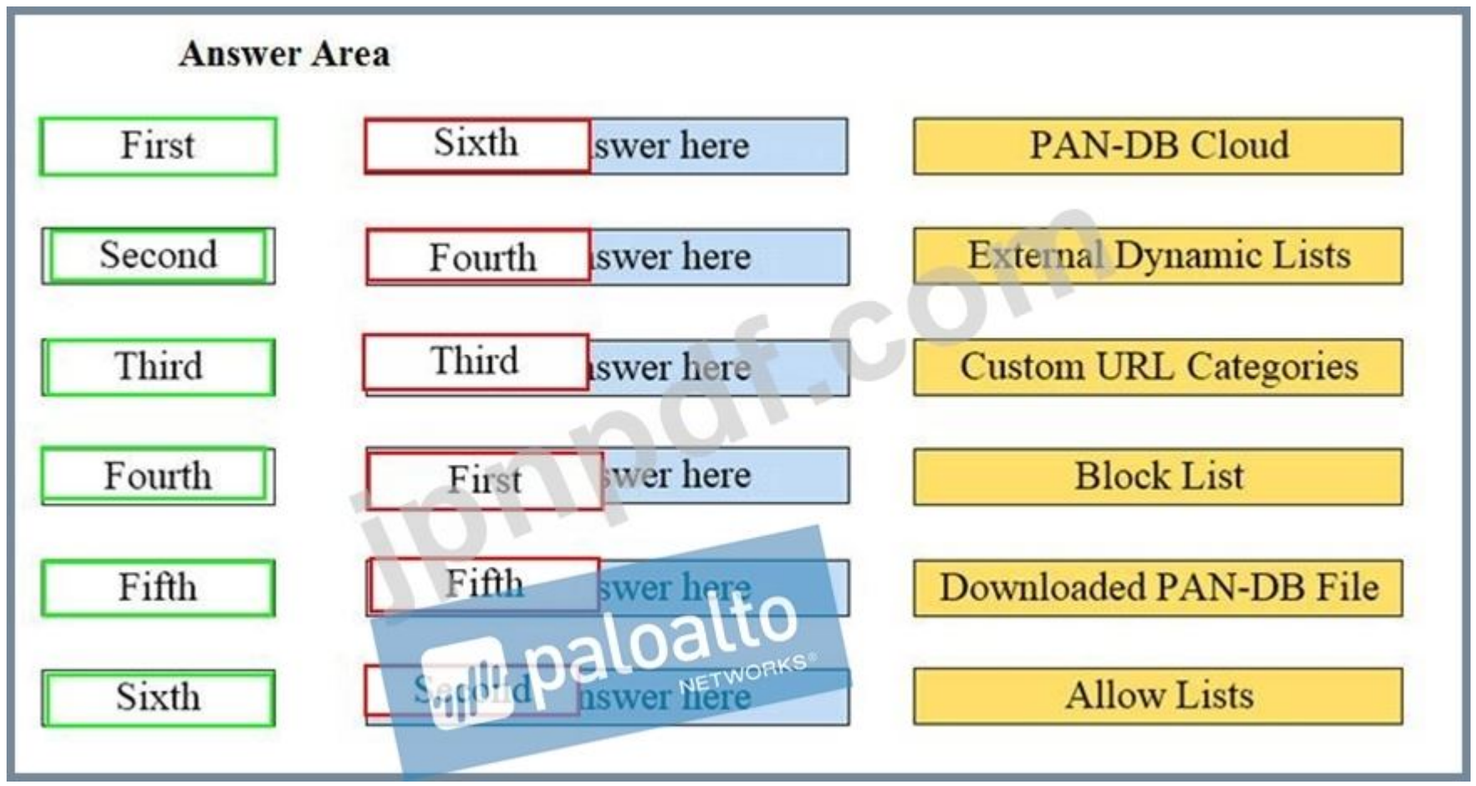


最新問題: **219**

システム内でURL分類が処理される正しい順序を設定してください。



Answer:



最新問題: **220**

管理者は、特定のアプリケーションに対するデフォルトの拒否アクションを上書きし、代わりにトラフィックをブロックしてICMPコード 宛先との通信は管理上禁止されています」を送信したいと考えています。どのセキュリティポリシーアクションがこれを引き起こしますか？

A. サーバーをリセット

B. ICMP到達不能を破棄して送信します
C. ドロップ
D. 両方をリセット
Answer: (解答を表示する**)**

最新問題**: 221**
PAN-OS 10.0でポートベースのセキュリティポリシールールの一覧を表示するパスはどれですか？
A. ポリシー > セキュリティ > ルールの使用 > アプリが指定されていません
B. ポリシー > セキュリティ > ルール使用 > ポートのみ指定
C. ポリシー > セキュリティ > ルールの使用 > ポートベースのルール
D. ポリシー > セキュリティ > ルールの使用状況 > 未使用のアプリ
Answer: A (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/security-policy-rule-optimization/migrate-po

最新問題**: 222**
提示された画像に基づいて、セキュリティポリシー規則について正しい選択肢を2つ選びなさい。2つ選択してください。）

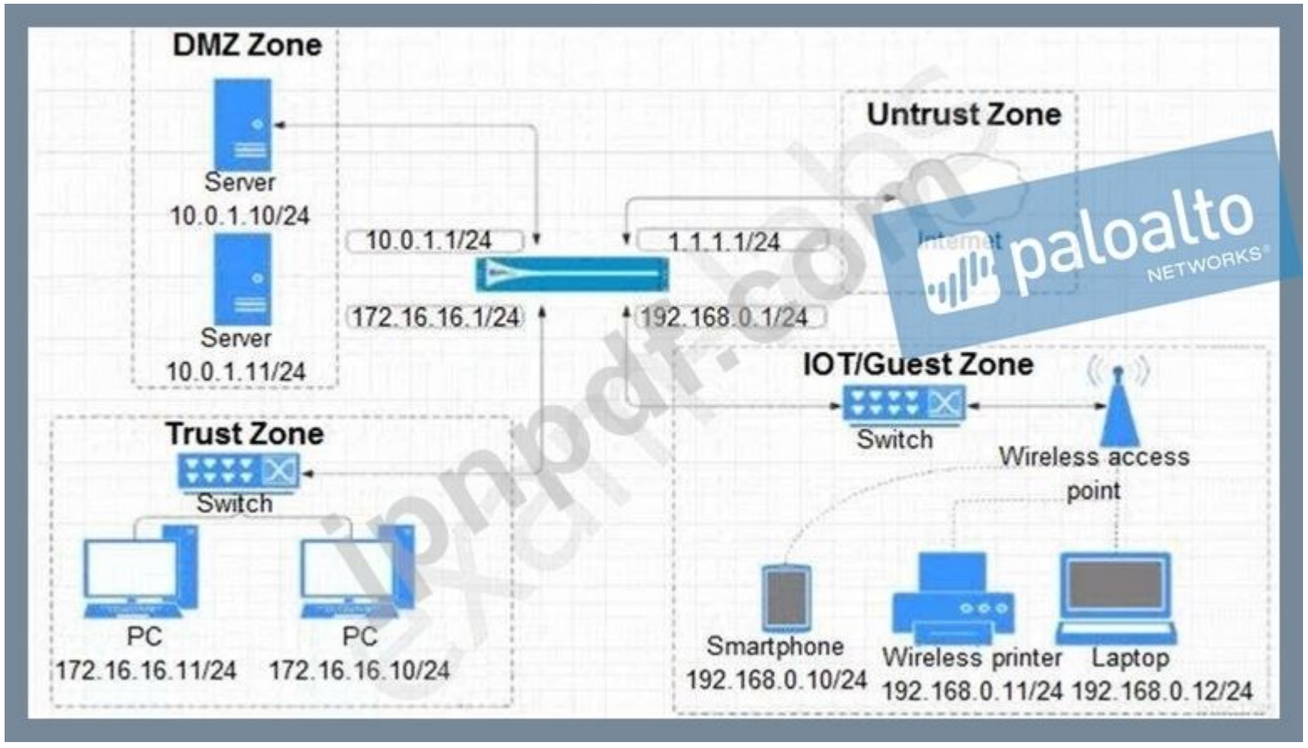
				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit	Application	Service	Action	Profile
1	Allow Office Programs	None	Universal	Inside	Any	Any	Any	Outside	Any	-	-	-	Office-program	Application-d…	Allow	None
2	Allow FTP to web ser…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

A. Webサーバーへの FTPを許可するルールでは、App-IDを使用してFTPが許可されます。
B. 『ソーシャルネットワーキングを許可する」ルールでは、Facebookのすべての機能を許可します。
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. 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
Answer: A,C (メーッセージを残す**)**

最新問題**: 223**
セキュリティポリシールールの構成要素となるコンポーネントはどれですか？
A. 復号プロファイル
B. 宛先インターフェース
C. タイムアウト（分）
D. アプリケーション
Answer: D (メーッセージを残す**)**
参照：
<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/policies/policies-security/buildingblocks-in-a-security-policy-rule.html>

最新問題: **224**
Active Directoryを使用していない場合に、ユーザー識別情報を取得するための有効なソリューションはどれですか？
A. クラウドアイデンティティエンジン
B. 認証ポータル
C. グループマッピング
D. ディレクトリ同期サービス
Answer: B (メーッセージを残す**)**

最新問題: **225**
ネットワーク図を考慮すると、信頼済みユーザーとゲストユーザーの両方が、SSH、ウェブブラウジング、およびSSLアプリケーションを使用して、一般的なインターネットサーバーとDMZサーバーにアクセスできるようにする必要があります。



どの政策が望ましい結果をもたらすのか？

A.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
03-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	1.1.1.0/24 10.0.1.0/24	any	ssh ssl web-browsing	app

B.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
04-A	none	universal	IOT-Guest Trust	172.16.16.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

C.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
01-A	none	universal	IOT-Guest Trust	10.0.1.0/24 172.16.16.0/12	any	any	DMZ Untrust	1.1.1.0/24 192.168.0.0/24	any	ssh ssl web-browsing	app

D.

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE
02-A	none	universal	IOT-Guest Trust	172.16.18.0/24 192.168.0.0/24	any	any	DMZ Untrust	any	any	ssh ssl web-browsing	app

Answer: B (メーッセージを残す)

最新問題**: 226**
セキュリティポリシールールとセキュリティプロファイルの動作を説明する3つの記述はどれですか？
（3選択してください。）
A. セキュリティポリシールールは、トラフィックをブロックまたは許可することができます。
B. セキュリティポリシールールはトラフィックを検査しますが、ブロックしません。
C. セキュリティポリシールールはセキュリティプロファイルに紐付けられています。
D. セキュリティプロファイルはセキュリティポリシールールに添付されます。
E. セキュリティプロファイルは、許可されたトラフィックに対してのみ使用する必要があります。
Answer: A,D,E (メーッセージを残す)

最新問題**: 227**
Palo Alto Networksファイアウォールにおいて、構成ログ記録およびレポート機能を別のプロセッサ上で提供するプレーンはどれですか？
A. データ
B. セキュリティ処理
C. 管理
D. ネットワーク処理

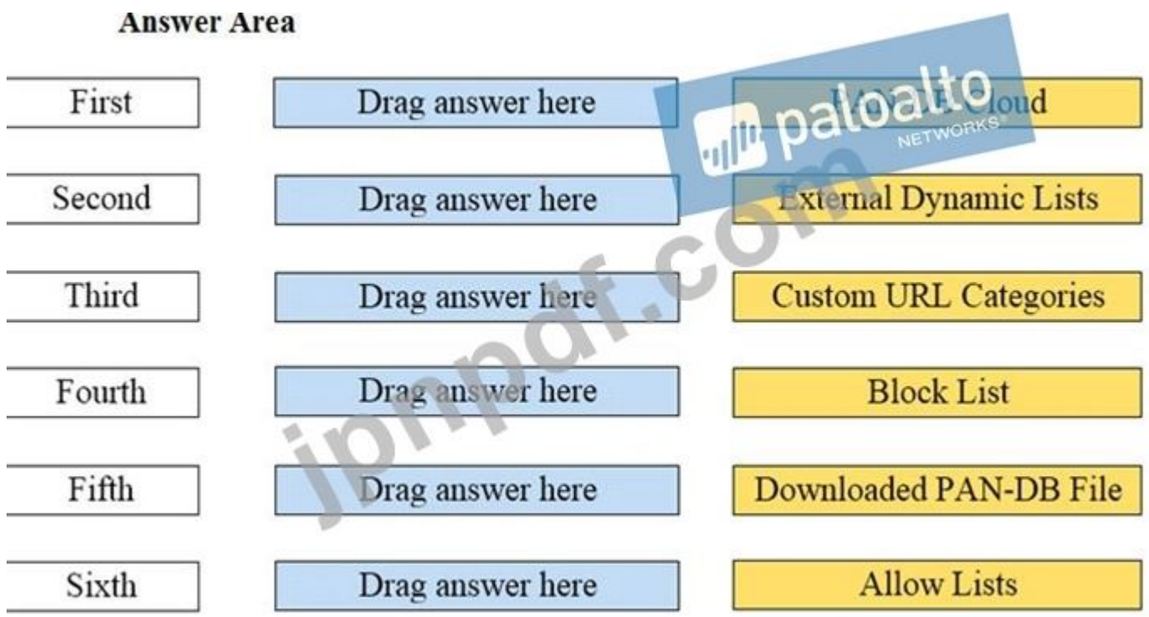
Answer: C (メーッセージを残す)

最新問題: **228**
管理者は、既知のマルウェアドメインをすべてブロックまたはシンクホールするために、リアルタイムのシグネチャ検索を実行する機能を追加する必要があります。
この結果を得るには、どのタイプの単一統合エンジンを使用すればよいでしょうか？
A. ユーザーID
B. セキュリティ処理エンジン
C. アプリID
D. コンテンツID
Answer: (解答を表示する)

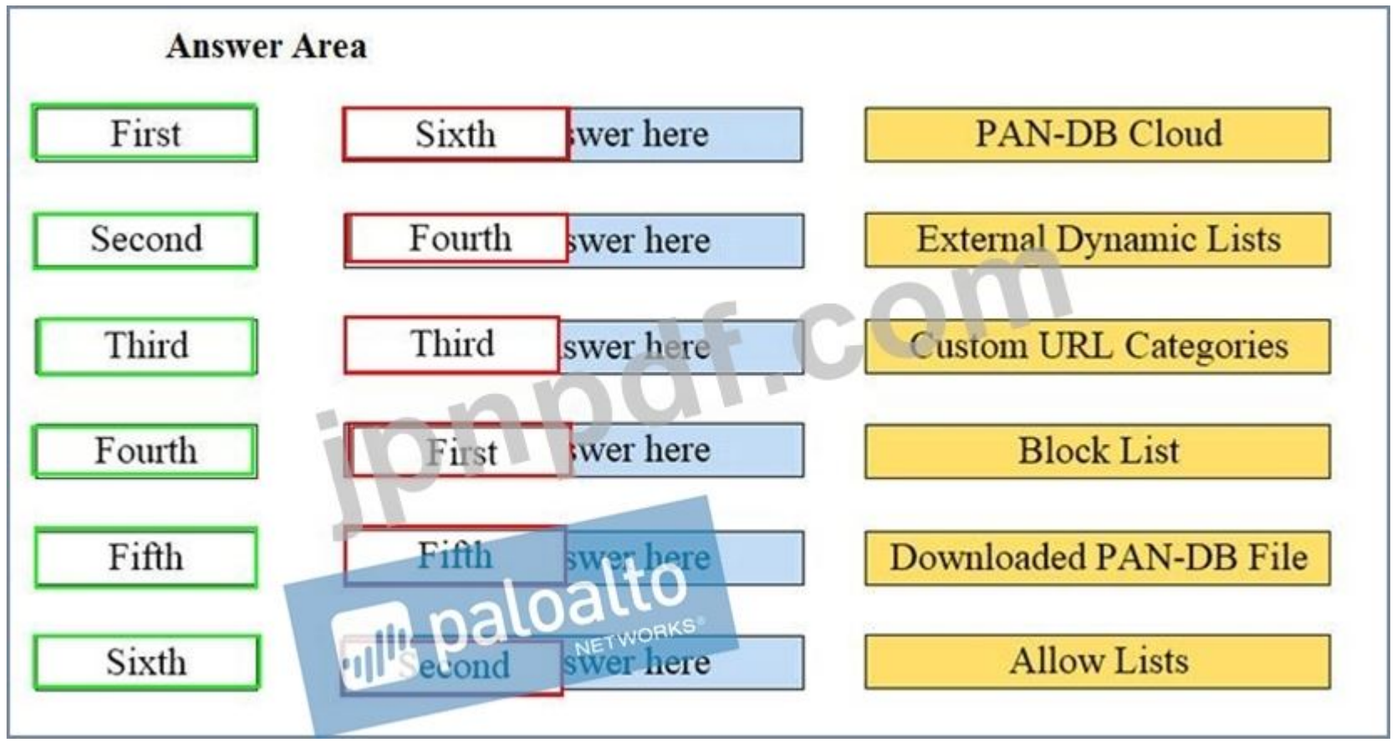
最新問題: **229**
ユーザーがURLにアクセスしようとしたときにログエントリを生成しないURLフィルタリングプロファイルアクションはどれですか？
A. オーバーライド
B. 許可する
C. ブロック
D. 続ける
Answer: B (メーッセージを残す)
説明/参考資料 :https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/url-filtering/url-filtering-concepts/url-filtering-profile-actions

最新問題: **230**
動的ユーザーグループでは、どのような操作が必要になりますか？
A. 異常なユーザー行動や悪意のある活動に対する自動修復を提供するQoSポリシーを作成する
B. 異常なユーザー行動や悪意のある活動に対して自動サイズ調整を行うポリシーを作成する
C. 異常なユーザー行動や悪意のある活動に対する自動修復を提供するポリシーを作成する
D. ファイアウォール管理者の動的なリストを作成する
Answer: (解答を表示する)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Dynamic%20user%20groups%20help%20you,activity%20while%20maintaining%20user%20visibility.

最新問題: **231**
システム内でURL分類が処理される正しい順序を設定してください。

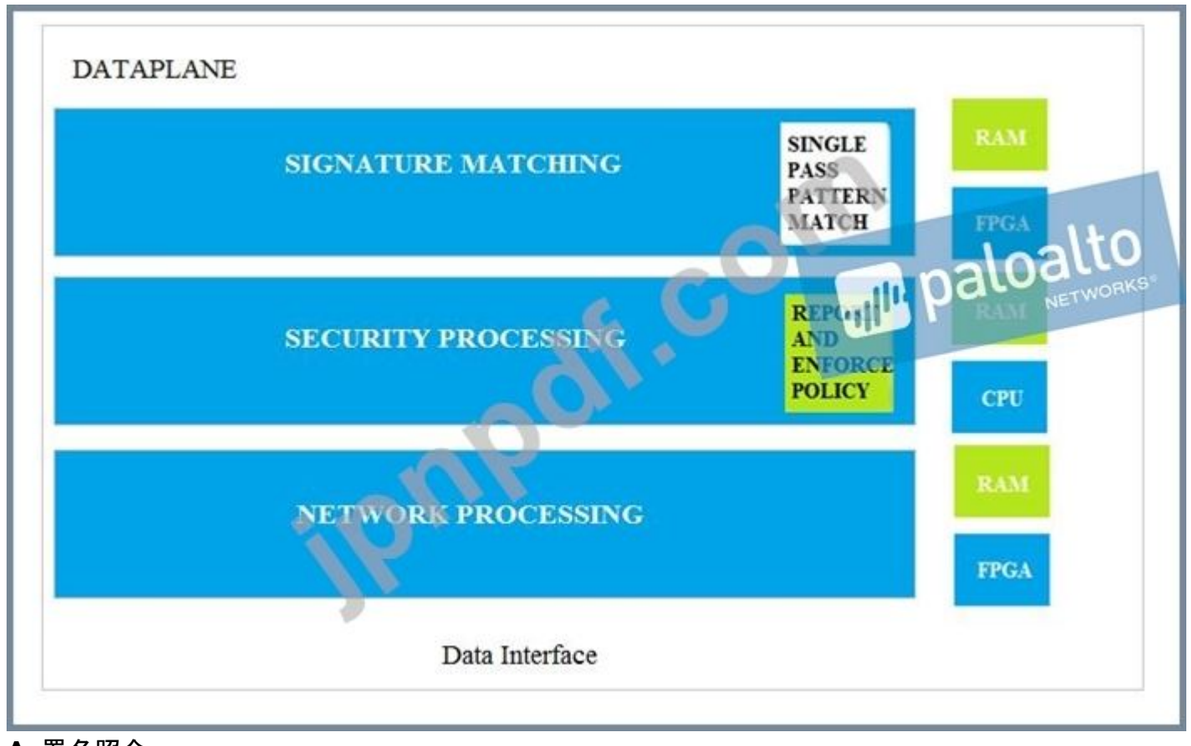


Answer:



最新問題**: 232**

図に示すデータプレーンプロセッサ層のうち、Palo Alto Networksファイアウォール上でスパイウェアと脆弱性攻撃に対して均一なマッチングを提供する層はどれですか？



A. 署名照合
B. ネットワーク処理
C. セキュリティマッチング
D. セキュリティ処理
Answer: A (メーッセージを残す**)**

最新問題**: 233**
Panoramaからファイアウォールにコンテンツアップデートを展開する際に、推奨される考慮事項は何ですか？
A. コンテンツの更新をデプロイした後、コミットを実行して Panorama にプッシュします。
B. コンテンツアップデートを展開する前に、必ずコンテンツのリリースバージョンの互換性を確認してください。
C. ファイアウォール A/P HA ペアのコンテンツ更新は、アクティブなファイアウォールにのみプッシュされます。
D. ファイアウォール A/A HA ペアのコンテンツ更新には、マスター デバイスの定義が必要です。
Answer: A (メーッセージを残す**)**

最新問題**: 234**
Secure Shell (SSH) を使用して宛先ポート tcp/22 および tcp/4422 への送信トラフィックを許可するには、セキュリティポリシーをどのように記述する必要がありますか？
A. 管理者は、ポート tcp/4422 を持つ ftcp-4422」という名前のカスタムサービスオブジェクトを作成します。
管理者は、アプリケーション §ssh」とサービス ftcp-4422」を許可するセキュリティポリシーを作成します。
B. 管理者は、ポート tcp/4422 を持つ ftcp-4422」という名前のカスタムサービスオブジェクトを作成します。
管理者は、アプリケーション §ssh」、サービス ftcp-4422」、およびサービス §application-default」を許可するセキュリティポリシーを作成します。
C. 管理者は、ポート tcp/4422 を持つ ftcp-4422」という名前のカスタムサービスオブジェクトを作成します。
管理者は、ポートtcp/22を持つ ftcp-22」という名前のカスタムサービスオブジェクトも作成します。

管理者は、アプリケーション「ssh」、サービス「tcp-4422」、およびサービス「tcp-22」を許可するセキュリティポリシーを作成します。
D. 管理者は、アプリケーション「ssh」とサービス「application-default」を許可するセキュリティ ポリシーを作成します。
Answer: C (メーッセージを残す**)**
アプリケーションのデフォルト設定を選択した場合、他のサービスは追加されません。

最新問題**: 235**
ファイアウォールで新しいWildFireシグネチャをチェックするために設定できる最小期間はどれくらいですか？
A. 30分ごと
B. 5分ごと
C. 24時間ごとに1回
D. 1分ごと
Answer: (解答を表示する**)**
説明
WildFireライセンスが有効になっているファイアウォールは、5分ごとに最新のWildFireシグネチャを取得できます。WildFireのサブスクリプションをお持ちでない場合、有効な脅威防御ライセンスを持つファイアウォール向けのウイルス対策アップデートの一環として、24～48時間以内にシグネチャが利用可能になります。
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-concepts/wildfire-sign

最新問題**: 236**
システム内でURL分類が処理される正しい順序を設定してください。

Answer Area

First	Drag answer here	[illegible] Cloud
Second	Drag answer here	External Dynamic Lists
Third	Drag answer here	Custom URL Categories
Fourth	Drag answer here	Block List
Fifth	Drag answer here	Downloaded PAN-DB File
Sixth	Drag answer here	Allow Lists

Answer:

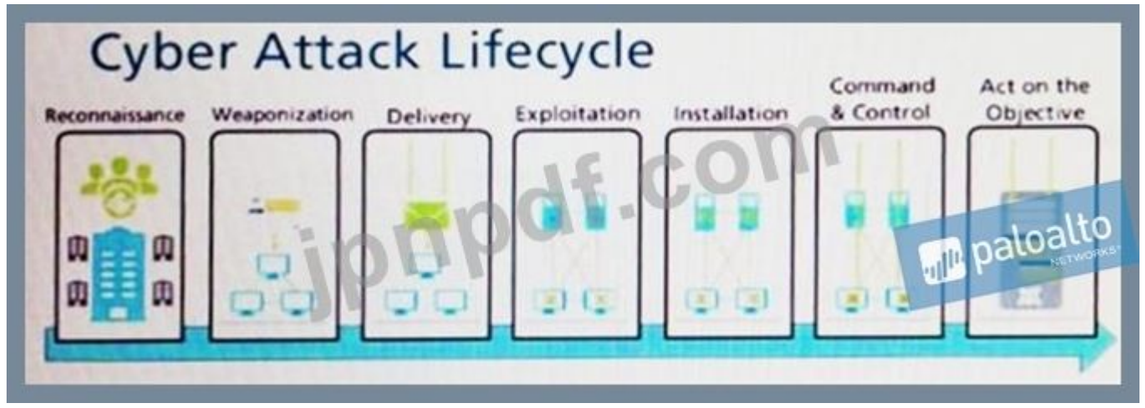
Answer Area

最新問題: **237**
ドラッグアンドドロップ問題
パケット処理の正しい順序で手順を配置してください。

Answer:

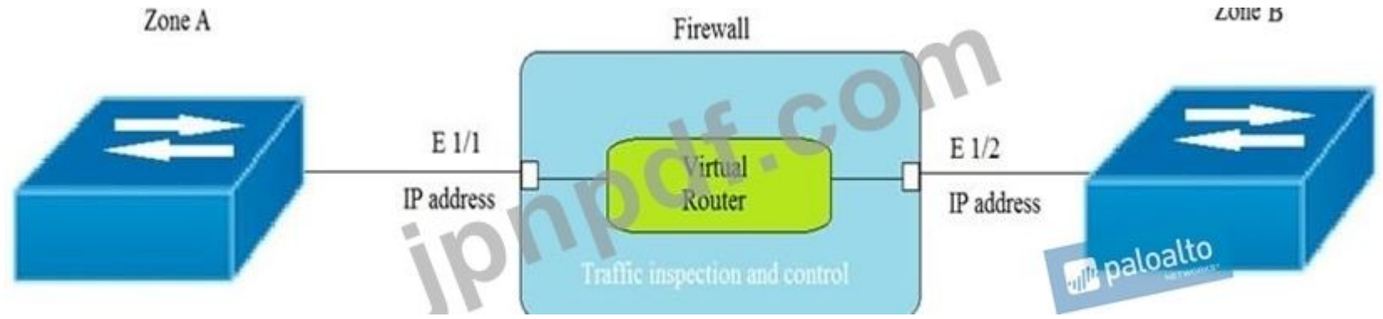
Operational Task	Answer Area	
	zone protection	first
	decryption	second
	Security profile enforcement	third
	App-ID	fourth

最新問題: **238**
サイバー攻撃ライフサイクル図に基づいて、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てください。



A. 認識
B. 目標に基づいて行動する
C. 搾取
D. 設置
Answer: (解答を表示する)

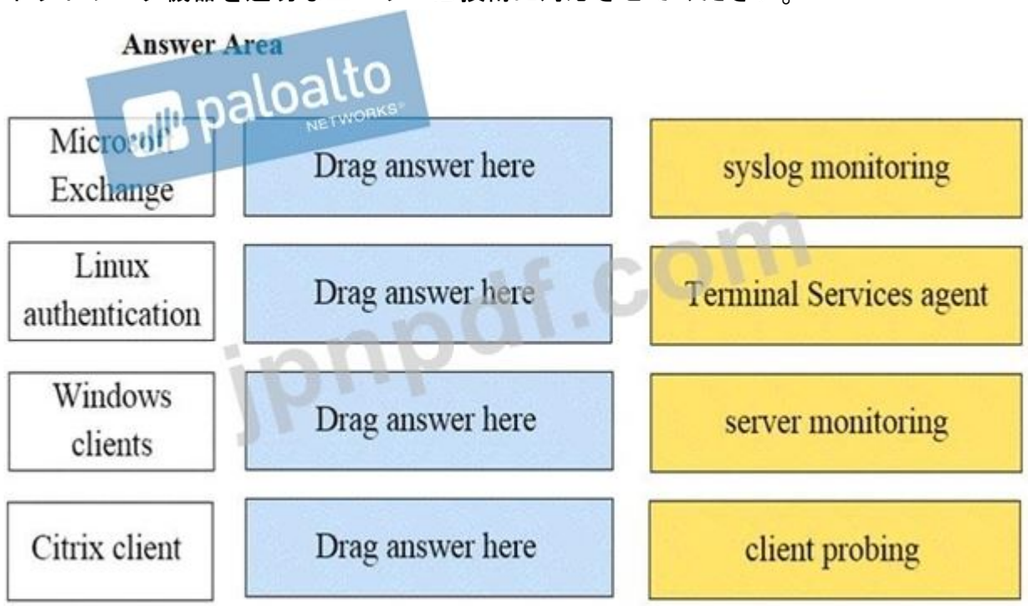
最新問題: **239**
トポロジーを考慮すると、ゾーンAとゾーンBにはどのゾーンタイプを設定すべきでしょうか？



A. レイヤー3
B. レイヤー2
C. バーチャルワイヤー
D. タップ
Answer: A (メーッセージを残す)

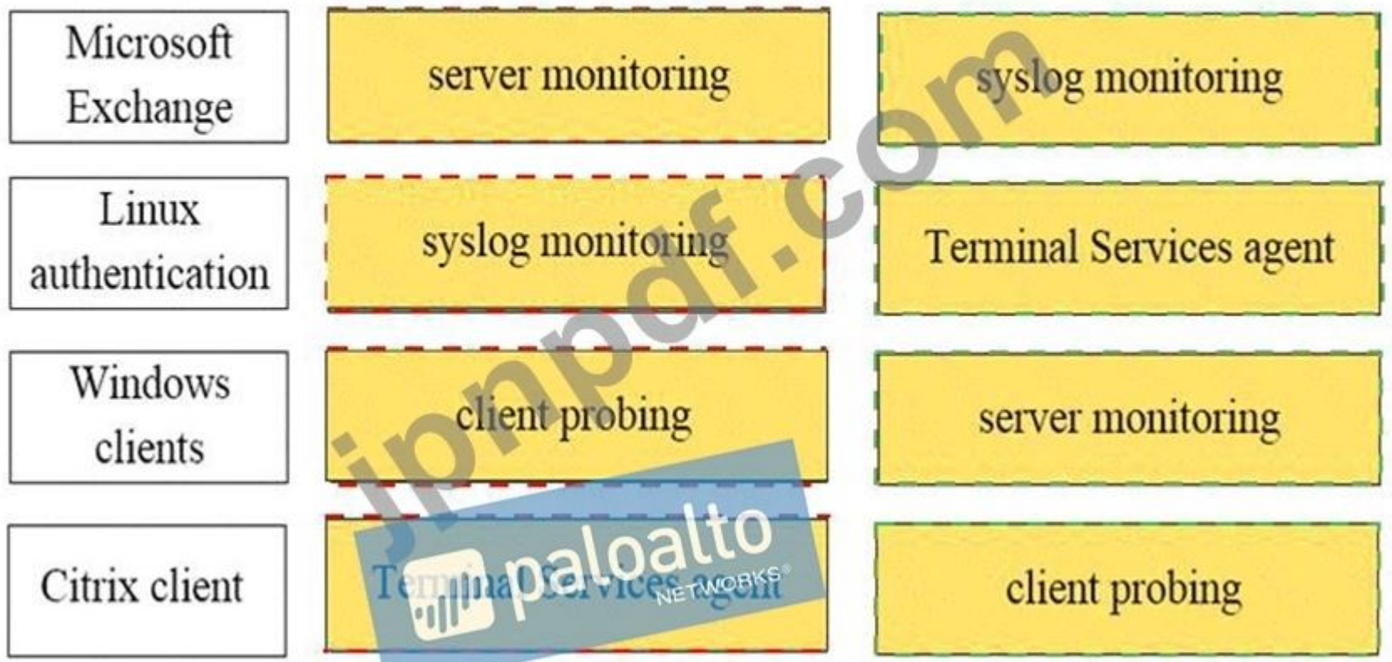
最新問題: **240**
企業がセキュリティポリシーに紐づいたファイルブロックプロファイルを持つべき理由は？
A. 特定の種類のファイルのアップロードとダウンロードをブロックする
B. サンドボックス環境でファイルを爆発させる
C. ファイルの種類を分析する
D. あらゆる種類のファイルのアップロードとダウンロードをブロックする
Answer: A (メーッセージを残す)

最新問題: **241**
ネットワーク機器を適切なユーザーID技術に対応させてください。



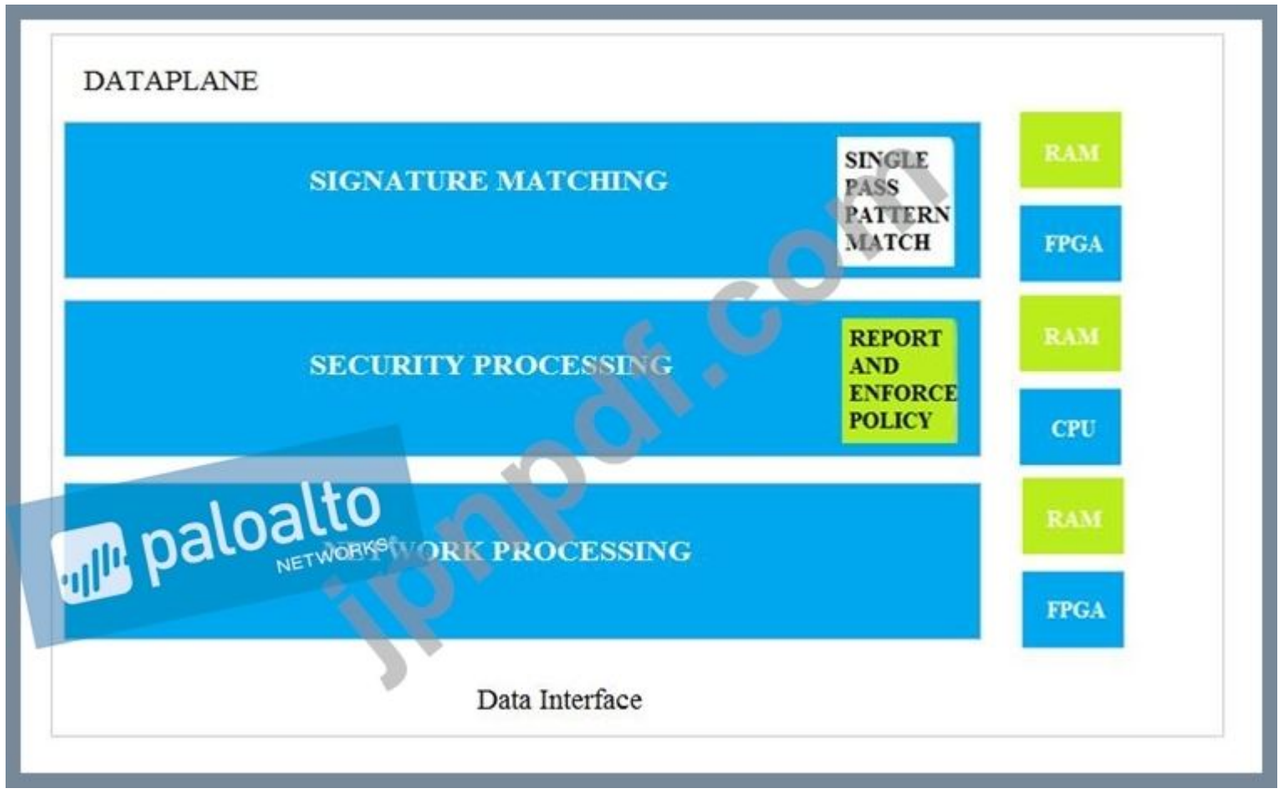
Answer:

Answer Area



説明
Microsoft Exchange - サーバー監視
Linux認証 - syslog監視
Windowsクライアント - クライアントプロービング
Citrixクライアント - ターミナルサービスエージェント

最新問題: **242**
図に示すデータプレーンプロセッサ層のうち、Palo Alto Networksファイアウォール上でスパイウェアと脆弱性攻撃に対して均一なマッチングを提供する層はどれですか？

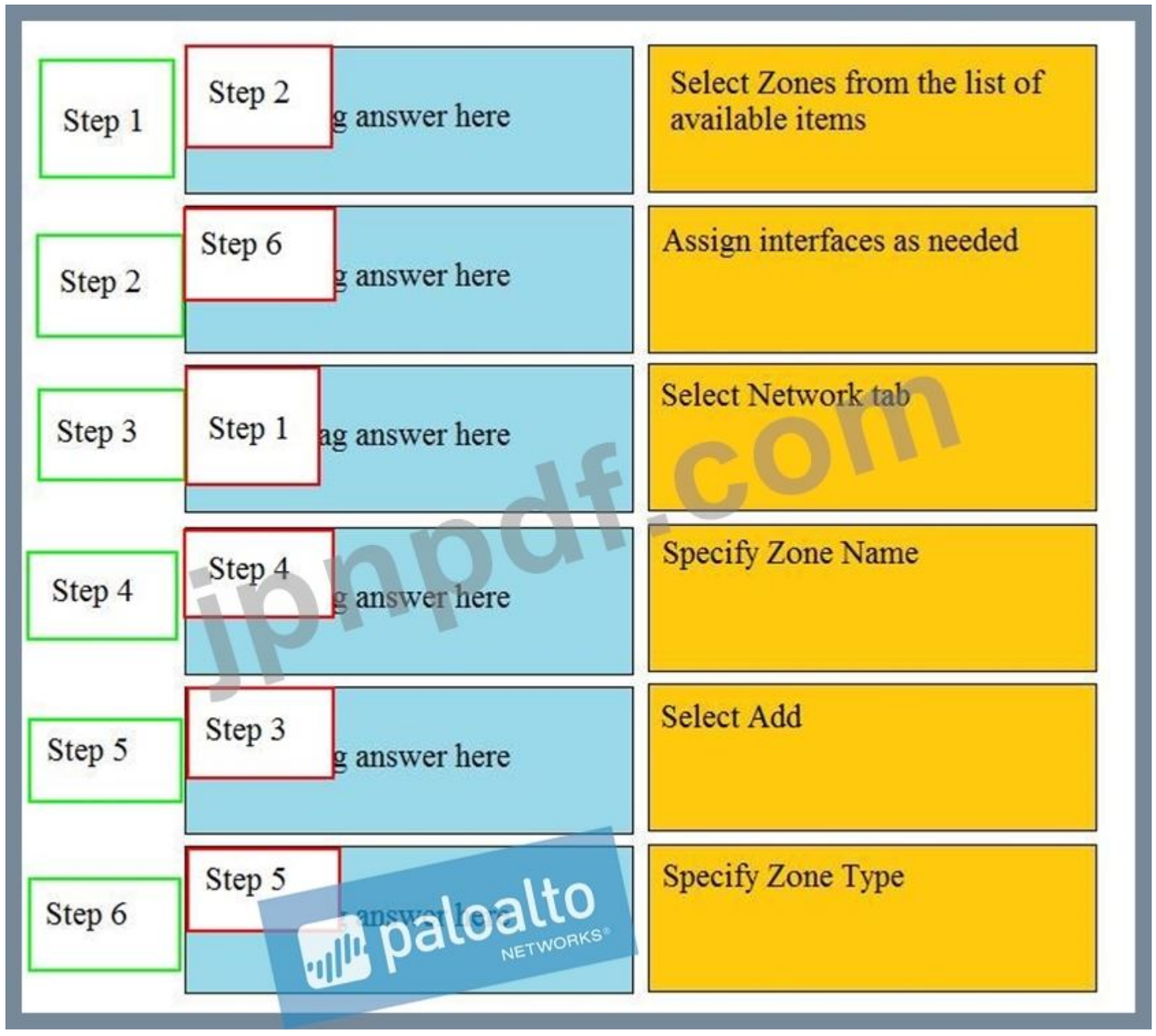


A. ネットワーク処理
B. セキュリティマッチング
C. 署名照合
D. セキュリティ処理
Answer: C (メーッセージを残す**)**

最新問題**: 243**
Palo Alto Networks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順番に説明します。

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:



最新問題: **244**
以下の手順を、パケット処理の操作順序に従って、最初から最後までの順に並べてください。

Answer:

最新問題: **245**

セキュリティポリシーにおいて、すべてのポリシールールのヒットカウンターをゼロにする最も迅速な方法は何ですか？

A. ファイアウォールを再起動してください。
B. 各ルールをハイライトし、[ルールヒットカウンターのリセット] > [選択したルール] を使用します。
C. [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。
D. CLIを使用して、reset rules allコマンドを入力します。
Answer: D (メーッセージを残す)

最新問題: **246**
管理者がセキュリティポリシールールを設定し、一致条件に単一のアプリケーションを含め、アクションを拒否するように設定しました。ファイアウォールはどのような拒否アクションを実行しますか？
A. セッションのパケットを破棄し、TCPリセットパケットを送信して、セッションが終了したことをクライアントに通知します。
B. 静かに交通を遮断する
C. アプリケーションに対してApp-IDデータベースで定義されているデフォルトの拒否アクションを実行します。
D. クライアント側およびサーバー側のデバイスにTCPリセットパケットを送信する
Answer: A (メーッセージを残す)

最新問題: **247**
示されているセキュリティポリシーの例では、どの2つのウェブサイトが不正行為を行っていますか？ 2つ選択してください。）

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

最新問題: **248**
管理者は、10個のデバイスグループと5つのテンプレートにまたがる、100台のPanorama管理ファイアウォール上のセキュリティポリシーで、同じアドレスオブジェクトを参照したいと考えています。
管理者はアドレスオブジェクトを作成する際に、どの設定操作を行うべきですか？
A. 共有」オプションがチェックされていることを確認してください。
B. 共有」オプションがオフになっていることを確認してください。
C. オーバーライド無効化が解除されていることを確認してください。
D. アドレスオブジェクトにグローバルタグを付ける。
Answer: A (メーッセージを残す)
10 台の Panorama 管理ファイアウォール上のセキュリティ ポリシーで、10 のデバイス グループと 5 つのテンプレートにわたって同じアドレス オブジェクトを参照するには、管理者はアドレス オブジェクトの作成時に [共有] オプションがチェックされていることを確認する必要があります。このオプションを使用すると、管理者は Panorama 上のすべてのデバイス グループとテンプレートで使用できる共有アドレス オブジェクトを作成できます。共有アドレス オブジェクトは、複数のファイアウォール ポリシー ルール、フィルタ、およびその他の機能で使用できます 1。これによ

り、複数のファイアウォールにわたるアドレス オブジェクトの管理の複雑さと重複が軽減されます 2。参照: アドレス オブジェクト、共有アドレス オブジェクトの作成、認定 - Palo Alto Networks、Palo Alto Networks 認定ネットワーク セキュリティ アドミニストレーター (PAN-OS 10.0) または [Palo Alto Networks 認定ネットワーク セキュリティ アドミニストレーター (PAN-OS 10.0)]。

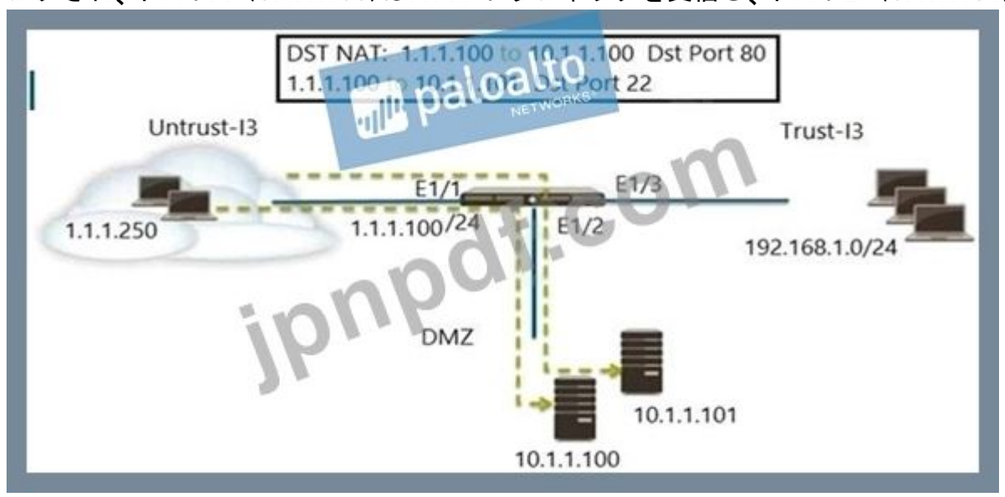
最新問題: **249**
図に基づいて、SSL/TLSサービスプロファイル構成オプションの目的は何ですか？

A. 管理インターフェースを保護するために使用されるSSL/TLS暗号化の強度を定義します。
B. クライアントのブラウザを検証するために使用される CA 証明書を定義します。
C. 管理インターフェースからクライアントのブラウザに送信する証明書を定義します。
D. ファイアウォールのグローバルなSSL/TLSタイムアウト値を定義します。
Answer: C (メーッセージを残す)

SSL/TLSサービスプロファイルは、SSL/TLSを使用するファイアウォールまたはPanoramaサービス（Webインターフェースへの管理アクセスなど）のサーバー証明書とプロトコルバージョン、またはバージョン範囲を指定します。プロトコルバージョンを定義することで、プロファイルは、サービスを要求するクライアントシステムとの通信を保護するために使用できる暗号スイートを制限できます。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/device/device-certificate-management-ssltls-service-profile

最新問題: **250**
管理者がセキュリティポリシーのルールベースを確認し、未使用のルールを特定できる機能はどれですか？
A. テストポリシーの一致
B. ポリシーオプティマイザ
C. ルールベースをグループとして表示
D. セキュリティポリシータグ eb
Answer: B (メーッセージを残す**)**
Policy Optimizerは、従来のセキュリティポリシールールベースをApp-IDベースのルールベースに移行するためのシンプルなワークフローを提供します。これにより、攻撃対象領域が縮小し、アプリケーションの可視性が向上するため、セキュリティが強化され、アプリケーションを安全に有効化できるようになります。Policy Optimizerは、未使用のルール、重複するルール、およびルールベースを最適化するためにマージまたは並べ替え可能なルールを特定することもできます。Policy Optimizerを使用して、ルールの使用統計を確認し、必要に応じてルールベースをクリーンアップまたは変更するアクションを実行できます1。参照 :セキュリティポリシールールの最適化、PAN-OS 10.1の認定資格の更新、Palo Alto Networks PCNSE試験の無料PCNSE問題

最新問題: **251**
図を参照してください。管理者はDNATを使用して、2台のサーバーを1つのパブリックIPアドレスにマッピングしています。トラフィックはアプリケーションに基づいて特定のサーバーにルーティングされ、ホストA（10.1.1.100）はHTTPトラフィックを受信し、ホストB（10.1.1.101）はSSHトラフィックを受信します。



この構成を実現するには、どのセキュリティポリシールールを2つ選択すればよいですか？（2つ選択してください。）
A. DMZ (10.1.1.100、10.1.1.101) への不信 (任意)、ssh、ウェブブラウジング許可
B. DMZ (1.1.1.100) への接続を信頼しない (任意)、ssh - 許可
C. 信頼しない (すべて) から信頼しない (10.1.1.1)、ウェブブラウジング - 許可
D. Untrust (Any) から Untrust (10.1.1.1) へ、ssh -Allow
E. DMZ (1.1.1.100) への不信 (任意)、ウェブブラウジング - 許可
Answer: (解答を表示する**)**

最新問題: **252**
スクリーンショットに示されているように、管理者はどのような2種類のルートを設定していますか？ 2つ選択してください）

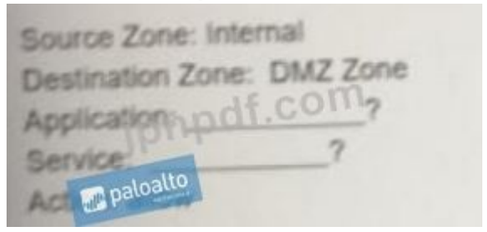
A. BGP
B. 静的ルート
C. OSPF
D. デフォルトルート
Answer: D (メーッセージを残す**)**

最新問題: **253**
保護されたネットワーク上のuwallユーザーデータベースで感染したホストを特定するには、どのセキュリティプロファイルを適用しますか？
A. 脆弱性対策
B. URLフィルタリング
C. アンチウイルス
D. スパイウェア対策
Answer: D (メーッセージを残す**)**

最新問題: **254**
PAN-OS 9.0でポートベースのセキュリティポリシールールの一覧を表示するパスはどれですか？
A. ポリシー > セキュリティ > ルールの使用 > アプリが指定されていません
B. ポリシー > セキュリティ > ルール使用 > ポートのみ指定

C. ポリシー > セキュリティ > ルールの使用 > ポートベースのルール
D. ポリシー > セキュリティ > ルールの使用状況 > 未使用のアプリ
Answer: C (メーッセージを残す**)**
説明／参考資料：

最新問題**: 255**
内部ゾーンのすべてのユーザーは、DMZゾーン内のサーバーへのTelnetアクセスのみを許可される必要があります。このタイプのアクセスのみを許可するセキュリティポリシールールの空欄2つを埋めてください。



2つ選択してください。
A. サービス - "application-default"
B. アプリケーション = "任意"
C. サービス＝ 任意の」
D. アプリケーション = "Telnet"
Answer: A,D (メーッセージを残す**)**

最新問題**: 256**
ファイアウォールポリシーにおいて、アプリケーションフィルタやアプリケーショングループはどのように使用されますか？
A. アプリケーションフィルタは、アプリケーションをグループ化するための動的な方法であり、アプリケーショングループのネストされたメンバーとして構成できます。
B. アプリケーショングループはアプリケーションをグループ化する静的な方法であり、アプリケーショングループのネストされたメンバーとして構成することはできません。
C. アプリケーショングループは、アプリケーションをグループ化する動的な方法であり、アプリケーショングループのネストされたメンバーとして構成できます。
D. アプリケーションフィルタは、アプリケーションをグループ化する静的な方法であり、アプリケーショングループのネストされたメンバーとして構成できます。
Answer: A (メーッセージを残す**)**

最新問題**: 257**
管理者は、インターネットからFTPサーバーへのトラフィックをサイレントモードで遮断したいと考えています。管理者はどのセキュリティポリシーアクションを選択すべきでしょうか？
A. サーバーリセット
B. 拒否する
C. ドロップ
D. ブロック

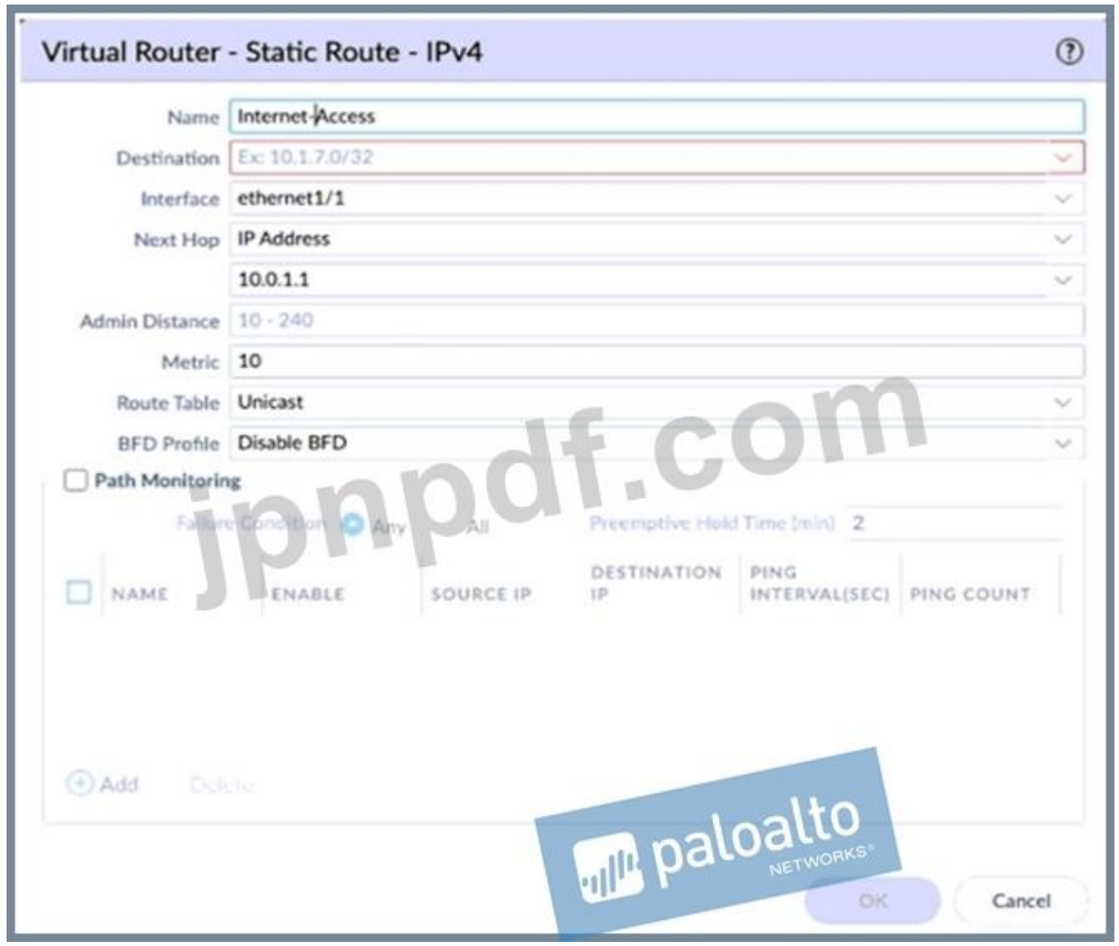
Answer: C (メーッセージを残す)
Dropはパケットをサイレントに破棄するのに対し、denyは更新情報を提供する。

最新問題: **258**
送信元IPアドレスを1対1で変換しつつ、送信元ポートの変更を可能にする機能はどれですか？ 2つ選択してください。）
A. 固定IPアドレス
B. 動的IP/ポートフォールバック
C. 動的IP
D. 動的IPおよびポート（DIPP）
Answer: A,D (メーッセージを残す)
静的IPと動的IPおよびポート（DIPP）は、送信元IPアドレスを1対1で変換しながら、送信元ポートを変更できるようにする2つの機能です。静的IPは、単一の送信元アドレスを特定のパブリックアドレスに変換し、送信元ポートを動的に変更できるようにします1。動的IPおよびポート（DIPP）は、送信元IPアドレスまたは範囲を単一のIPアドレスに変換し、送信元ポートを使用して、同じ変換済みアドレスを共有する複数の送信元IPを区別します2。これらの機能はどちらもIPアドレスの1対1変換を提供しますが、送信元ポートを制限しません。参考文献：
固定IPアドレス - パロアルトネットワークス
動的IPアドレスとポート番号 - パロアルトネットワークス

最新問題: **259**
どのタイプのセキュリティルールが、内部ゾーンと外部ゾーン間、内部ゾーン内、および外部ゾーン内のトラフィックに一致しますか？
A. グローバル
B. イントラゾーン
C. インターゾーン
D. ユニバーサル
Answer: (解答を表示する)
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcns a-study-guide-latest.pdf

最新問題: **260**
Windows Active Directoryで認証を行わないクライアントが存在する環境では、どのユーザーIDマッピング方法を使用すべきでしょうか？
A. ドメインコントローラーを介したWindowsセッション監視
B. Windowsベースのエージェントを使用したパッシブサーバー監視
C. キャプティブポータル
D. PAN-OS統合型User-IDエージェントを使用したパッシブサーバー監視
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: **261**
Ethernet 2/1 は、ゾーン「trust」（LAN）に属し、IP アドレスは 10.0.1.2 です。
両方のインターフェースが同じ仮想ルーターに接続されている場合、管理者はインターネットにアクセスするために、宛先フィールドにどのIPアドレス情報を入力する必要がありますか？



A. 10.0.1.254/32
B. 10.0.2.1/32
C. 0.0.0.0
D. 0.0.0.0/0
Answer: (解答を表示する**)**

最新問題**: 262**
管理者が、以下のスクリーンショットに示されているセキュリティポリシールールを確認しています。
表示されている情報について、正しい記述はどれですか？

A. ビュー 『ルールベースをグループとして表示」がチェックされています。
B. 未使用ルールのハイライト表示にチェックが入っています。
C. 11個のルールが 『インフラストラクチャ*」タグを使用しています。
D. このファイアウォールには7つのセキュリティポリシールールがあります。
Answer: A (メーッセージを残す**)**

最新問題**: 263**
DNSシンクホーリングを有効にするには、どの2つのアドレスを予約する必要がありますか？ 2つ選択してください。）
A. MAC
B. IPv6
C. メール
D. IPv4
Answer: B,D (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGECA0

最新問題**: 264**
ある管理者が、別の管理者のセキュリティポリシーログ設定を確認している。
通常のトラフィックにおけるベストプラクティスに合致するログ設定構成はどれですか？
A. セッション開始時のログ記録は無効、セッション終了時のログ記録は有効
B. セッション開始時のログ記録有効 セッション終了時のログ記録無効
C. セッション開始時のログ記録とセッション終了時のログ記録の両方が有効になっています
D. セッション開始時のログ記録とセッション終了時のログ記録の両方が無効になっています。
Answer: A (メーッセージを残す**)**

最新問題**: 265**

コンプライアンス担当者は、インターネットへのすべての境界ファイアウォールで、回避的なアプリケーションをすべてブロックする必要があると要求しています。ファイアウォールは2つのゾーンで構成されています。
1. 内部ネットワークに対する信頼
2. インターネットへの不信感
Palo Alto Networks NGFWの機能に基づいて、この要求を満たすためにApp-IDを使用してセキュリティポリシーを設定する2つの方法は何ですか？ 2つ選択してください）
A. ポリシーの最上位に、信頼から非信頼への拒否ルールを作成し、すべてのサービスに対して、アプリケーションとして回避を選択します。
B. ポリシーの最上位に、信頼から非信頼への拒否ルールを任意のサービスに対して作成し、回避特性を持つアプリケーションフィルタを追加します。
C. ポリシーの最上位に、サービス application-default を使用して、信頼から信頼しないへの拒否ルールを作成し、アプリケーションとして evasive を選択します。
D. ポリシーの最上位に、サービス application-default を使用して、信頼から非信頼への拒否ルールを作成し、回避特性を持つアプリケーションフィルタを追加します。
Answer: (解答を表示する**)**

最新問題**: 266**
PAN-OS統合型USER-IDエージェントを設定する正しい順序を特定してください。
3. サーバーを監視するためのサービスアカウントを追加する
2. ファイアウォール上で監視対象サーバーのアドレスを定義します。
4. 設定をコミットし、エージェントの接続状態を確認します。
1. ドメインコントローラー上に、User-IDエージェントを実行するための十分な権限を持つサービスアカウントを作成します。
A. 2-3-4-1
B. 1-4-3-2
C. 3-1-2-4
D. 1-3-2-4
Answer: D (メーッセージを残す**)**
まずアカウントを作成し、次にファイアウォールにそのアカウントを追加し、監視したいサーバーを追加し、最後に変更を適用します。

最新問題**: 267**
提示されたセキュリティポリシー規則に基づくと、SSHはどのポートで許可されますか？

			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. 一時的な港のみ
B. 任意の港
C. SSLおよびSNMPv3と同じポート
D. デフォルトポート

Answer: D (メーッセージを残す)

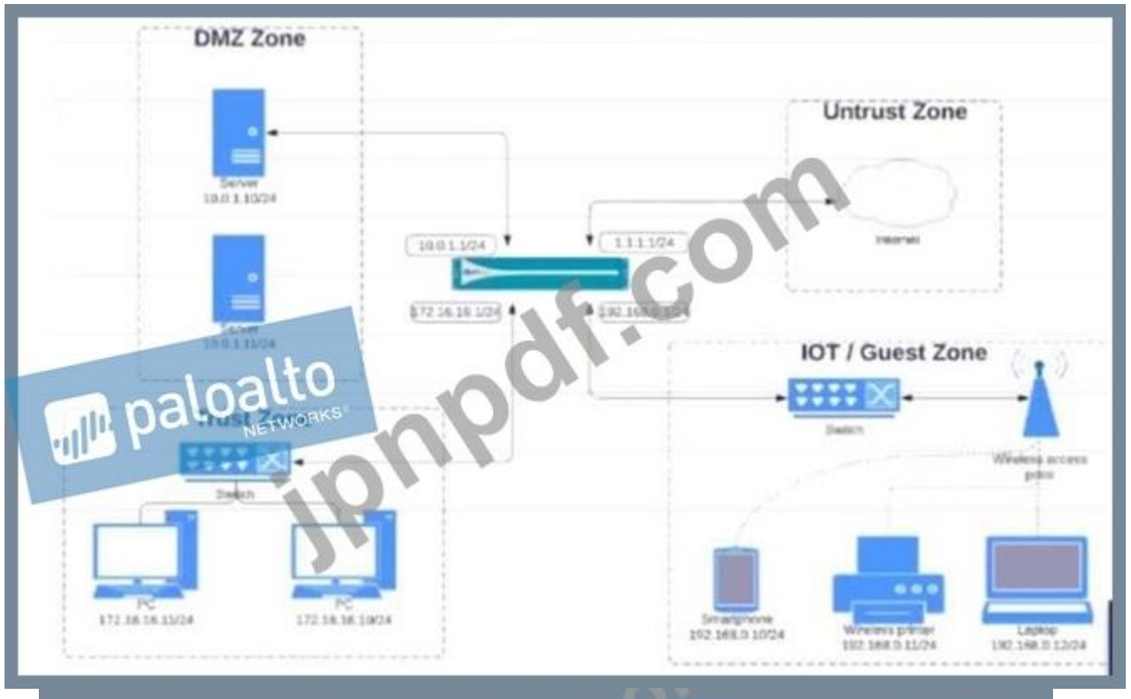
最新問題: **268**
ゼロトラストアーキテクチャの基本原則を最も適切に表している定義はどれですか？
A. 信頼、しかし真実
B. 決して信用せず、決して繋がらない
C. 常に接続して確認する
D. 決して信用せず、常に検証せよ
Answer: D (メーッセージを残す)

最新問題: **269**
ドメイン生成アルゴリズムで使用できる3つの要素は何ですか？ 3つ選択してください。）
A. 暗号鍵
B. 時刻
C. その他の固有値
D. URLカスタムカテゴリ
E. IPアドレス
Answer: (解答を表示する)
ドメイン生成アルゴリズム（DGA）は、悪意のあるコマンド＆コントロール（C2）通信チャネルを確立する際に、通常、多数のドメインを自動生成するために使用されます。DGAベースのマルウェア（Pushdo、BankPatch、CryptoLockerなど）は、多数の候補ドメインの中にアクティブなC2サーバーの場所を隠すことで、ブロックされるドメインの数を制限します。また、時間帯、暗号鍵、その他の固有の値などの要素に基づいてアルゴリズム的に生成することができます。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/threat-prevention/dns-security/domain-generation-algorithm-detection

最新問題: **270**
ローカルファイアウォールでタグを作成する際に編集できる設定項目はどれですか？
A. 優先
B. 色
国境
C. 場所
Answer: B (メーッセージを残す)

最新問題: **271**
ファイアウォールのGUIのどこで、既存のすべてのタグを表示できますか？
A. ネットワーク > タグ
B. ポリシー > タグ
C. モニター > タグ
D. オブジェクト > タグ
Answer: D (メーッセージを残す)

最新問題: **272**
ネットワーク図を考慮すると、信頼済みユーザーとゲストユーザーの両方が、SSH、Webブラウジング、およびSSLアプリケーションを使用して、一般的なインターネットおよびDMZサーバーにアクセスできるようにする必要があります。
どの政策が望ましい結果をもたらすのか？



A.

B.

C. 

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
04-A	none	universal	IOT-Guest	172.16.16.0/24	any	any	DMZ	any
	Trust		192.168.0.0/24				Untrust	

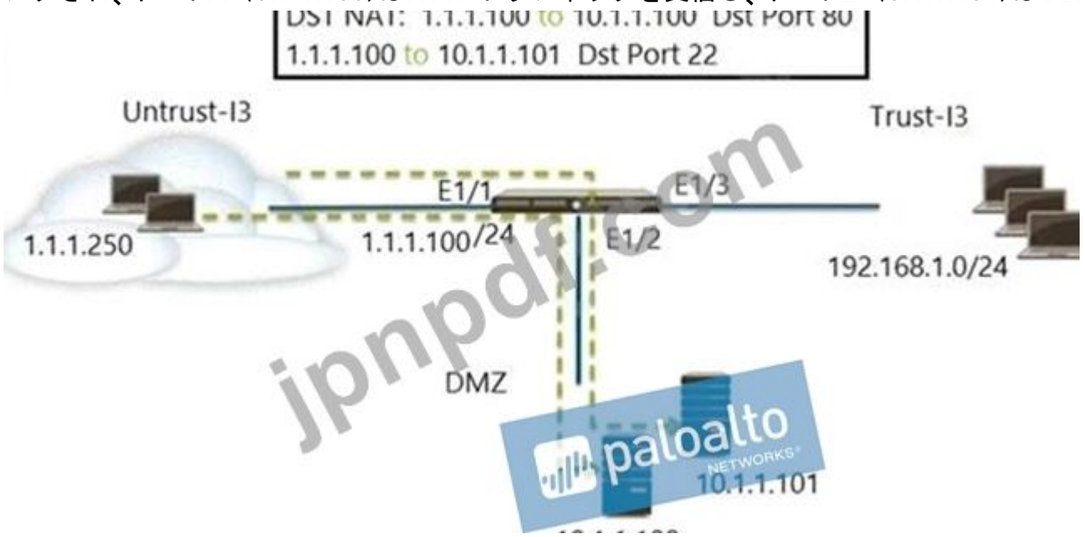
D. 

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS
01-A	none	universal	IOT-Guest	1.0/24	any	any	DMZ	1.1.1.0/
	Trust		172.16.16.0/12				Untrust	192.168

Answer: B (メーッセージを残す)

最新問題**: 273**
IEEE 802.1Q VLANには、どのインターフェースタイプが割り当てられますか？
A. トンネルインターフェース
B. レイヤ2サブインターフェース
C. レイヤ3サブインターフェース
D. ループバックインターフェース
Answer: B (メーッセージを残す)
IEEE 802.1Qは、イーサネットネットワークにおけるVLANタギングの標準規格です。Cisco IOSでは、VLANは通常、レイヤ2サブインターフェイスに割り当てられます。レイヤ2サブインターフェイスとは、物理インターフェイスを複数の仮想インターフェイスに分割できる論理インターフェイスです。各レイヤ2サブインターフェイスには固有のVLAN IDを割り当てることができ、VLANメンバーシップに基づいてトラフィックを分離および管理できます。

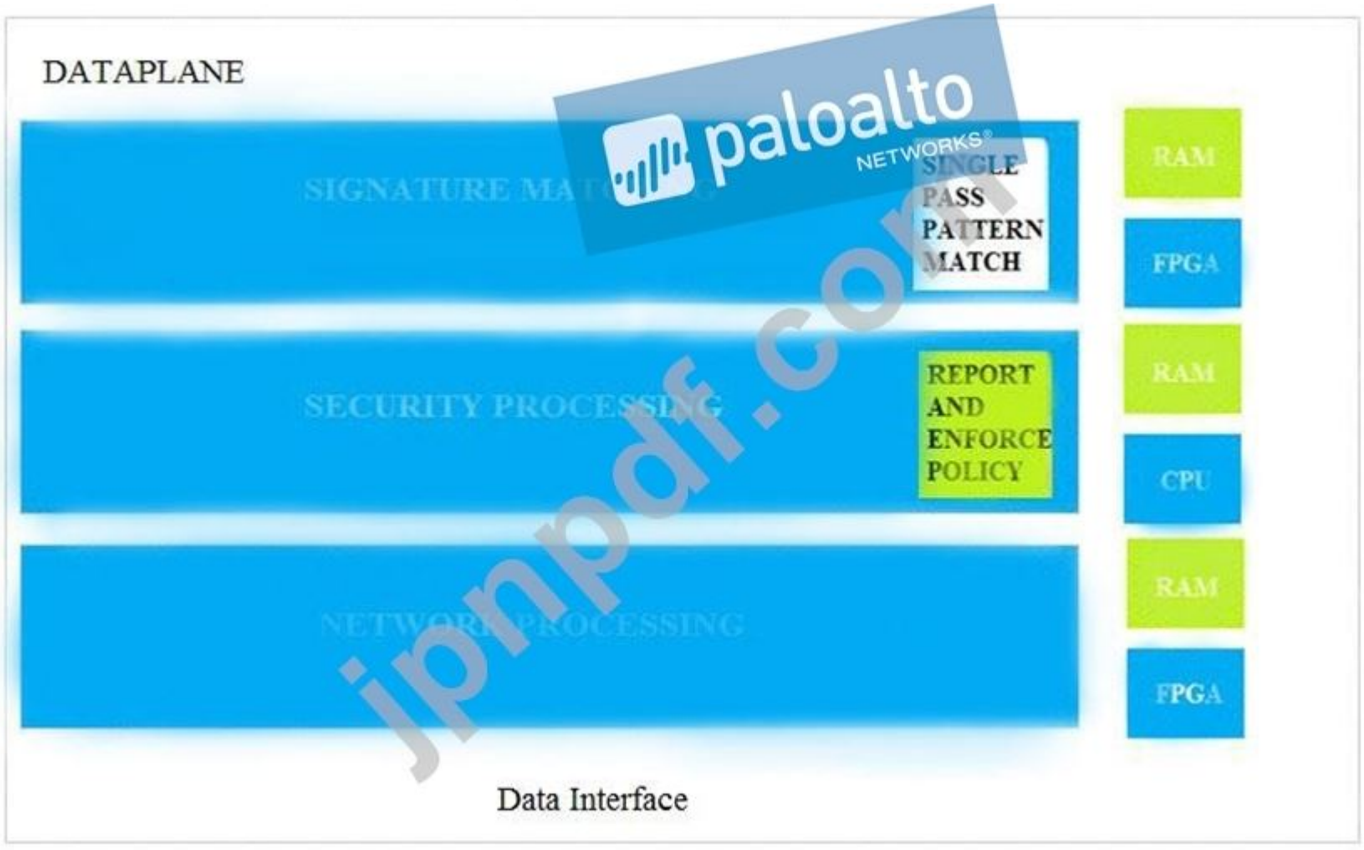
最新問題**: 274**
図を参照してください。管理者はDNATを使用して、2台のサーバーを1つのパブリックIPアドレスにマッピングしています。トラフィックはアプリケーションに基づいて特定のサーバーにルーティングされ、ホストA（10.1.1.100）はHTTPトラフィックを受信し、ホストB（10.1.1.101）はSSHトラフィックを受信します。



この構成を実現するには、どのセキュリティポリシールールを2つ選択すればよいですか？（2つ選択してください。）

A. DMZ (10.1.1.100、10.1.1.101) への不信 (任意)、ssh、ウェブブラウジング許可
B. DMZ (1.1.1.100) への接続を信頼しない (任意)、ssh - 許可
C. Untrust (Any) から Untrust (10.1.1.1)、ssh -Allow
D. DMZ (1.1.1.100) への不信 (任意)、ウェブブラウジング - 許可
E. 信頼しない (すべて) から信頼しない (10.1.1.1)、ウェブブラウジング - 許可
Answer: B,D (メーッセージを残す**)**

最新問題**: 275**
図に示すデータプレーンプロセッサ層のうち、Palo Alto Networksファイアウォール上でスパイウェアと脆弱性攻撃に対して均一なマッチングを提供する層はどれですか？

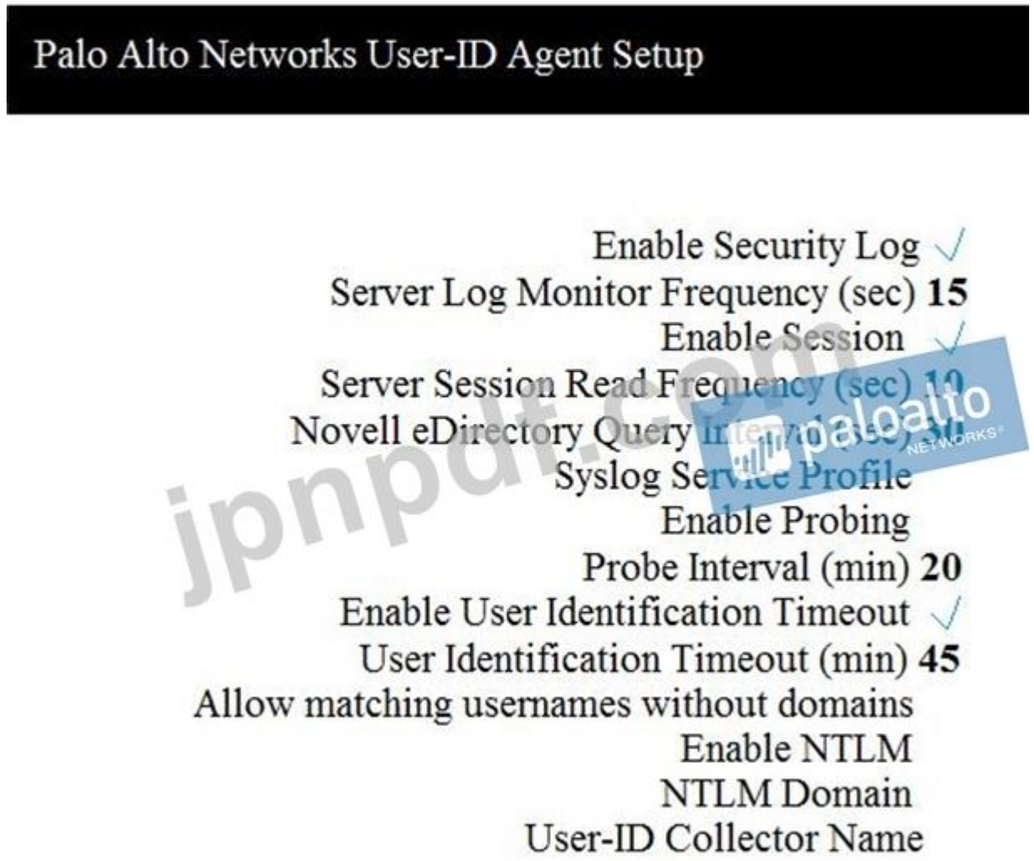


A. ネットワーク処理
B. 署名照合
C. セキュリティ処理
D. セキュリティマッチング
Answer: B (メーッセージを残す**)**

最新問題**: 276**
図に基づいて、サーバー監視パネルに表示される出力内容を正確に説明しているのはどの記述ですか？

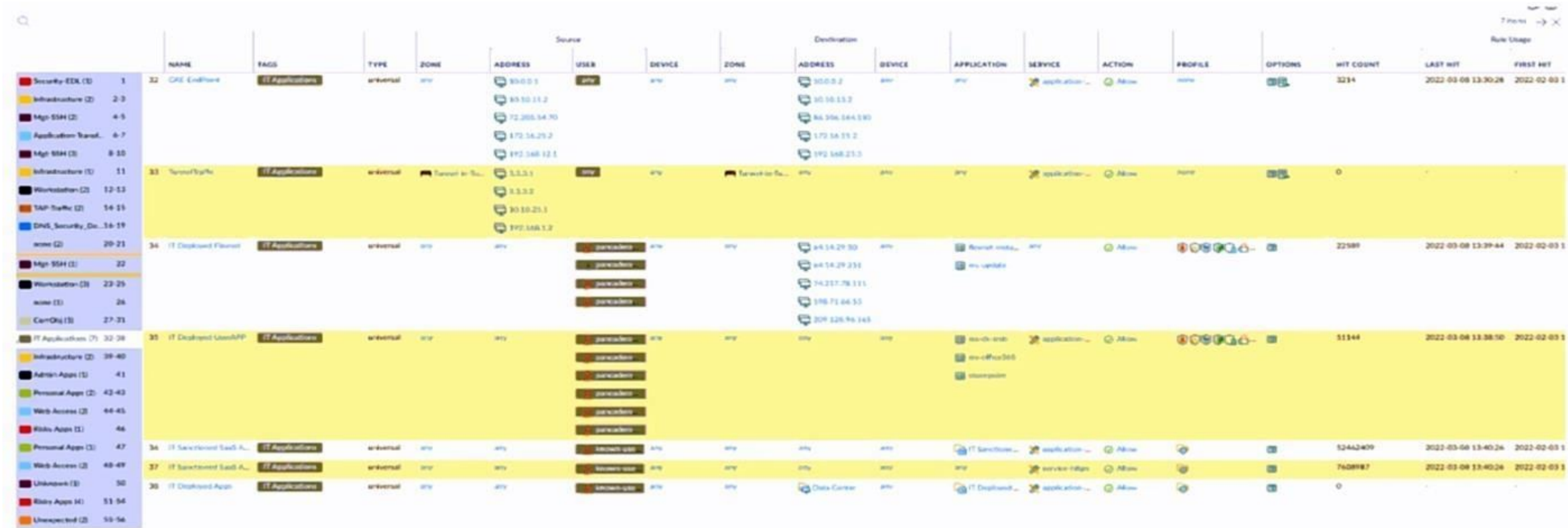
A. ホスト lab-client がユーザー ID エージェントによって検出されました。
B. ホスト lab-client がドメイン コントローラによって検出されました。
C. User-IDエージェントは、lab-clientというラベルの付いたファイアウォールに接続されています。
D. User-IDエージェントは、lab-clientというラベルの付いたドメインコントローラに接続されています。
Answer: D (メーッセージを残す)

最新問題**: 277**
表示されている設定項目のうち、デフォルト設定ではないものはどれですか？ 2つ選択してください。）



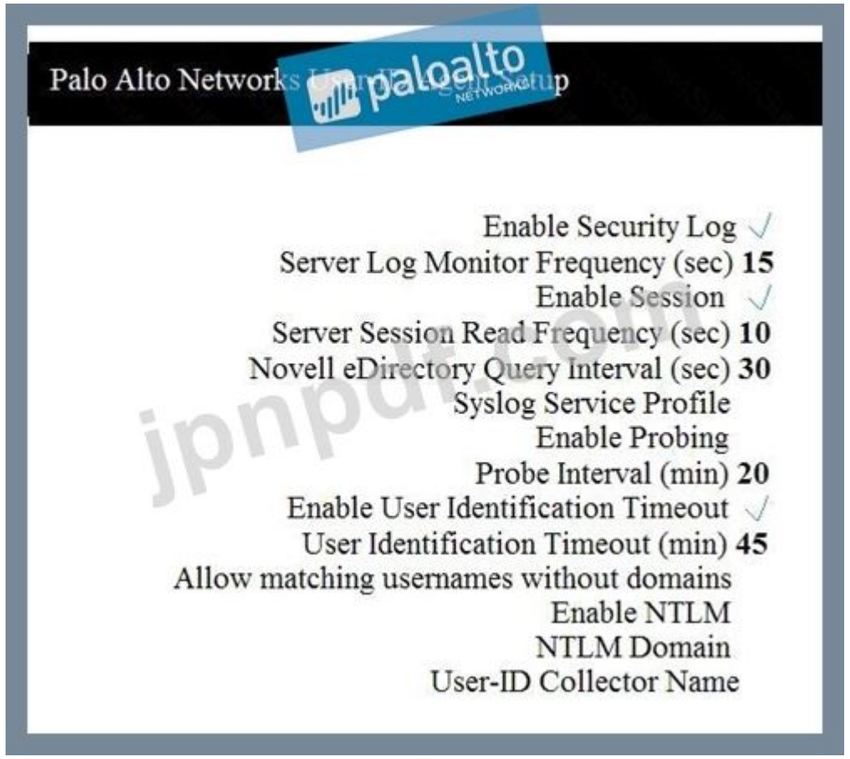
A. プロービングを有効にする
B. セキュリティログを有効にする
C. セッションを有効にする
D. サーバーログモニターの頻度（秒）
Answer: C,D (メーッセージを残す**)**

最新問題**: 278**
管理者が、以下のスクリーンショットに示されているセキュリティポリシールールを確認しています。表示されている情報について、正しい記述はどれですか？



A. 未使用ルールのハイライト表示にチェックが入っています。
B. このファイアウォールには7つのセキュリティポリシールールがあります。
C. 11個のルールが ｲンフラストラクチャ*」タグを使用しています。
D. ルールベースをグループとして表示する」にチェックが入っています。
Answer: D (メーッセージを残す)

最新問題**: 279**
表示されている設定項目のうち、デフォルト設定ではないものはどれですか？ 2つ選択してください。）

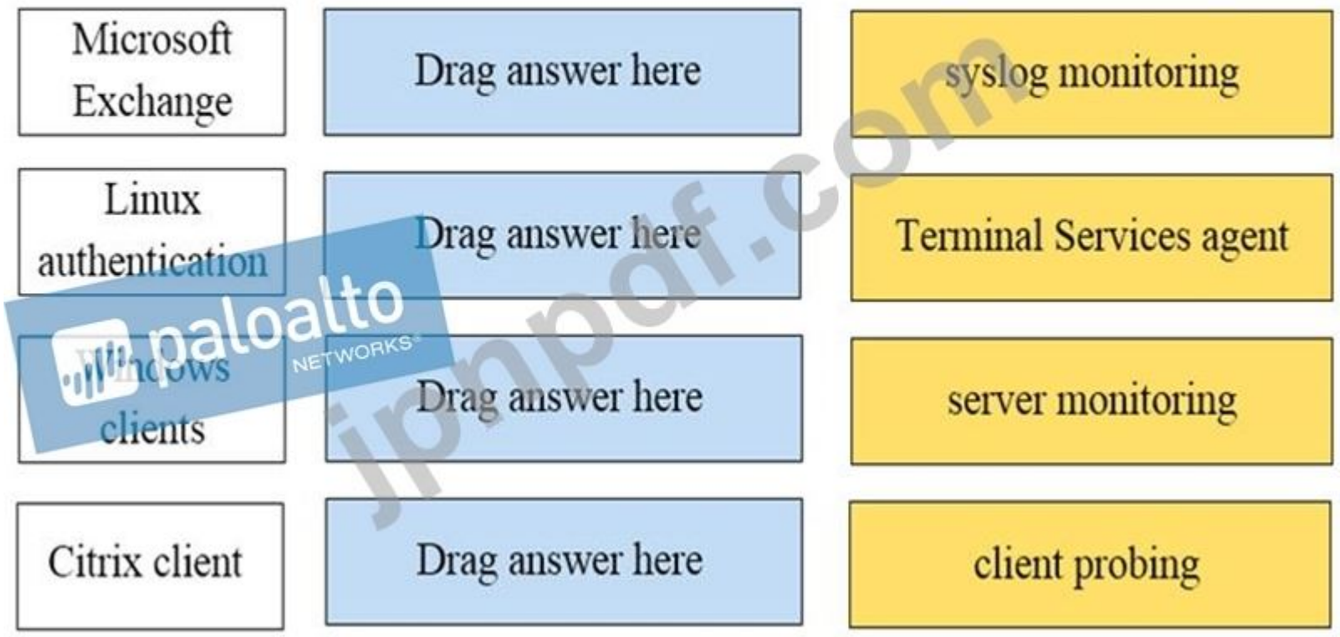


A. セッションを有効にする
B. プロービングを有効にする
C. セキュリティログを有効にする
D. サーバーログモニターの頻度（秒）
Answer: (解答を表示する**)**

最新問題**: 280**
PAN-OS 11.0のリリースに伴い、脆弱性セキュリティプロファイル内で新たに利用可能になるタブはどれですか？
A. 上級ルール
B. WildFire Inline ML
C. インラインクラウド分析
D. 脆弱性例外
Answer: D (メーッセージを残す**)**

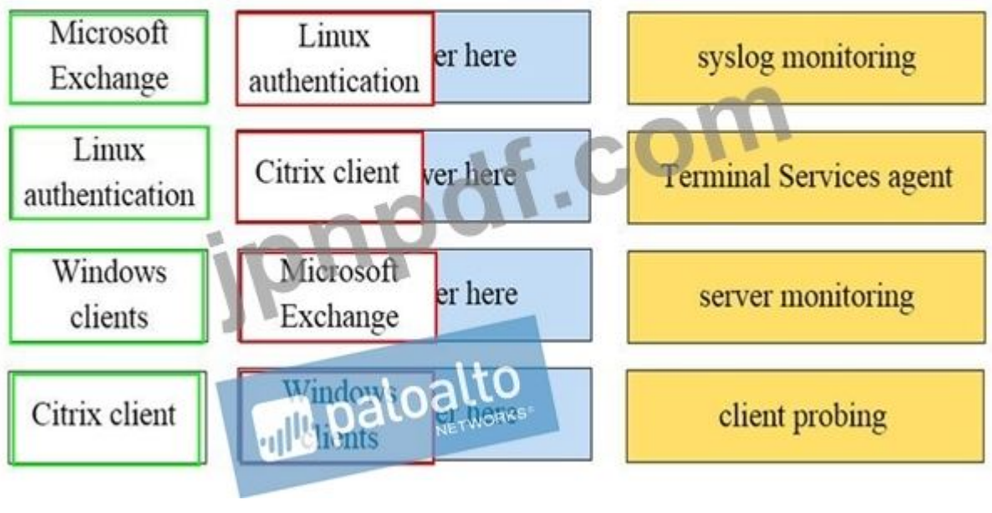
最新問題**: 281**
ネットワーク機器を適切なユーザーID技術に対応させてください。

Answer Area



Answer:

Answer Area



最新問題: **282**

セキュリティ管理者がApp-IDのアップデートを自動的にダウンロードしてインストールするように設定しました。同社は現在、App-IDでSuperApp_baseとして識別されるアプリケーションを使用しています。

コンテンツ更新通知によると、パロアルトネットワークスはSuperApp_chatとSuperApp_downloadというラベルの新しいアプリ署名を追加し、30日以内に展開する予定だ。

この情報に基づくと、30日経過後、スーパーアプリのトラフィックはどのように影響を受けるのでしょうか？
A. SuperApp_chatおよびSuperApp_downloadに一致するすべてのトラフィックは、SuperAppベースのアプリケーションに一致しなくなったため拒否されます。
B. アプリは自動的にダウンロードおよびインストールされたため、影響はありません。
C. ファイアウォールがルールをApp-IDインターフェースに自動的に追加するため、影響はありません。
D. SuperApp_base、SuperApp_chat、SuperApp_download に一致するすべてのトラフィックは、セキュリティ管理者がアプリケーションを承認するまで拒否されます。
Answer: (解答を表示する**)**
説明
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**: 283**
ゼロトラストアーキテクチャの基本原則を最も適切に表している定義はどれですか？
A. 決して信用せず、決して繋がらない
B. 常に接続して確認する
C. 決して信用せず、常に検証せよ
D. 信頼、しかし真実
Answer: C (メーッセージを残す**)**
参照：
https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

最新問題**: 284**
有効な企業ユーザー名とそれに関連付けられたパスワードが送信されたかどうかを確認するために、URLフィルタリングセキュリティプロファイル内でどのユーザー認証情報検出方法を適用すべきでしょうか？
A. ドメイン認証情報
B. IPユーザー
C. 有効なユーザー名が検出されました ログの重大度
D. グループマッピング
Answer: (解答を表示する**)**

最新問題**: 285**
内部ゾーンのすべてのユーザーは、DMZゾーン内のサーバーへのTelnetアクセスのみを許可される必要があります。このタイプのアクセスのみを許可するセキュリティポリシールールの空欄2つを埋めてください。


2つ選択してください。
A. アプリケーション = "Telnet"
B. アプリケーション＝「任意」
C. サービス - "application-default"

D. サービス＝ 任意」
Answer: A,C (メーッセージを残す**)**

最新問題**: 286**
アンチスパイウェアプロファイル内で有効な選択肢を2つ挙げてください。2つ選択してください。）
A. デフォルト
B. 拒否する
C. ランダム早期ドロップ
D. ドロップ
Answer: A,D (メーッセージを残す**)**
拒否はポリシーアクションであり、ランダムな早期ドロップはDoS防御の内部動作の一部である。

最新問題**: 287**
どの機能へのアクセスにPAN-OSフィルタリングライセンスが必要ですか？
A. PAN-DBデータベース
B. DNSセキュリティ
C. カスタムURLカテゴリ
D. URL外部動的リスト
Answer: A (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/getting-started/activate-licenses-and-subscriptions.html

最新問題**: 288**
アプリケーションフィルターを設定する際に選択可能な属性を表示するオプションはどれですか？
A. カテゴリ、サブカテゴリ、技術、特性
B. カテゴリ、サブカテゴリ、技術、リスク、特性
C. 名称、カテゴリー、技術、リスク、特性
D. カテゴリ、サブカテゴリ、リスク、標準港、およびテクノロジー
Answer: (解答を表示する**)**
説明/参考資料: https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/objects/objects-application-filters

最新問題**: 289**
App-IDの更新プロセスにおいて、既存のポリシー規則がApp-IDの更新によって影響を受けるかどうかを判断できるのはどの時点ですか？
A. 動的更新ウィンドウで 今すぐ確認」をクリックした後
B. ファイアウォール設定をコミットした後

C. アップデートをインストールした後
D. アップデートをダウンロードした後
Answer: D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/device/device-dynamic-updates