PaloAltoNetworks.PCNSE.v2023-01-06.q209

試験コード:	PCNSE
試験名称:	Palo Alto Networks Certified Network Security Engineer Exam
認定資格:	Palo Alto Networks
無料問題数:	209
バージョン:	v2023-01-06
アクセス数:	3271
ページビュー数:	2090
https://www.jpnpdf.com/PaloAltoNetworks.PCNSE.v2023-01-06.q209-mondaishu.html	

最新問題: **1**
管理者は、Panoramaと複数のPalo AltoNetworksNGFWを使用しています。すべてのデバイスを最新のPAN-OSソフトウェアにアップグレードした後、管理者はファイアウォールからPanoramAへのログ転送を有効にします。
ファイアウォールからの既存のログはPanoramAに表示されません。
ファイアウォールが既存のログをPanoramaに送信できるようにするアクションはどれですか？
A. インポートオプションを使用して、ログをパノラマにプルします。
B. CLIコマンドは、既存のログをPanoramaに転送します。
C. ACCを使用して、既存のログを統合します。
D. ログデータベースはファイアウォールからエクスポートし、Panoramaに手動でインポートする必要があります。
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewall-log-forwarding-to-panorama
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/migrate-panorama-logs-to-new-ログ形式

最新問題: **2**
管理者は、すべてのポートでトラフィックを復号化するSSL復号化ルールを作成します。管理者は、アプリケーションDNS、SSL、およびWebブラウジングのみを許可するセキュリティポリシールールも作成します。
管理者は3つの暗号化されたBitTorrent接続を生成し、トラフィックログをチェックします。3つのエントリがあります。最初のエントリは、アプリケーション不明としてドロップされたトラフィックを示しています。次の2つのエントリは、アプリケーションSSLとして許可されるトラフィックを示しています。
2番目以降の暗号化されたBitTorrent接続がSSLとして許可されないようにするアクションはどれですか？
A. アクション ‟No-Decrypt」を使用して暗号化されたBitTorrentトラフィックに一致する復号化ルールを作成し、そのルールを復号化ポリシーの先頭に配置します。
B. アプリケーション ‟暗号化されたBitTorrent」に一致するセキュリティポリシールールを作成し、そのルールをセキュリティポリシーの一番上に配置します。

C. ファイアウォールのキャッシュ除外オプションを無効にします。
D. サポートされていないサイファーを使用してトラフィックをブロックする復号化プロファイルを作成し、プロファイルを復号化ルールに添付します。
Answer: D (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRtCAK
サポートしていない暗号スイートを使用するセッションをブロックします。[SSLプロトコル設定]タブで許可する暗号スイート（暗号化アルゴリズム）を構成します。ユーザーが弱い暗号スイートを持つサイトに接続することを許可しないでください。

最新問題**: 3**
「ドメインクレデンシャルフィルター」方式を使用してファイアウォールがクレデンシャルフィッシング防止用に構成されている場合、どのログインがクレデンシャルの盗難として検出されますか？
A. ログインしているユーザーのIPアドレスにマッピングします。
B. 有効な企業ユーザー名と一致するユーザー名の最初の4文字。
C. 同じユーザーの企業ユーザー名とパスワードを使用します。
D. 有効な企業ユーザー名をマーチングします。
Answer: A (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-entionリファレンス：
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/crede phishing-prevention

最新問題**: 4**
セキュリティポリシールールは、脆弱性保護プロファイルと「拒否」アクションで構成されます。
これにより、一致したトラフィックの構成が発生するアクションはどれですか。
A. 脆弱性シグニチャが検出されない限り、設定は一致したセッションを許可します。「拒否」アクションは、関連する脆弱性保護プロファイルで定義された重大度ごとに定義されたアクションに優先します。
B. 構成は有効です。これにより、ファイアウォールは一致したセッションを拒否します。セキュリティポリシールールのアクションが「拒否」に設定されている場合、構成されたセキュリティプロファイルは効果がありません。
C. 構成が無効です。アクションが「拒否」に設定されている場合、「プロファイル設定」セクションはグレー表示されます。
D. 設定が無効です。これにより、ファイアウォールはこのセキュリティポリシールールをスキップします。コミット中に警告が表示されます。
Answer: A (メーッセージを残す**)**

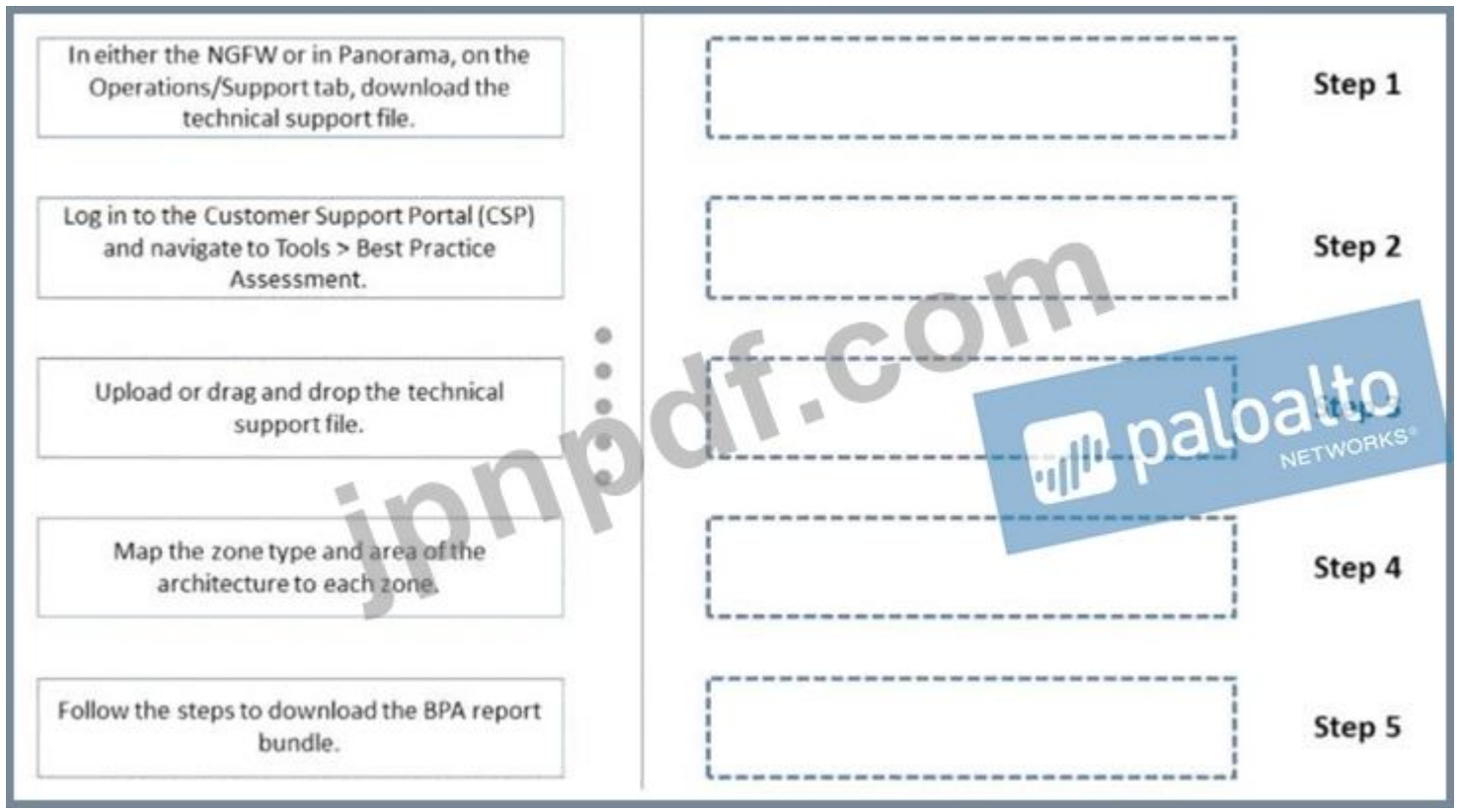
最新問題**: 5**
ネットワーク管理者がSSL/TLSサービスプロファイルに証明書を使用したい管理者はどのタイプの証明書を使用する必要がありますか？
A. クライアント証明書
B. 認証局（CA）証明書
C. マシン証明書
D. サーバー証明書
Answer: B (メーッセージを残す**)**

最新問題: **6**
アクティブ/アクティブ高可用性ペアを構成する場合、どの2つのリンクを使用できますか？ 2つ選択してください）
A. HA2バックアップ
B. HSCI-C
C. HA3
D. コンソールバックアップ
Answer: A,C (メーッセージを残す**)**

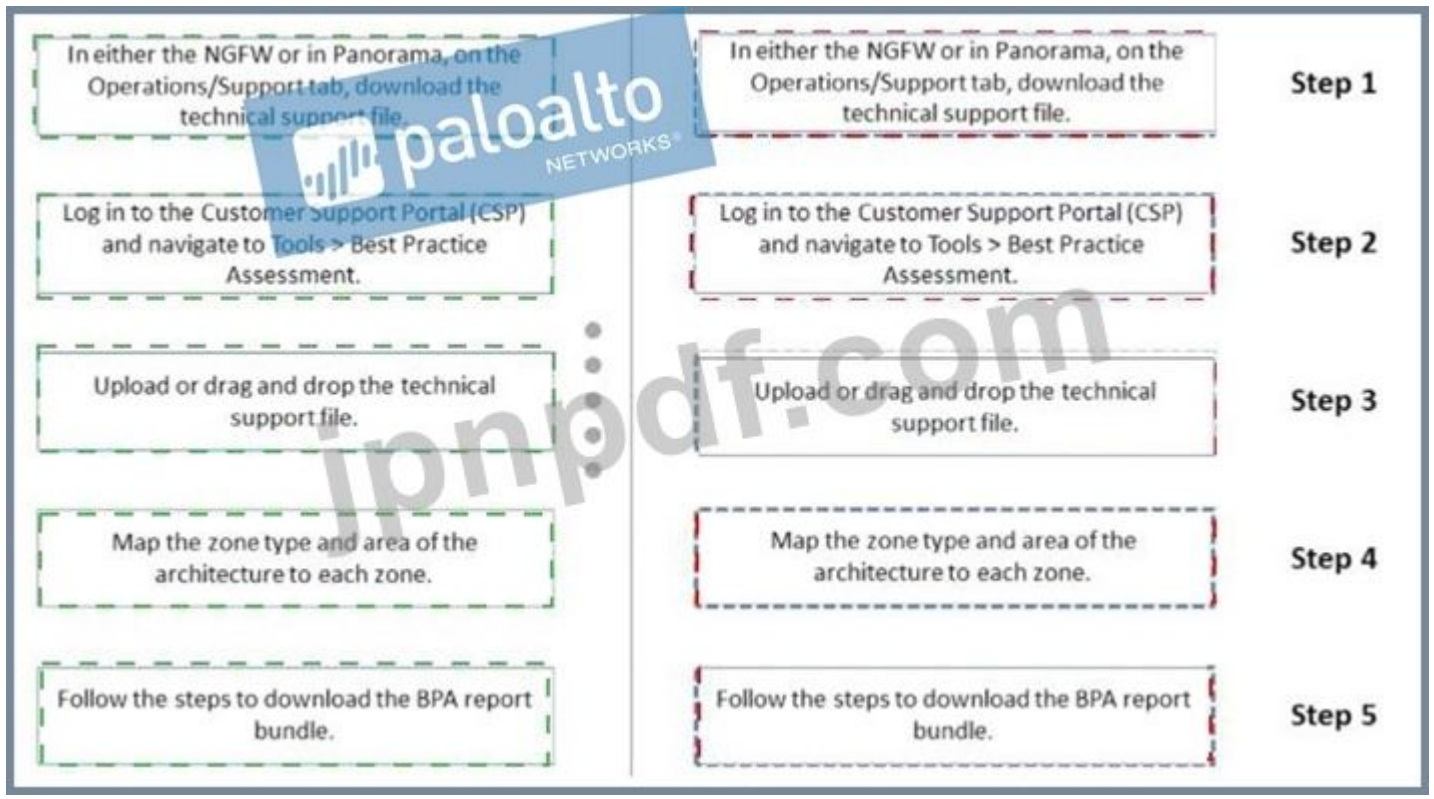
最新問題: **7**
管理者がWebサイトの証明書を持っていない場合、ユーザーがHTTP $）Webサイトを参照するときに、どのSSL復号化モードでパロアルトネットワークNGFWが検査できるようになりますか？
A. SSL転送プロキシ
B. SSLインバウンド検査
C. TLS双方向プロキシ
D. SSLアウトバウンド検査
Answer: A (メーッセージを残す**)**
https://live.paloaltonetworks.com/t5/Learning-Articles/Difference-Between-SSL-Forward-Proxy- and-Inbound-Inspection / ta-p / 55553

最新問題: **8**
Palo Alto Networks NGFWにタグを動的に登録する方法はどれですか？
A. ファイアウォールまたはUser-IDエージェントまたはready-onlyドメインコントローラー（RODC）上のRestfulAPIまたはVMwareAPI
B. ファイアウォールまたはユーザーIDエージェント上のRestfulAPIまたはVMwareAPI
C. ファイアウォールまたはユーザーIDエージェントまたはCLI上のXMLAPIまたはVMwareAPI
D. NGFWまたはUser-IDエージェント上のXMLAPIまたはVM監視エージェント
Answer: (解答を表示する**)**
説明/参照 :https ://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/register-ip-addresses-and-tags-dynamicly

最新問題: **9**
以下は、ファイアウォールとパノラマ構成でベストプラクティス評価を作成するためのワークフローの手順です。手順を順番に並べます。



Answer:



説明

手順1.NGFWまたはPanoramaの[Operations/Support]タブで、テクニカルサポートファイルをダウンロードします。

ステップ2.カスタマーサポートポータル (CSP)にログインし、[ツール]>[ベストプラクティスの評価]に移動します。

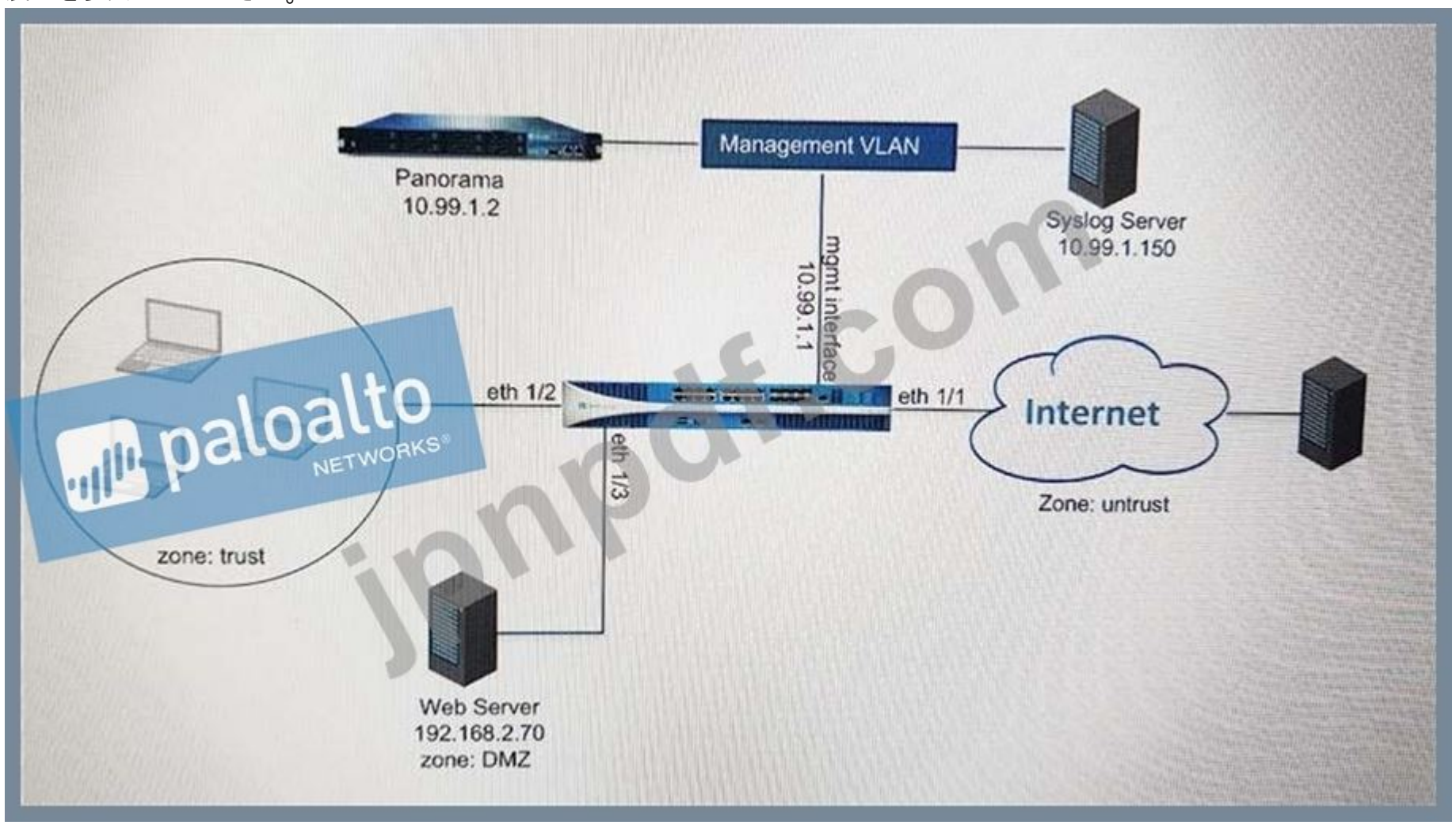
ステップ3.テクニカルサポートファイルをアップロードまたはドラッグアンドドロップします。

ステップ4.アーキテクチャのゾーンタイプとエリアを各ゾーンにマッピングします。

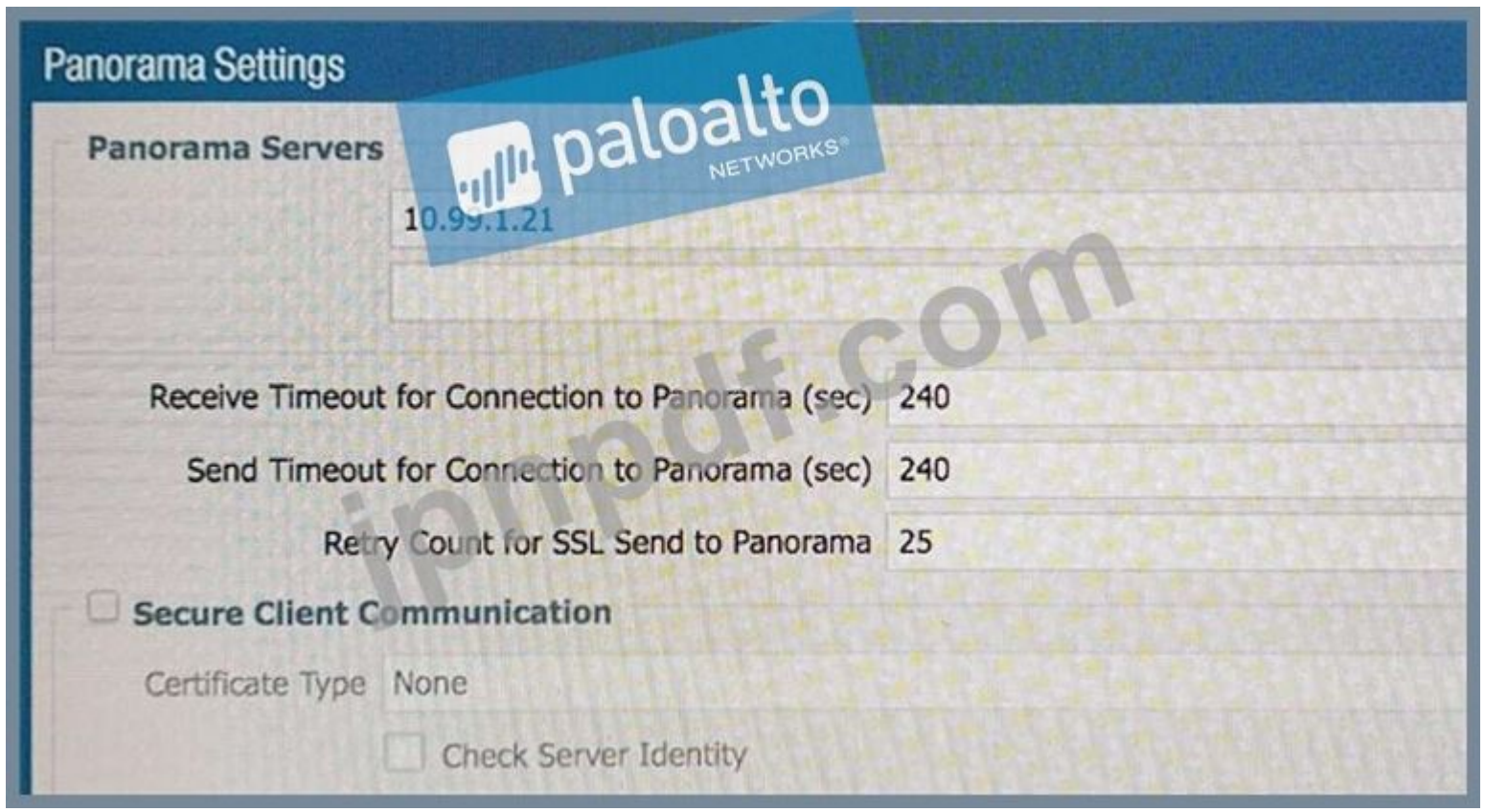
ステップ5.ステップに従って、BPAレポートバンドルをダウンロードします。

参照：
https://www.paloaltonetworks.com/resources/videos/how-to-run-a-bpa

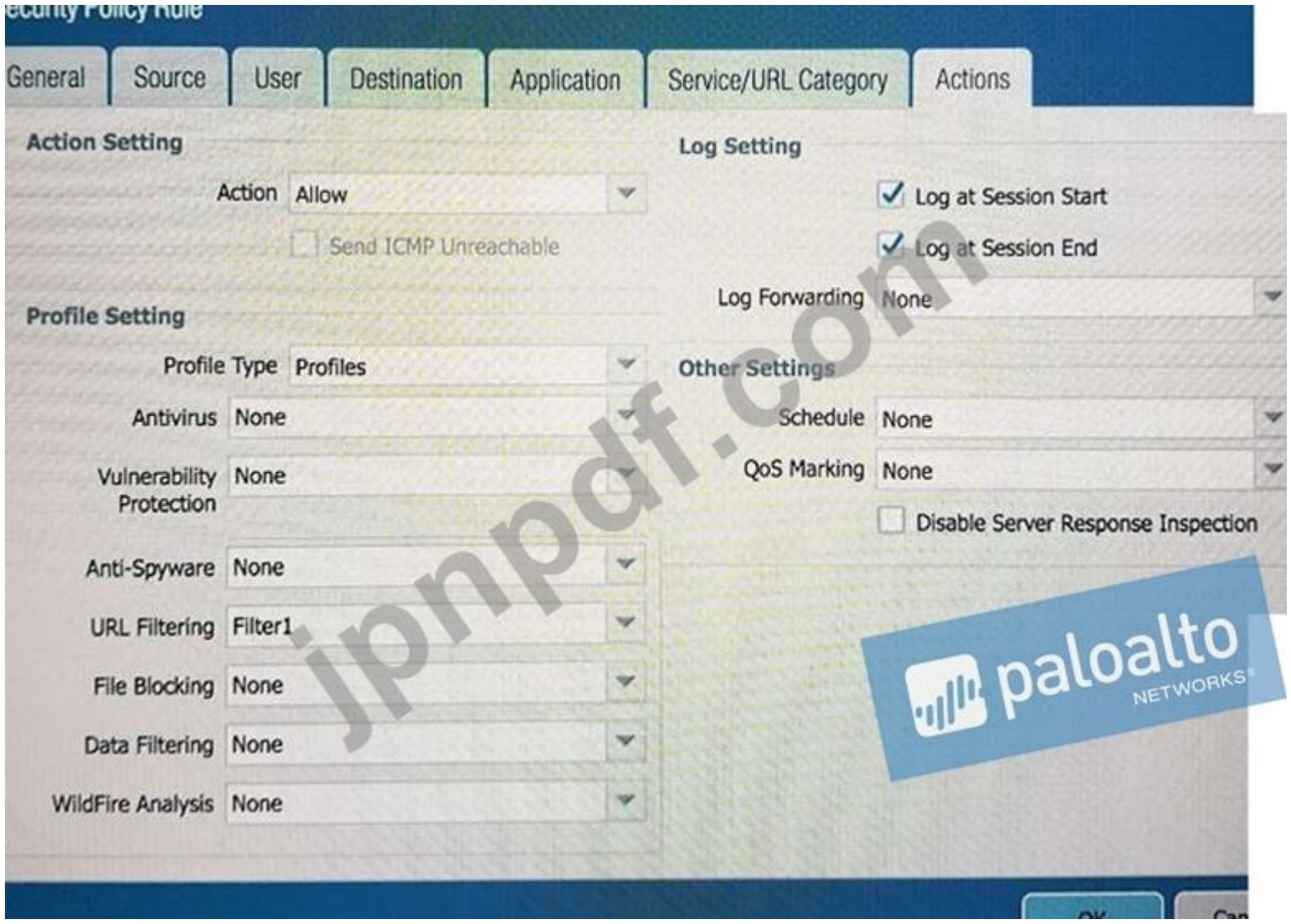
最新問題: 10
展示を参照してください。



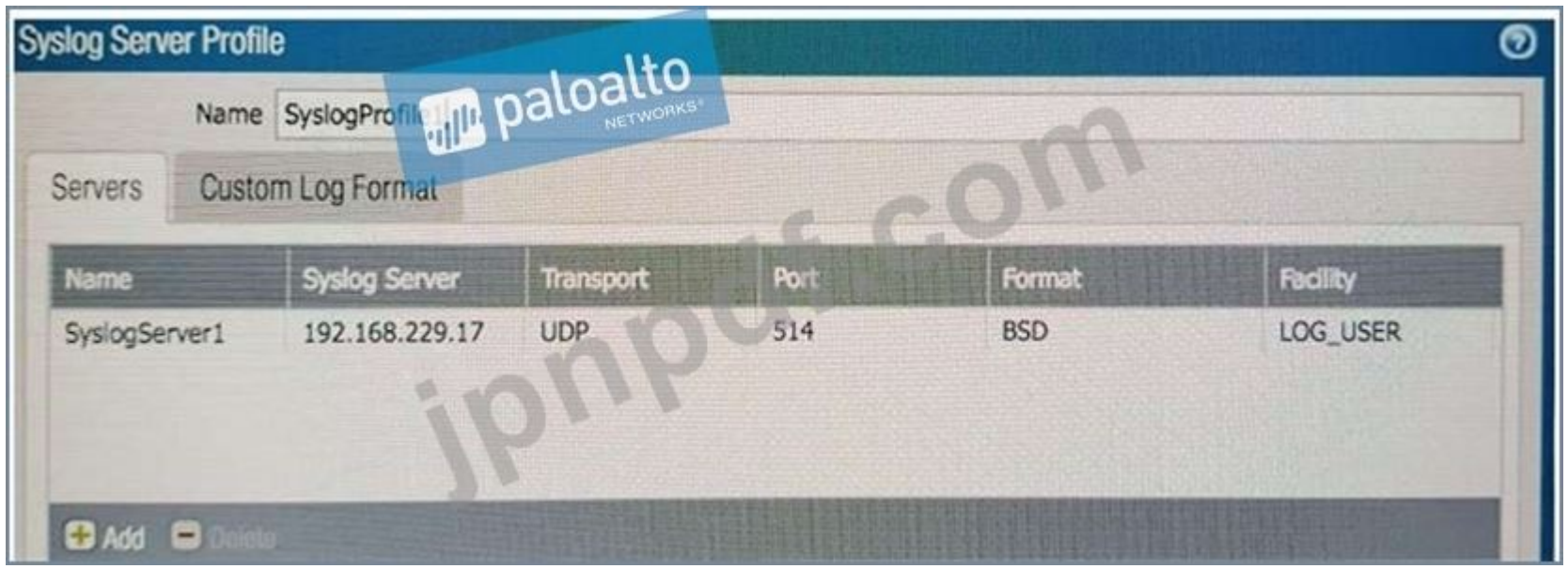
管理者は、PanoramaでPalo AltoNetworksNGFWからのトラフィックログを表示できません。構成の問題はファイアウォール側にあるようです。構成が正しいかどうかを確認するために、パロアルトネットワークスNGFWのどこが最適ですか？
A）


Panorama Settings
Panorama Servers
10.99.1.21
Receive Timeout for Connection to Panorama (sec) 240
Send Timeout for Connection to Panorama (sec) 240
Retry Count for SSL Send to Panorama 25
Secure Client Communication
Certificate Type None
Check Server Identity

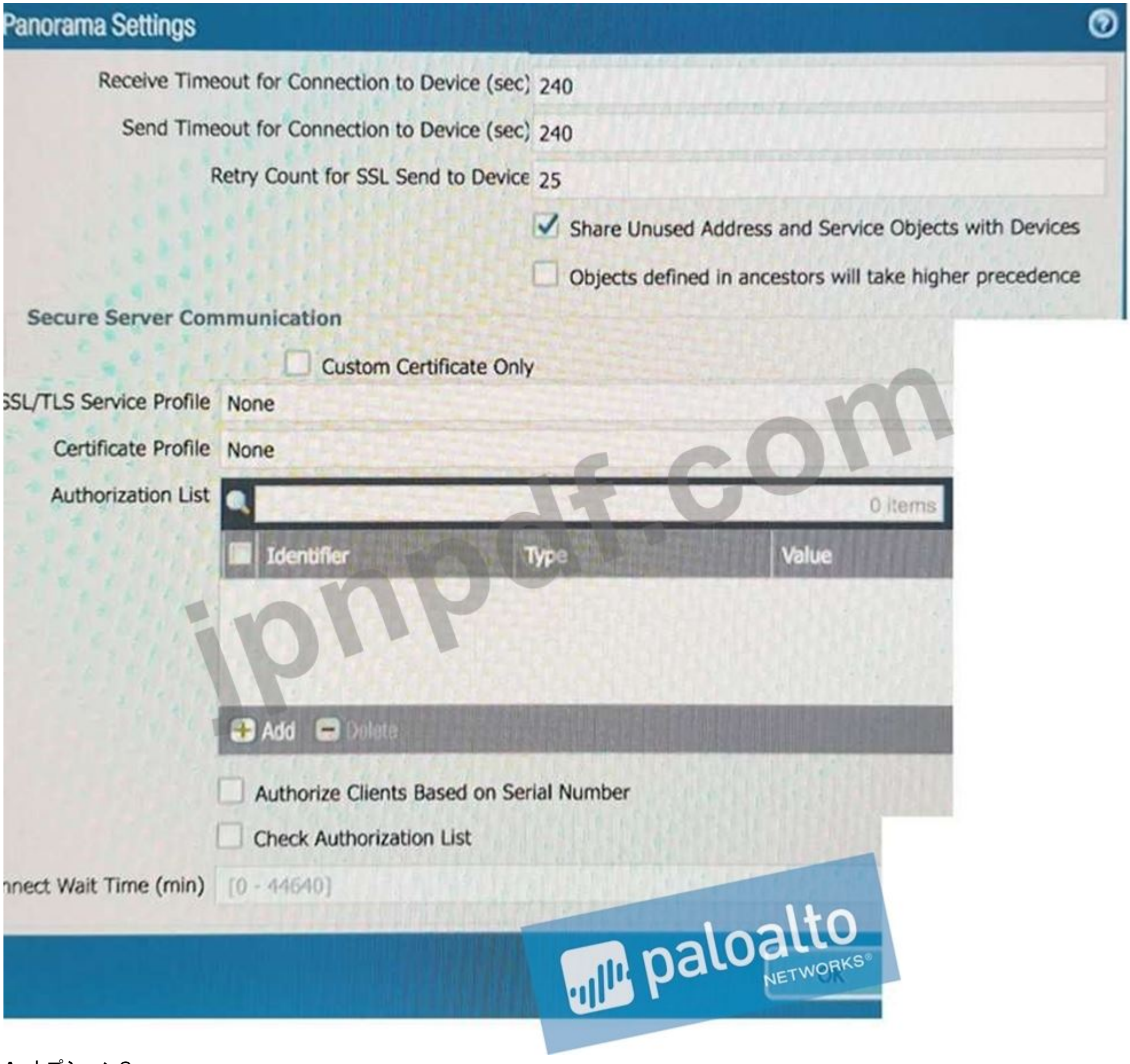
B)


General
Source
User
Destination
Application
Service/URL Category
Actions
Action Setting
Action
Allow
Send ICMP Unreachable
Profile Setting
Profile Type
Profiles
Antivirus
None
Vulnerability Protection
None
Anti-Spyware
None
URL Filtering
Filter1
File Blocking
None
Data Filtering
None
WildFire Analysis
None
Log Setting
Log at Session Start
Log at Session End
Log Forwarding
None
Other Settings
Schedule
None
QoS Marking
None
Disable Server Response Inspection
paloalto NETWORKS
jpnpdf.com

C)


Syslog Server Profile
Name
Servers
Custom Log Format
Name
Syslog Server
Transport
Port
Format
Facility
SyslogServer1
192.168.229.17
UDP
514
BSD
LOG_USER
Add
Delete
paloalto NETWORKS
jpnpdf.com

D)



A. オプションC
B. オプションA

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

最新問題**: 11**
パケットフロープロセス中に、アプリケーションの識別で実行される2つのプロセスはどれですか。（選ぶ2。）
A. コンテンツ検査からアプリケーションが変更されました
B. アプリケーションオーバーライドポリシーの一致
C. セッションアプリケーションが識別されました。
D. パターンベースのアプリケーション識別
Answer: B,C (メーッセージを残す**)**

最新問題**: 12**
パロアルトネットワークスNGFWは、分析のためにファイルをWildFireに送信しました。分析のために5分のウィンドウを想定します。ファイアウォールは、5分ごとに判定をチェックするように構成されています。
ファイアウォールはどのくらいの速さで評決を受け取りますか？
A. 15分以上
B. 5分
C. 10〜15分
D. 5〜10分
Answer: (解答を表示する**)**
新しいWildFireシグニチャは5分ごとに利用可能であるため、この設定により、ファイアウォールはアベイラビリティの1分以内にこれらのシグニチャを確実に取得します。」
つまり、WildFireが06:00 PMに評決をチェックする場合、次に06:05にチェックされます。ただし、06 :06にファイルを送信すると、WildFireは06:10にチェックされますが、評決は06:11に行われます。06:15にWildFireによってフェッチされます。つまり、送信してから9分です。したがって、提出の時間に応じて5〜10分です。

最新問題**: 13**
展示を参照してください。
フォワードトラスト証明書として使用できる証明書はどれですか？
A. デフォルトの信頼できる認証局からの証明書
B. ドメインルート証明書
C. ドメインサブCA
D. フォワードトラスト
Answer: C (メーッセージを残す**)**

最新問題**: 14**
パノラマのテンプレートオブジェクト内で定義されている3つの設定はどれですか？ 3つ選択してください。）
A. アプリケーションのオーバーライド

B. セキュリティ
C. インターフェース
D. 仮想ルーター
E. セットアップ
Answer: C,D,E (メーッセージを残す)

最新問題**: 15**
仮想ルーターでは、どのオブジェクトにすべての潜在的なルートが含まれていますか？
A. MIB
B. RIB
C. SIP
D. FIB
Answer: B (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers

最新問題**: 16**
ある会社が、VLANトランクリンク上の2つのコアスイッチの間にPA-3060ファイアウォールを設置したいと考えています。各VLANを独自のゾーンに割り当て、タグなし（ネイティブ）トラフィックを独自のゾーンに割り当てる必要があります。
複数のVLANを別々のゾーンに区別するオプションはどれですか。
A. VLANごとにVLANオブジェクトを作成し、各VLANIDに一致するVLANインターフェイスを割り当てます。追加のVLANごとに繰り返し、タグなしトラフィックにはVLANID0を使用します。各インターフェース/サブインターフェースを一意のゾーンに割り当てます。
B. 2つのV-Wireサブインターフェイスを使用してV-Wireオブジェクトを作成し、V-Wireオブジェクトの[TagAllowed]フィールドに1つのVLANIDのみを割り当てます。追加のVLANごとに繰り返し、タグなしトラフィックにはVLANID0を使用します。各インターフェース/サブインターフェースを一意のゾーンに割り当てます。
C. それぞれが単一のVLANIDと共通の仮想ルーターに割り当てられるレイヤー3サブインターフェースを作成します。
物理レイヤー3インターフェースは、タグなしトラフィックを処理します。各インターフェース/サブインターフェースを一意のゾーンに割り当てます。インターフェイスにIPアドレスを割り当てないでください。
D. 2つのV-Wireインターフェイスを使用してV-Wireオブジェクトを作成し、V-Wireオブジェクトの[TagAllowed]フィールドに「0-4096」の範囲を定義します。
Answer: (解答を表示する)

最新問題**: 17**

管理者は、Panoramaと複数のPalo AltoNetworksNGFWを使用しています。すべてのデバイスを最新のPAN-OS®ソフトウェアにアップグレードした後、管理者はファイアウォールからPanoramAへのログ転送を有効にします。ファイアウォールからの既存のログはPanoramAに表示されません。
ファイアウォールが既存のログをPanoramaに送信できるようにするアクションはどれですか？
A. インポートオプションを使用して、ログをパノラマにプルします。
B. CLIコマンドは、既存のログをPanoramaに転送します。
C. ACCを使用して、既存のログを統合します。
D. ログデータベースはファイアウォールからエクスポートし、Panoramaに手動でインポートする必要があります。
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/management-features/pa-7000-series-firewall-log-forwarding-to-panorama

最新問題**: 18**
管理者が過去30日間に検出された脅威など、一定期間のトラフィックの傾向を確認できるツールはどれですか。
A. セッションブラウザ
B. アプリケーションコマンドセンター
C. TCPダンプ
D. パケットキャプチャ
Answer: (解答を表示する**)**
説明/参照 :https ://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Command-Center-ACC/ta-p/67342

最新問題**: 19**
ファイアウォールは、人気のあるアプリケーションをunknown-tcpとして識別します。
アプリケーションを識別するために使用できる2つのオプションはどれですか？ 2つ選択してください。）
A. カスタムアプリケーションを作成します。
B. カスタムアプリケーションサーバーのカスタムオブジェクトを作成して、カスタムアプリケーションを識別します。
C. Apple-IDリクエストをパロアルトネットワークスに送信します。
D. カスタムアプリケーションを識別するためのセキュリティポリシーを作成します。
Answer: A,D (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applications

最新問題**: 20**
仮想ルーターでは、どのオブジェクトにすべての潜在的なルートが含まれていますか？
A. MIB
B. RIB
C. SIP
D. FIB
Answer: B (メーッセージを残す**)**
参照 :https ://www.google.com/url？

sa = t&rct = j&q = &esrc = s&source = web&cd = 10&ved = 0ahUKEwiOkbfYzPzXAhVnEJoKHcwVCg4QFghiMAk
&url = https%3A%2F%
2Flive.paloaltonetworks.com%2Ftwzvq79624%2Fattachments%2Ftwzvq79624%2Fdocumentation_tk b%2F487%2F1%2FRoute
%2520Redistribution%2520and%2520Filtering%2520TechNote%2520-
%2520Rev%2520B。pdf&usg = AOvVaw0H9qgaJK0oI2xjIJBNo1Km

最新問題: **21**
新しいURLカテゴリが原因で、管理者のデバイスグループのコミットプッシュが減少しています。管理者はこの問題をどのように修正する必要がありますか？
A. URLシードタイルがダウンロードされ、ファイアウォールでアクティブ化されていることを確認します
B. アラートに新しいカテゴリアクションを変更してください」と設定を再度プッシュします
C. ファイアウォールアプリと脅威のバージョンをPanoramaのバージョンと一致するように更新します
D. ファイアウォールがURLクラウドと通信できることを確認します
Answer: C (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw

最新問題: **22**
パロアルトネットワークスNGFWを通過するユーザーのトラフィックが到達する場合があります
http://www.company.com。それ以外の場合、セッションはタイムアウトになります。NGFWは、ユーザーのトラフィックが次の場所に移動したときに一致するPBFルールで構成されています。
http://www.company.com。
ネクストホップがダウンした場合にファイアウォールを自動的に無効にする方法を教えてください。
A. 問題のPBFルールでフェイルオーバーのアクションを使用してモニタープロファイルを作成および追加します。
B. 仮想ルーターのデフォルトルートでネクストホップゲートウェイのパス監視を構成します。
C. ファイアウォールの外部インターフェイスのリンク監視プロファイルを有効にして構成します。
D. 問題のPBFルールでWaitRecoverのアクションを使用してモニタープロファイルを作成して追加します。
Answer: (解答を表示する**)**

最新問題: **23**
ネットワーク管理者は、SSL/TLSサービスプロファイルに証明書を使用したいと考えています。
管理者はどのタイプの証明書を使用する必要がありますか？
A. 認証局（CA）証明書
B. クライアント証明書
C. マシン証明書
D. サーバー証明書
Answer: (解答を表示する**)**
SSL / TLSサービスプロファイルでは、CA証明書ではなく、署名付き証明書のみを使用してくださ
い。https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service-profile.html

最新問題: **24**

基本的なWildFireサービスの一部として分析のためにWildFireに転送できる3つのファイルタイプはどれですか？ 3つ選択してください。）
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar
Answer: D,E,F (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

最新問題**: 25**
[展示]ボタンをクリックします

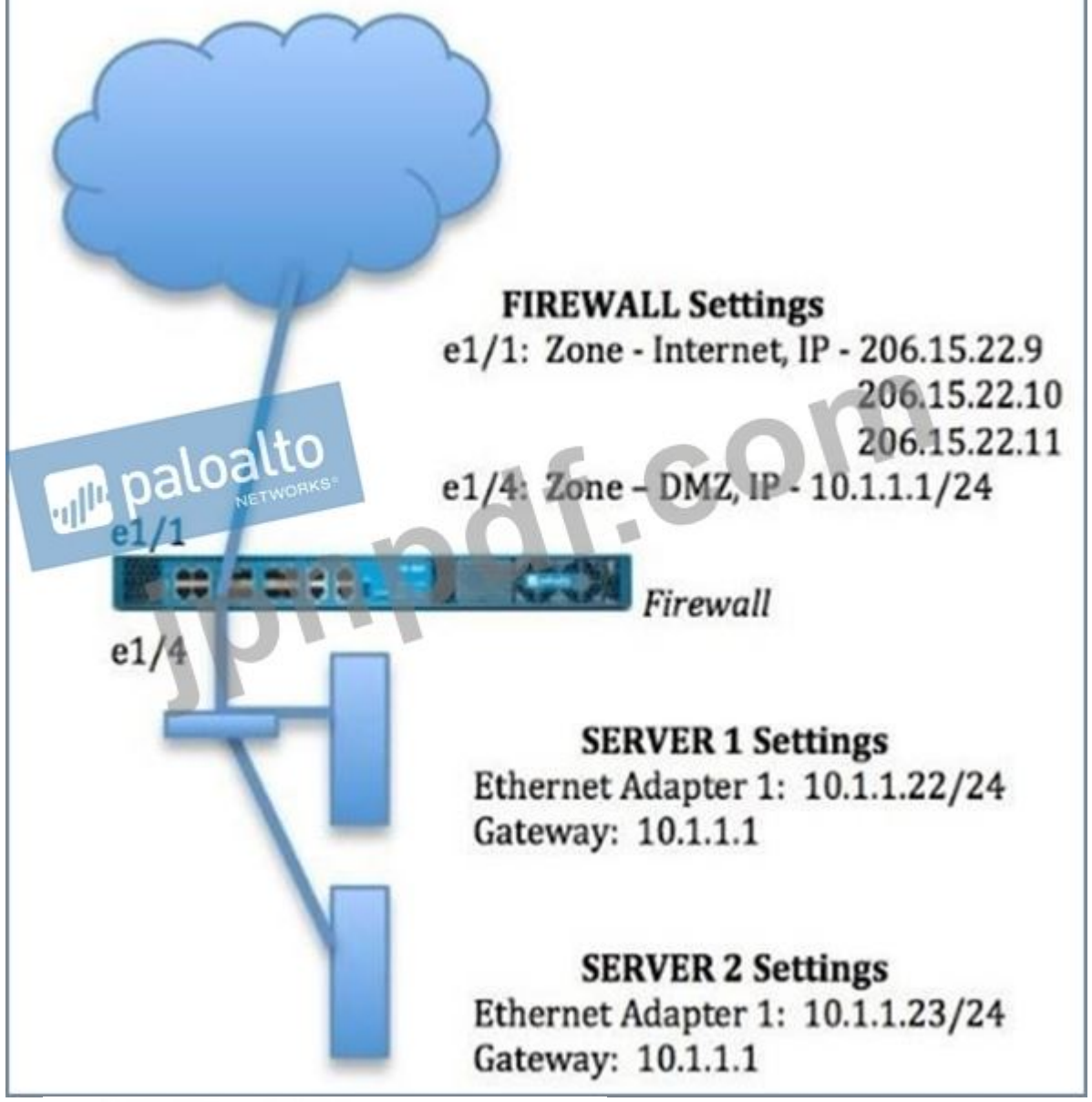
管理者は、bittorrentアクティビティの大幅な増加に気づきました。管理者は、トラフィックが会社のどこに向かっているのかを判断したいと考えています。
管理者の次のステップは何でしょうか？
A. ネットワークアクティビティを表示するには、bittorrentアプリケーションのリンクをクリックします
B. ビットトレントトラフィックのグローバルフィルターを作成してから、トラフィックログを表示します。
C. ビットトレントトラフィックのローカルフィルターを作成してから、トラフィックログを表示します。
D. ビットトレントリンクを右クリックして、コンテキストメニューから[値]を選択します
Answer: A (メーッセージを残す)

最新問題**: 26**

PAN-OSバージョン9.1でスターリングし、GlobalProtectのログ情報がどのファイアウォールログに記録されるようになりましたか？
A. 構成
B. 認証
C. GlobalProtect
D. システム
Answer: B (メーッセージを残す**)**

最新問題**: 27**
正誤問題：多く のお客様は、トラフィックフローの可視性をこれまで利用できなかったレベルにするためだけに、パロアルトネットワークスNGFW（次世代ファイアウォール）を購入しています。
A. FALSE
B. TRUE
Answer: (解答を表示する**)**

最新問題**: 28**
管理者は、DMZ内の複数のWebサーバーがインターネットから開始された接続を受信することを望んでいます。206.15.22.9ポート80 / TCP宛てのトラフィックは、10.1.1.22のサーバーに転送する必要があります。
画像に示されている情報に基づいて、どのNATルールがWebブラウジングトラフィックを正しく転送しますか？



A.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

B.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

C.

D.

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: None

Answer: D (メーッセージを残す)

最新問題: **29**

次のパノラマの画像で、一部の値が赤で表示されているのはなぜですか？

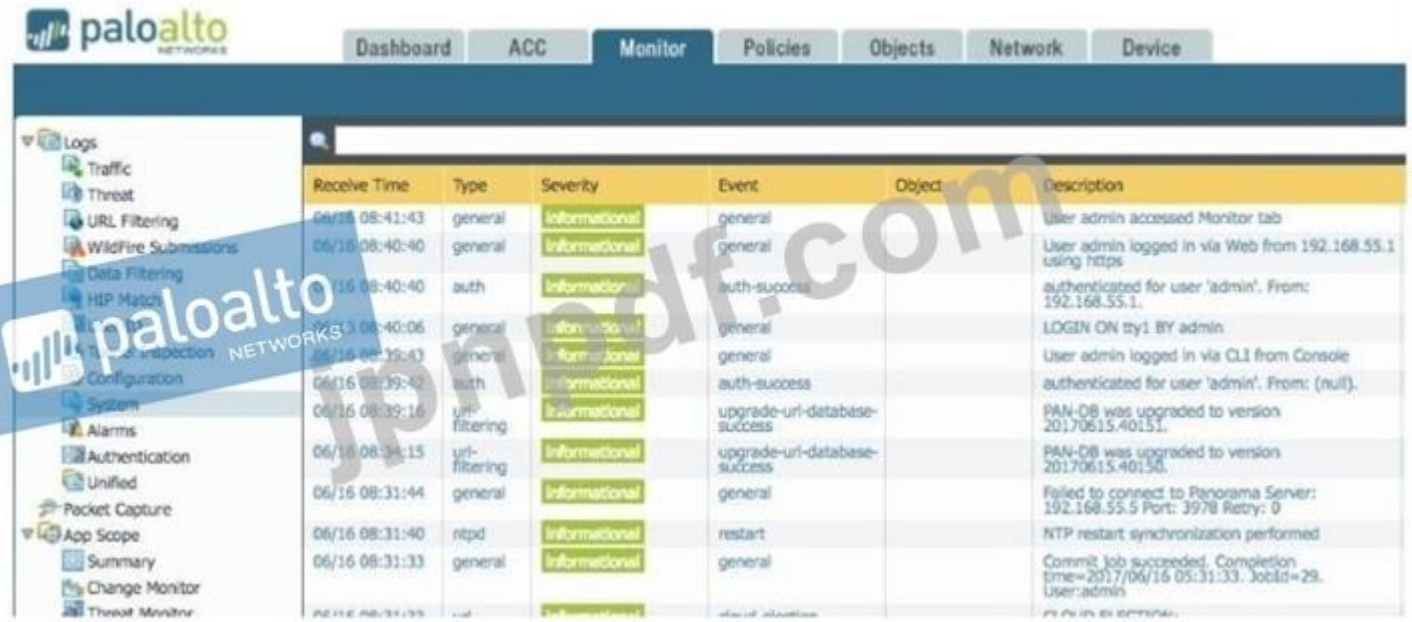
Device Name	Logging Rate (Log/sec)	Device	Session
		Throughput (KB/sec)	Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. uk3のログレートは、7日間の計算ベースラインから外れています。
B. us3のログレートは、管理者が設定したしきい値から外れています。
C. sg2のセッションしきい値が正しく構成されていません。
D. sg2セッション数は、他の管理対象デバイスと比較して最も少なくなっています。
Answer: D (メーッセージを残す)

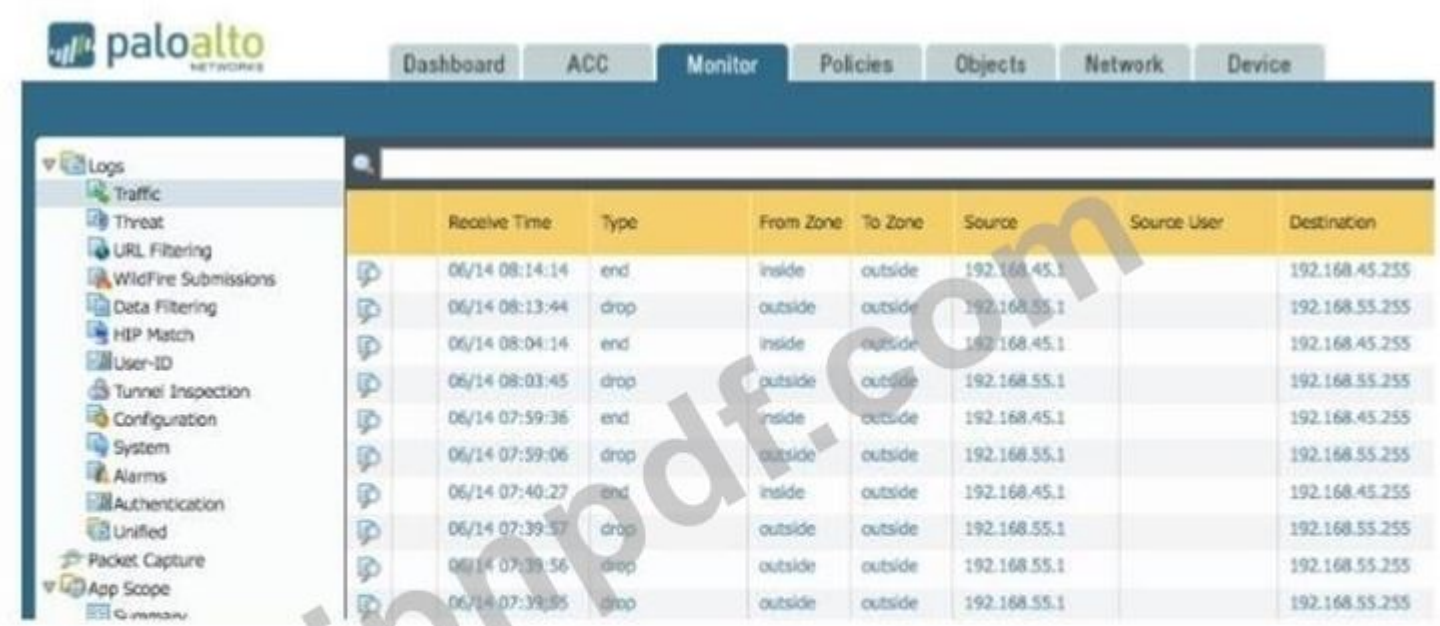
最新問題**: 30**
セキュリティポリシーの一致のためにサービスを使用することとアプリケーションを使用することの違いは何ですか？
A. 『サービス」を使用すると、十分なパケットがApp-IDの識別を可能にした後、ファイアウォールがアクションを実行できるようになります
B. 『サービス」を使用すると、ファイアウォールはポート番号に基づいて最初に観測されたパケットに対して即座にアクションを実行できます。『アプリケーション」を使用すると、十分なパケットがApp-IDの識別を可能にした後、ファイアウォールがアクションを実行できます。使用されているポート。
C. 『サービス」と 『アプリケーション」に違いはありません。『アプリケーション」を使用すると、ポート番号の代わりにわかりやすいアプリケーション名を使用できるため、構成が簡素化されます。
D. 『サービス」を使用すると、ファイアウォールはポート番号に基づいて最初に監視されたパケットに対して即座にアクションを実行できます。『アプリケーション」を使用すると、使用されているポートがアプリケーションの標準ポートリストのメンバーである場合に、ファイアウォールが即座にアクションを実行できます。
Answer: B (メーッセージを残す)
説明
https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508# Palo Alto Networksファイアウォールのサービスは、ポートが開いているか閉じているTCPまたはUDPポートです。レイヤー4を超えては見えません。レイヤー7の検査を受けて、データフローでアクティブなアプリケーションを確認し、 通常の」動作を強制するアプリケーション、DNSクエリ
https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508#コンセプト1パロアルトネットワークファイアウォールのサービスは、TCPまたはUDPポートです。従来のファイアウォールまたはアクセスリストで定義されます。これは、どのポートが開いているか閉じているかを定義するだけで、レイヤー4を超えて見えません。
コンセプト2
アプリケーションは、パロアルトネットワークスの次世代ファイアウォールを非常に強力にするものです。レイヤーに入ります
7どのアプリケーションがデータフローでアクティブであり、 通常の」動作を強制するかを確認するための検査 たとえば、SQLクエリを突然送信するDNSとして識別されたセッションは異常であり、ブロックされます）。

最新問題**: 31**
管理者は、コミットが終了する前に誤ってコミットウィンドウ/画面を閉じました。管理者がそのコミットタスクの進行状況または成功を確認するために使用できる2つのオプションはどれですか？ 2つ選択してください。）

A



B



C

A. 展示物A

B. 展示物B

C. 展示物C

D. 展示物D

Answer: (解答を表示する)

説明

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/web-interface-basics/commit-changes.h

最新問題: **32**

展示を参照してください。

DMZ内のWebサーバーは、DNATを介してパブリックアドレスにマップされています。
トラフィックがWebサーバーに流れることを許可するセキュリティポリシールールはどれですか？
A. Untrust（any）からUntrust（10.1.1.100）、Webブラウジング許可
B. 信頼できない（任意から信頼できない（1.1.1.100）、Webブラウジング許可
C. DMZ（1.1.1.100）への信頼（任意）、Webブラウジング許可
D. DMZ（10.1.1.100）、Webブラウジングへの信頼（任意）許可
Answer: C (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping

最新問題**: 33**
グローバルな企業オフィスには、ユーザーIDエージェントが1つしかない大規模なネットワークがあり、ユーザーIDエージェントサーバーの近くにボトルネックが生じます。この場合、PAN-OSソフトウェアのどのソリューションが役立ちますか？
A. 仮想ワイヤーモード
B. ユーザーマッピングの再配布
C. コンテンツ検査
D. アプリケーションのオーバーライド
Answer: B (メーッセージを残す)

最新問題**: 34**
インターネットゾーンのユーザーがDMZゾーンでホストされているWebサーバーに正常に接続できるようにするゾーンペアとルールタイプはどれですか。Webサーバーは、パロアルトネットワークファイアウォールの宛先NATポリシーを使用して到達可能です。
A. ゾーンペア：
ソースゾーン :インターネット
宛先ゾーン :DMZ

ルールタイプ：
「ゾーン内」
B. ゾーンペア：
ソースゾーン :インターネット
宛先ゾーン :DMZ
ルールタイプ：
「ゾーン内」または「ユニバーサル」
C. ゾーンペア：
ソースゾーン :インターネット
宛先ゾーン :インターネット
ルールタイプ：
「ゾーン内」または「ユニバーサル」
D. ゾーンペア：
ソースゾーン :インターネット
宛先ゾーン :インターネット
ルールタイプ：
「ゾーン内」
Answer: B (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zone-defense-tools.html
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

最新問題**: 35**
管理者がインバウンド復号化で問題に遭遇しました。管理者はトリアージの一部としてどのオプションを調査する必要がありますか？
A. ターゲットサーバーへのSSLを許可するセキュリティポリシールール
B. CRLへのファイアウォール接続
C. 「信頼」が有効になっているファイアウォールにインポートされたルート証明書
D. HSMからの証明書のインポート
Answer: A (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspectio

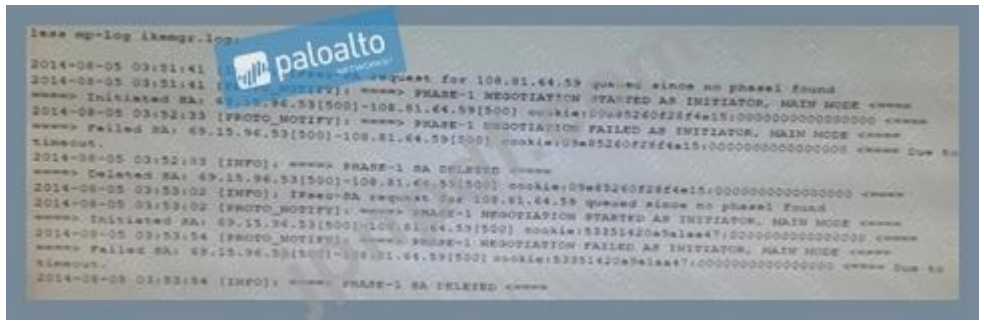
最新問題**: 36**
HA Liteでサポートされている3つのオプションはどれですか？ （3つ選択してください。）
A. 仮想リンク
B. アクティブ/パッシブ展開
C. IPsecセキュリティアソシエーションの同期
D. 構成の同期
E. セッションの同期
Answer: B,C,D (メーッセージを残す)

説明/参照：
参照 :https ://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device- high-availability / ha-lite

最新問題: **37**
会社には、悪いと分類したすべてのアプリケーションを拒否し、良いと分類したアプリケーションのみを許可するというポリシーがあります。ファイアウォール管理者は、会社のファイアウォールに次のセキュリティポリシーを作成しました。

どのインターフェイス設定が特定のVLANIDを受け入れますか？
ルール2とルール3の両方を提示することで得られる2つの利点はどれですか？ 2つ選択してください）
A. ネットワーク上の未分類のトラフィックを識別するレポートを作成できます。
B. ルール2と3は、異なるポートのトラフィックに適用されます。
C. 個別のログ転送プロファイルをルール2と3に適用できます。
D. トラフィックマッチングルール2および3には、さまざまなセキュリティプロファイルを適用できます。
Answer: C,D (メーッセージを残す**)**

最新問題: **38**
管理者が管理者の自宅でCiscoASAへのIPSecVPNを設定していて、接続の完了で問題が発生しています。コマンドからの出力は次のとおりです。



この問題の原因は何でしょうか？
A. 共有シークレットがPalo AltoNetworksFirewallとASAの間で一致しません。
B. デッドピア検出設定がPalo AltoNetworksFirewallとASAの間で一致していません。
C. パブリックIPアドレスは、パロアルトネットワークファイアウォールとASAの両方で一致しません。
D. Palo AltoNetworksFirewallのプロキシIDがASAの設定と一致しません。
Answer: C (メーッセージを残す**)**

最新問題: **39**
HA2リンクを介して何が交換されますか？
A. こんにちはハートビート
B. ユーザーID情報
C. セッションの同期
D. HA状態情報

Answer: C (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links
「データリンク-HA2リンクは、HAペア内のデバイス間でセッション、転送テーブル、IPSecセキュリティアソシエーション、およびARPテーブルを同期するために使用されます。HA2リンクのデータフローは常に単方向です（HA2キープアライブを除く）。アクティブデバイスからパッシブデバイスへ。」
https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/hig

最新問題**: 40**
クライアントは、アクティブ/パッシブモードで高可用性（HA）を使用してPA-5000シリーズファイアウォールのペアを展開しています。この展開について正しい説明はどれですか。
A. 2つのデバイスはルーティング可能なフローティングIPアドレスを共有する必要があります
B. 2つのデバイスは、PA-5000シリーズ内の異なるモデルである可能性があります
C. 各ピアのHA1IPアドレスは異なるサブネット上にある必要があります
D. 管理ポートはバックアップ制御接続に使用できます
Answer: (解答を表示する)
バックアップ制御リンク接続を設定します。
1.[デバイス]>[高可用性]>[一般]で、[制御リンク（HA1バックアップ）]セクションを編集します。
2. HA1バックアップインターフェイスを選択し、IPv4/IPv6アドレスとネットマスクを設定します。
注：HA1リンクの管理ポートを使用してください。
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/high-availability/configure- active-passive-ha

最新問題**: 41**
テンプレートスタックがデバイスに割り当てられており、スタックに設定が重複する3つのテンプレートが含まれている場合、テンプレートスタックがプッシュされたときに、どの設定がデバイスに公開されますか？
A. スタックの最上位にあるテンプレートに割り当てられた設定。
B. 管理者は、選択したファイアウォールの設定を選択するように昇格します。
C. すべてのテンプレートで構成されているすべての設定。
D. ファイアウォールの場所に応じて、Panoramaは送信する設定を決定します。
Answer: B (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

最新問題**: 42**
HAタイマー設定に関する正しい説明はどれですか。
A. 一般的なフェイルオーバータイマー設定には中程度のプロファイルを使用します
B. 一般的なフェイルオーバータイマー設定に推奨プロファイルを使用する
C. フェイルオーバータイマーの設定を遅くするには、アグレッシブプロファイルを使用します。
D. フェイルオーバータイマーの設定を高速化するには、クリティカルプロファイルを使用します。

Answer: B (メーッセージを残す)

最新問題: **43**
ネットワーク管理者は、Windows 10エンドポイントのログオン前にGlobalProtectを展開し、パロアルトネットワークスのベストプラクティスに従うことを望んでいます。
エンドポイントの証明書とキーをインストールするには、どの3つのコンポーネントが必要ですか？ 3つ選択してください。）
A. サーバー証明書
B. ローカルコンピュータストア
C. 秘密鍵
D. 自己署名証明書
E. マシン証明書
Answer: B,D,E (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/globalprotect-quick-configs/remote-acc

最新問題: **44**
ファイアウォールが再起動されたときのHighlightUnusedRulesとRuleUsageHitカウンターの2つの動作の違いは何ですか？ 2つ選択してください。）
A. 未使用のルールを強調表示すると、ゼロのルールが強調表示されます。
B. ルール使用ヒットカウンターがリセットされます。
C. 未使用のルールを強調表示すると、すべてのルールが強調表示されます。
D. ルール使用法ヒットカウンターはリセットされません
Answer: C,D (メーッセージを残す)

最新問題: **45**
管理者は、DMZとコアネットワークの間にNGFWを実装する必要があります。2つの環境間のEIGRPルーティングが必要です。このビジネス要件をサポートするインターフェイスタイプはどれですか。
A. レイヤ3インターフェイス、ただし接続された仮想ルータでEIGRPを設定する
B. EIGRPルーティングをコアとDMZの間に維持できるようにする仮想ワイヤインターフェイス
C. IPsecトンネルでEIGRPルーティングを終了するためのトンネルインターフェイス（SVPNおよびEIGRPプロトコルをサポートするGlobalProtectライセンスを使用）
D. レイヤ3またはアグリゲートイーサネットインターフェイス。ただし、サブインターフェイスでのみEIGRPを設定する
Answer: (解答を表示する)

最新問題: **46**
ファイアウォールでローカルにのみ構成でき、Panoramaテンプレートまたはテンプレートスタックからプッシュできない2つの設定はどれですか？ 2つ選択してください）
A. HA1IPアドレス
B. ネットワークインターフェースタイプ
C. マスターキー

D. ゾーン保護プロファイル
Answer: (解答を表示する**)**
説明
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-ex

最新問題**: 47**
GlobalProtectポータルを設定する場合、認証プロファイルを指定する目的は何ですか？
A. ポータルへのゲートウェイ認証を有効にするには
B. ゲートウェイへのポータル認証を有効にするには
C. ポータルへのユーザー認証を有効にする
D. ポータルへのクライアントマシン認証を有効にする
Answer: (解答を表示する**)**
ブラウザとサテライトの追加オプションを使用すると、特定のシナリオで使用する認証プロファイルを指定できます。「ブラウザー」を選択して、GlobalProtectエージェント（WindowsおよびMac）をダウンロードする目的でWebブラウザーからポータルにアクセスするユーザーを認証するために使用する認証プロファイルを指定します。
[衛星]を選択して、衛星の認証に使用する認証プロファイルを指定します。
参照https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/globalprotect/network-globalprotect-portals

最新問題**: 48**
管理者は、アクティブな脅威防止サブスクリプションを持つPA-820ファイアウォールを持っています。管理者は、WildFireサブスクリプションの追加を検討しています。
WildFireサブスクリプションを追加すると、組織のセキュリティ体制がどのように改善されますか1。
A. 未知のマルウェアに対する保護をほぼリアルタイムで提供できます
B. WildFireとThreat Preventionを組み合わせて、ファイアウォールに最大限のセキュリティ体制を提供します
C. 24時間後、WildFireシグネチャがウイルス対策アップデートに含まれます
D. WildFireとThreat Preventionを組み合わせて、攻撃対象領域を最小限に抑えます
Answer: (解答を表示する**)**

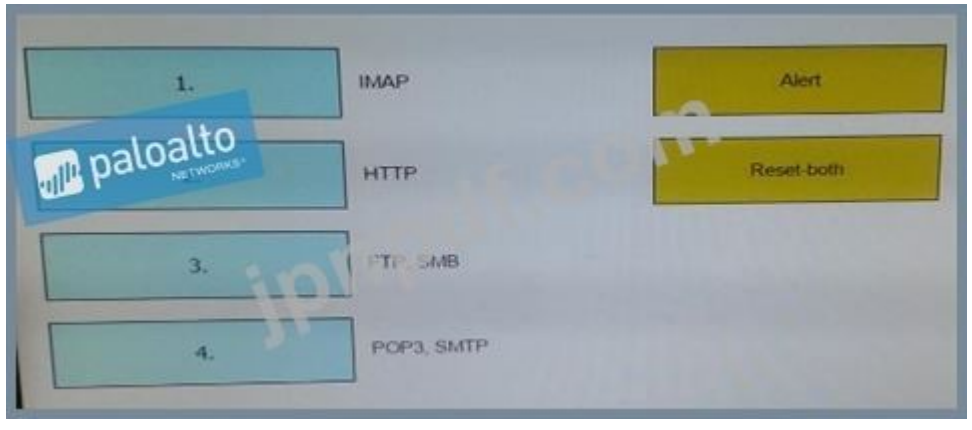
最新問題**: 49**
企業には、オンサイトファイアウォールとPanoramaによって管理されるモバイルユーザー向けのPrismaAccessを含む大きなパロアルトネットワークスのフットプリントがあります。企業はすでにGlobalProtectとSAML認証を使用して、iPからユーザーへのマッピング情報を取得しています。ただし、情報セキュリティはこの情報を使用したいと考えています。PrismaAccessでグループマッピングに基づくポリ

シー施行情報セキュリティはオンプレミスActive Directory（AD）を使用しますが、PrismaAccessがADからグループを学習するために何が必要かについては不明ですグループマッピングに基づくポータをPrismaAccessで学習および施行するにはどうすればよいですか？
A. SAMLアサーションを介してグループマッピングを学習するようにPrismaAccessを構成します
B. PrismaAccessがグループを学習するためのPanoramaのマスターデバイスを割り当てます
C. オンサイトのパロアルトネットワークファイアウォールとPrismaAccessの間にグループマッピングの再配布を設定します
D. オンプレミスドメインコントローラーを指すLDAPプロファイルを参照するグループマッピング構成を作成します
Answer: (解答を表示する**)**
ステップ3 :1つ以上の次世代オンプレミスまたはVMシリーズファイアウォールをマスターデバイスとして構成することにより、Panoramaがセキュリティポリシーでグループマッピングを使用できるようにします。Prisma Access User-IDデプロイメントを使用してマスターデバイスを設定しない場合は、代わりに長い形式の分散名（DN）エントリを使用してください。https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-access/configure-user-id-in-prisma-access。html

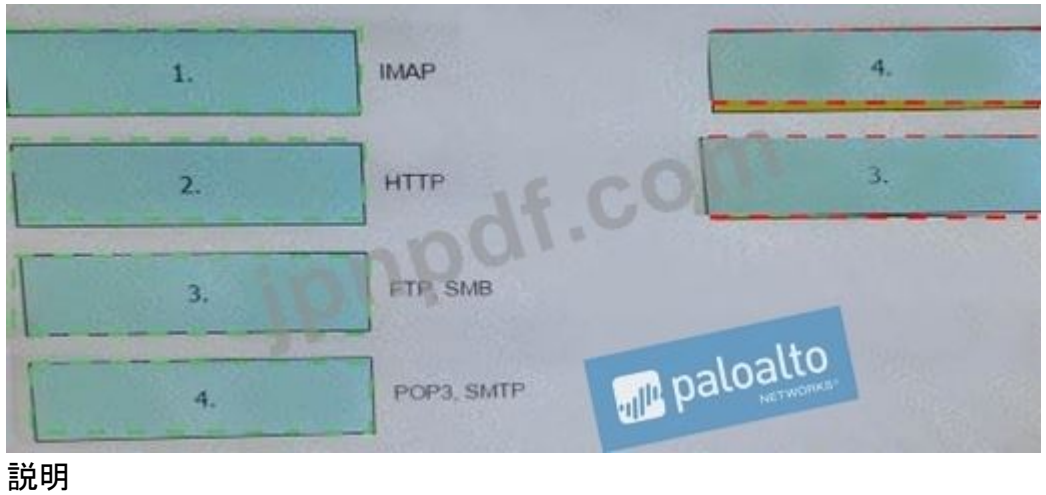
最新問題**: 50**
エンジニアは、新しいSSL復号化デプロイメントを構成する必要があります
SSL復号化ルールに一致するトラフィックを復号化する前に、どのプロファイルまたは証明書が必要ですか？
A. ForwardTrustオプションとForwardUntrustオプションの両方が選択された証明書が必要です
B. トラフィックが一致する復号化ポリシーに復号化プロファイルを添付する必要があります
C. トラフィックが一致するセキュリティポリシーに復号化プロファイルを添付する必要があります
D. 転送信頼オプションのみが選択された証明書が存在する必要があります
Answer: B (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html

最新問題**: 51**
ファイアウォールでローカルにのみ構成でき、Panoramaテンプレートまたはスタックテンプレートからプッシュできない2つの設定はどれですか？ 2つ選択してください。）
A. ネットワークインターフェースタイプ
B. ゾーン保護プロファイル
C. マスターキー
D. HA1IPアドレス
Answer: (解答を表示する**)**

最新問題**: 52**
事前定義されたデフォルトプロファイルを使用する場合、ポリシーはデコーダー上のウイルスを検査します。各デコーダーをデフォルトのアクションと一致させます。
回答オプションは、複数回使用することも、まったく使用しないこともできます。



Answer:



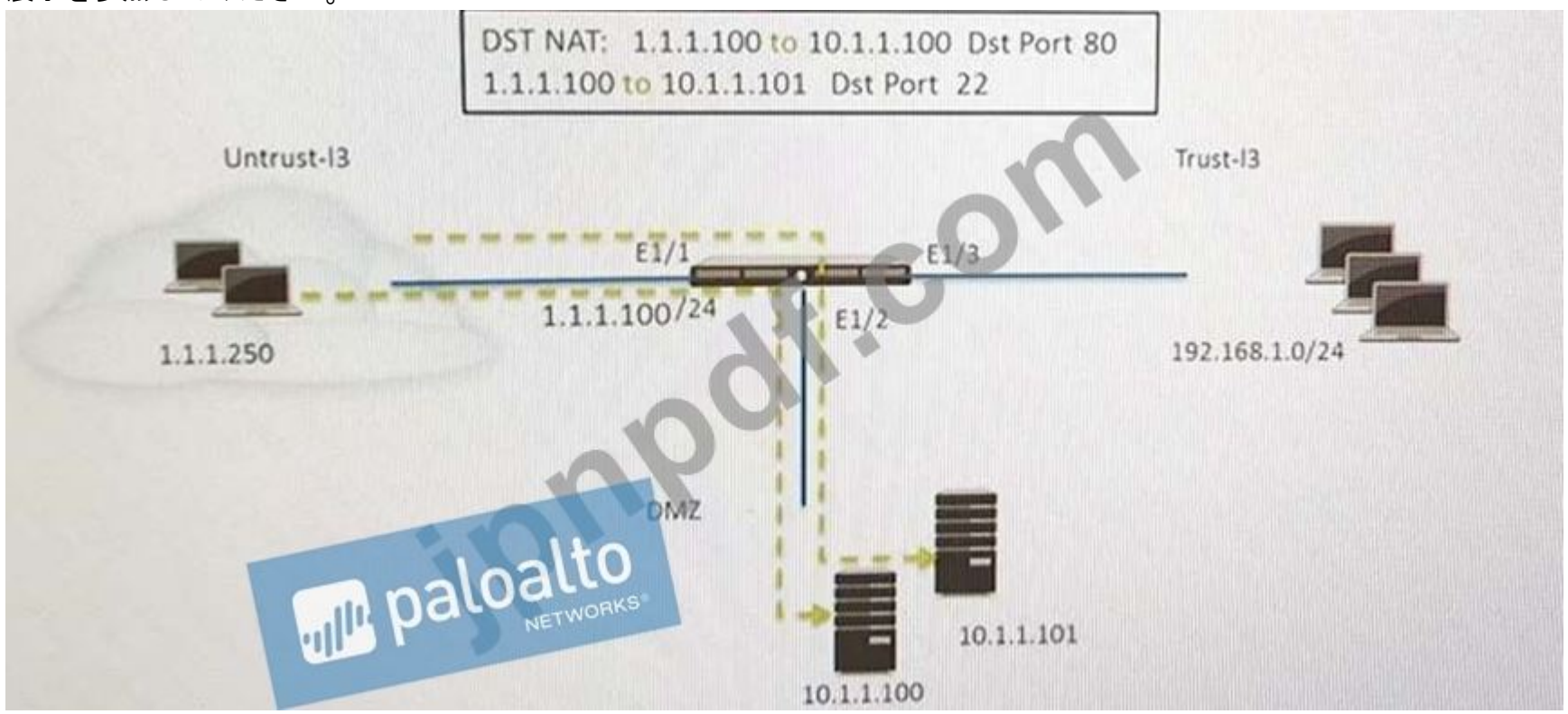
説明

IMAP、POP3、SMTP->アラート

HTTP、FTP、SMB->リセット両方

最新問題: **53**

展示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アドレスにマップしています。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誘導されます。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2つのセキュリティポリシールールはどれですか。（2つ選択してください。）

A. Untrust（Any）to Untrust（10.1.1.1）、web-browsing -Allow

B. Untrust（Any）to Untrust（10.1.1.1）、ssh -Allow

C. DMZ（10.1.1.1）に対する信頼できない（任意）、Webブラウジング許可

D. DMZ（10.1.1.1）に対する信頼できない（任意）、ssh -Allow

E. DMZ（10.1.1.100.10.1.1.101）、ssh、web-browsingへの信頼できない（任意）許可

Answer: C,D (メーッセージを残す**)**

説明

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

最新問題**: 54**

SD-WANポリシーに一致しないSD-WANファブリックを通過するトラフィックはどうなりますか？

A. トラフィックを転送するための一致するSD-WANポリシーがないため、トラフィックはドロップされます。

B. トラフィックは、SD-WANプラグインを介して作成されたキャッチオールポリシーに一致します。

C. トラフィックは暗黙のポリシールールに一致し、SD-WANリンク全体でラウンドロビンで再配布されます。

D. トラフィックは、最小のインターフェイス番号（つまり、Eth1/1からEth1/3）に基づいて、SD-WANに参加している最初の物理インターフェイスに転送されます。

Answer: (解答を表示する)

リスト内のSD-WANポリシールールに一致するものがない場合、セッションは、ラウンドロビン方式を使用して1つのSD内のすべてのリンクに一致しないセッションを分散するリストの最後にある暗黙のSD-WANポリシールールに一致します。ルートルックアップに基づくWANインターフェース。

最新問題**: 55**

テンプレートスタックがデバイスに割り当てられており、スタックに設定が重複する3つのテンプレートが含まれている場合、テンプレートスタックがプッシュされたときに、どの設定がデバイスに公開されますか？

A. スタックの最上位にあるテンプレートに割り当てられた設定。

B. 管理者は、選択したファイアウォールの設定を選択するように昇格します。

C. すべてのテンプレートで構成されているすべての設定。

D. ファイアウォールの場所に応じて、Panoramaは送信する設定を決定します。

Answer: A (メーッセージを残す**)**

参照：

https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

最新問題**: 56**

パノラマは、VMWare NSXに感染したVMを隔離するようにどのように促しますか？

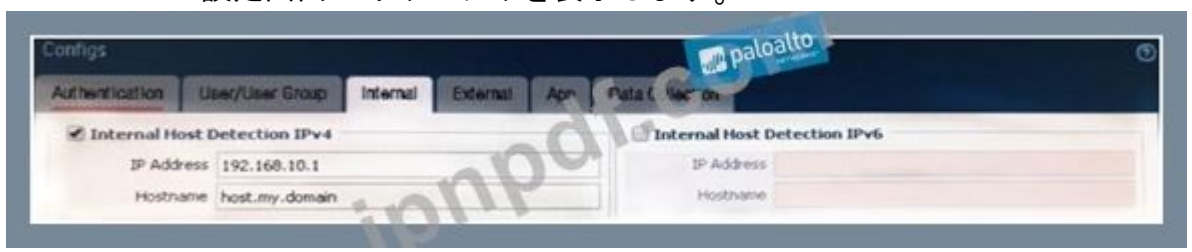
A. Syslogサーバープロファイル

B. HTTPサーバープロファイル

C. メールサーバープロファイル
D. SNMPサーバープロファイル
Answer: (解答を表示する**)**

最新問題**: 57**
M-100アプライアンスをログコレクターとして構成するには、どの2つのオプションが必要ですか？ 2つ選択してください）
A. パノラマGUIの[パノラマ]タブから[ログコレクターモード]を選択し、変更をコミットします
B. コマンドリクエストシステムシステムモードロガーを入力し、Yを入力してログコレクターモードへの変更を確認します。
C. パノラマGUIの[デバイス]タブから[ログコレクターモード]を選択し、変更をコミットします。
D. コマンドlogger-modeを入力し、Enterキーを押してログコレクターモードへの変更を確認します。
E. 専用のログコレクターのPanoramaCLIにログインします
Answer: B,E (メーッセージを残す**)**
説明
https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up

最新問題**: 58**
GlobalProtect設定画面のキャプチャを表示します。



この構成の目的は何ですか？
A. すべての内部クライアントのトンネルアドレスを192.168.10.1から始まるIPアドレス範囲に設定します。
B. 内部クライアントを強制的にIPアドレス192.168.10.1の内部ゲートウェイに接続します。
C. クライアントが192.168.10.1で逆DNSルックアップを実行して、それが内部クライアントであることを検出できるようにします。
D. ファイアウォールに動的DNS更新を実行させ、内部ゲートウェイのホスト名とIPアドレスをDNSサーバーに追加します。
Answer: C (メーッセージを残す**)**
参照：
https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations
「このオプションを選択すると、GlobalProtectエージェントがエンタープライズネットワーク内にあるかどうかを判断できます。このオプションは、内部ゲートウェイと通信するように構成されているエンドポイントにのみ適用されます。ユーザーがログインしようとすると、エージェントは指定されたホスト名を指定されたIPアドレスに使用する内部ホスト。ホストは、エンドポイントがエンタープライズネットワーク内にある場合に到達可能な参照ポイントとして機能します。エージェントがホストを検出した場合、エンドポイントはネットワーク内にあり、エージェントはに接続します。内部ゲートウェイ。エージェントが内部ホストを見つけられなかった場合、エンドポイントはネットワークの外部にあり、エージェントは外部ゲートウェイの1つへのトンネルを確立します。」

最新問題**: 59**

管理者は、特定のDNSサーバーをデバイスグループ内の1つのファイアウォールに割り当てる必要があります。管理者はどこでテンプレート変数をデバイスレベルで編集しますか？

A. パノラマ>テンプレートでの可変CSVエクスポート

B. 管理対象デバイス>デバイスの関連付け

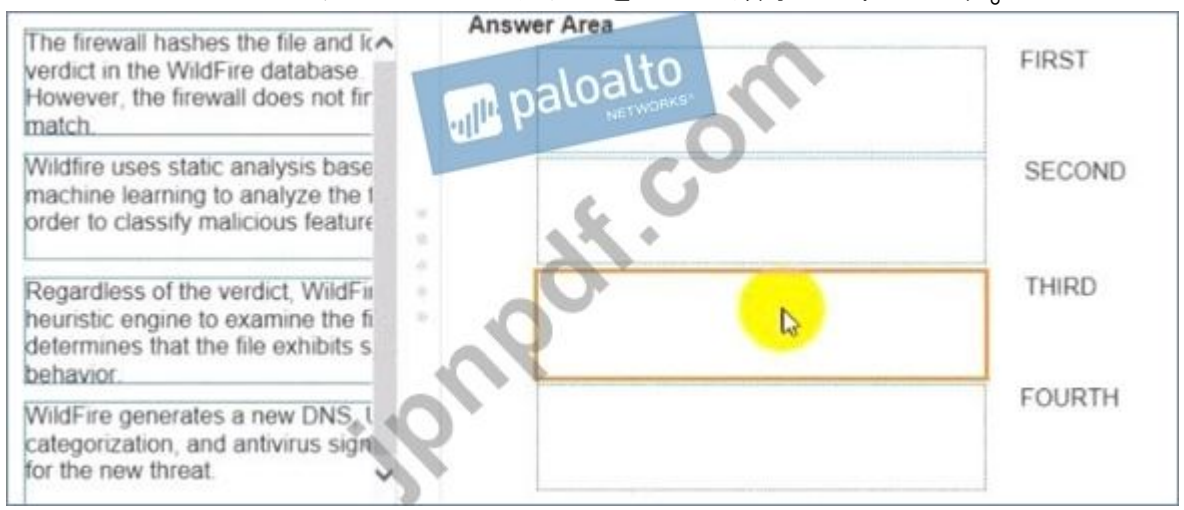
C. パノラマ>テンプレートで変数を管理する

D. パノラマの下でのPDFエクスポート>テンプレート

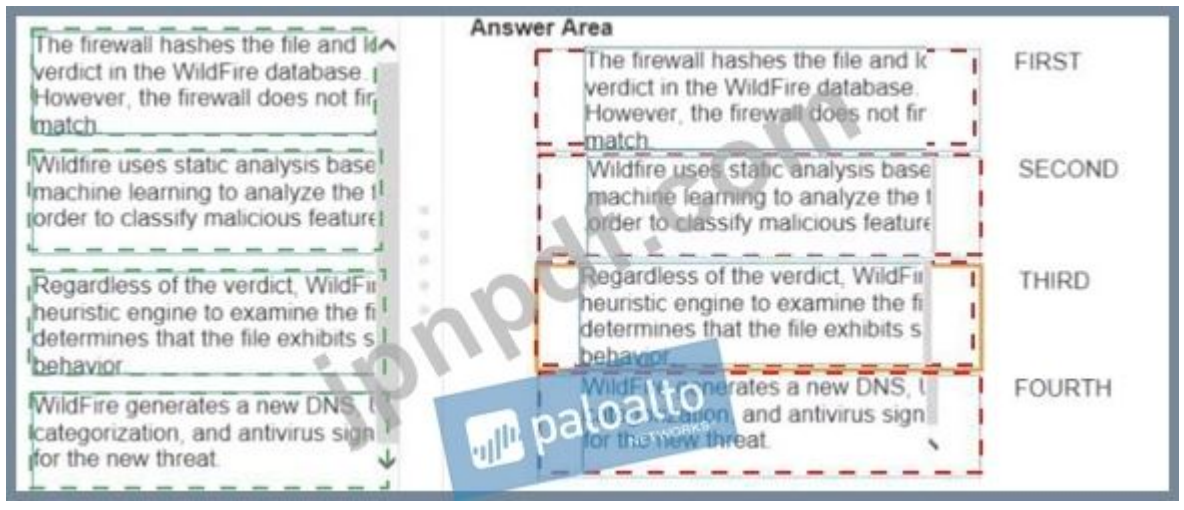
Answer: (解答を表示する**)**

最新問題: **60**

WildFireプロセスワークフローのステップを正しい順序で配置します。

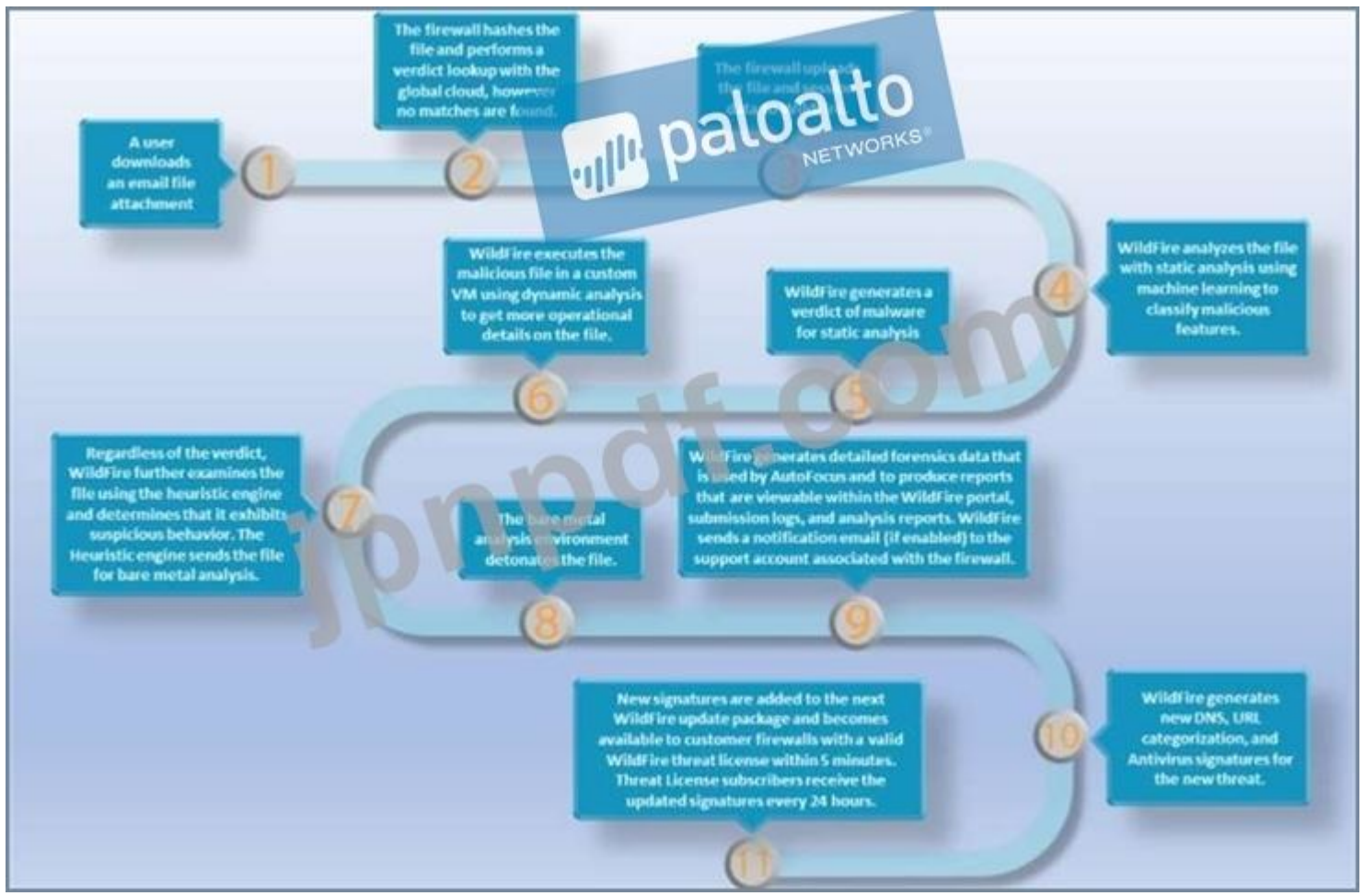


Answer:



説明

自動生成されたタイムラインの説明



https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html

最新問題**: 61**
ユーザーインターフェイスethernet1 / 3にIPV6DNSクエリをどのように構成しますか？
A. ネットワーク>仮想ルーター> DNSインターフェース
B. オブジェクト> CustomerObjects> DNS
C. ネットワーク>インターフェースマネージャー
D. デバイス>セットアップ>サービス>サービスルート構成
Answer: (解答を表示する**)**
サービスルートを構成します。
1. [デバイス]> [セットアップ]> [サービス]> [グローバル]を選択し、[サービスルートの構成]をクリックします。
注 :ライセンスをアクティブ化し、最新のコンテンツとソフトウェアの更新を取得するために、DNS、Palo Altoの更新、URLの更新、WildFire、およびAutoFocusのサービスルートを変更する必要があります。
2. [カスタマイズ]ラジオボタンをクリックして、次のいずれかを選択します。
事前定義されたサービスの場合は、IPv4またはIPv6を選択し、ソースインターフェイスを変更するサービスのリンクをクリックして、構成したインターフェイスを選択します。
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/set-up- network-access-for-external-services

最新問題: **62**
PAN-OSソフトウェアとのネイティブ統合がない802.1x対応のワイヤレスネットワークデバイスを介して接続するユーザーのユーザー名にIPアドレスをマップするユーザーIDの方法はどれですか？
A. XML API
B. ポートマッピング
C. クライアントプロービング
D. サーバー監視
Answer: (解答を表示する**)**
キャプティブポータルおよびその他の標準的なユーザーマッピング方法は、特定のタイプのユーザーアクセスでは機能しない場合があります。たとえば、標準の方法では、サードパーティのVPNソリューションから接続しているユーザーや802.1x対応のワイヤレスネットワークに接続しているユーザーのマッピングを追加することはできません。このような場合、PAN-OS XML APIを使用してログインイベントをキャプチャし、それらをPAN-OS統合ユーザーIDエージェントに送信できます。リファレンス：
https ://www.paloaltonetworks.com/documentation/80/pan-os/ pan-os / user-id / user-id-concepts / group-mapping＃id93306080-fd9b-4f1b-96a6-4bfe1c8e69df

最新問題: **63**
アクティブ/アクティブ高可用性の導入が必要な正当な理由は、次の3つのユースケースのうちどれですか。（3つ選択してください）
A. 環境では、動的ルーティングプロトコルのコンバージェンスを高速化するために、両方のファイアウォールが独自のルーティングテーブルを維持する必要があります
B. 環境では、ピーク時のトラフィックスパイクを処理するために、両方のファイアウォール間でトラフィックの負荷を分散する必要があります
C. 環境では、すべての構成がHAペアの両方のメンバー間で完全に同期されている必要があります
D. 環境には、常に両方のファイアウォールからの実際のフルタイムの冗長性が必要です
E. 環境にはデプロイメントにレイヤー2インターフェースが必要です
Answer: A,C,E (メーッセージを残す**)**

最新問題: **64**
リモート管理者は、信頼できないインターレースでファイアウォールにアクセスする必要があります。安全な管理アクセスのために、インターフェイス管理プロファイルで構成する3つのオプションはどれですか。（3つ選択してください）
A. HTTP
B. ユーザーID
C. SSH
D. HTTPS
E. 許可されたIPアドレス

Answer: B,C,D (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/use-interface-mana

最新問題: **65**
管理者は、更新のインストールを一定時間遅らせながら、アプリケーションと脅威の動的更新をどのようにスケジュールしますか？
A. ﾚしきい値」のオプションを設定します。
B. 平日の自動更新を無効にします。
C. 管理者が更新を承認した後、自動的に ﾀダウンロードのみ」、後でアプリケーションと脅威をインストールします。
D. 自動的に ﾀダウンロードしてインストール」しますが、 新しいアプリケーションを無効にする」オプションを使用します。
Answer: C (メーッセージを残す)
説明

最新問題: **66**
ファイアウォールはMineMeldからIPアドレスをダウンロードしていません。画像に基づいて、最も可能性の高いものは何が間違っていますか？


A. クライアント証明書を含む証明書プロファイルを選択する必要があります。
B. 送信元アドレスは、ftp :// <address/file>でホストされているファイルのみをサポートします。
C. CA証明書を含む証明書プロファイルを選択する必要があります。
D. 外部動的リストはSSL接続をサポートしていません。
Answer: C (メーッセージを残す)

最新問題: **67**
別紙を参照してください。ファイアウォールには、3つのPBFルールと、デフォルトVRで構成された172.20.10.1のネクストホップを持つデフォルトルートがあります。Willという名前のユーザーは、192.168.10.10のIPアドレスを持つPCを持っています。
彼は172.16.10.20にHTTPS接続します。
WillのPCからのHTTPSトラフィックのネクストホップIPアドレスはどれですか。

A. 172.20.10.1

B. 172.20.40.1

C. 172.20.30.1

D. 172.20.20.1

Answer: D (メーッセージを残す)

最新問題**: 68**

ICMPパケットの送信元アドレスは何になりますか？

A. 10.30.0.93

B. 10.46.72.93

C. 10.46.64.94

D. 192.168.93.1

Answer: C (メーッセージを残す)

最新問題**: 69**

管理者がデータプレーンのCPU使用率を確認できるCLIコマンドはどれですか。

A. 実行中のリソースモニターを表示します

B. デバッグデータプレーンdp-cpu

C. システムリソースを表示する

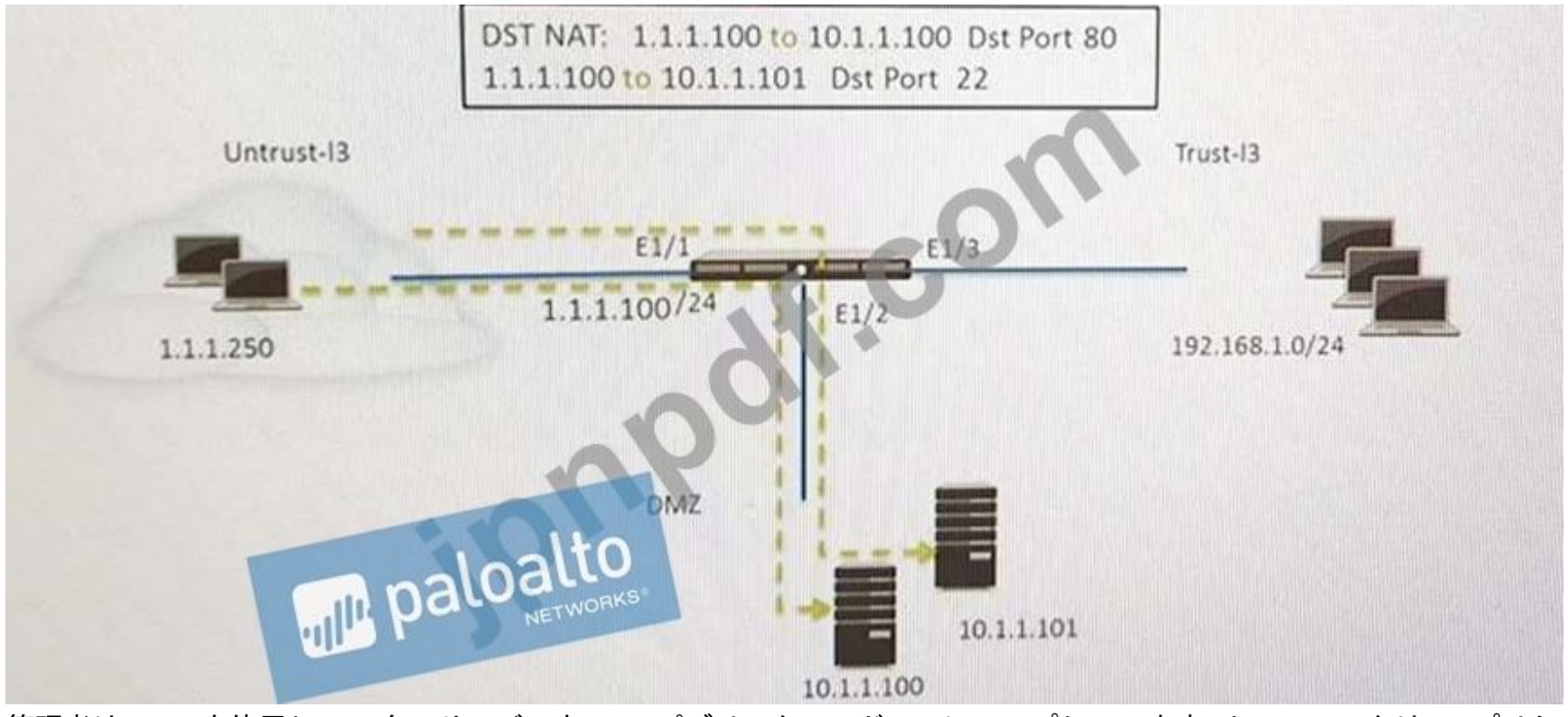
D. 実行中のリソースをデバッグします

Answer: A (メーッセージを残す)

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CluDCAS

最新問題: **70**
パノラマ管理者は、新しいゾーンを構成し、新しいセキュリティポリシーでそのゾーンを使用します。
管理者が構成をPanoramaにコミットした後、プッシュが成功することを確認するために、管理者はどのデバイスグループコミットプッシュ操作を使用する必要がありますか？
A. 候補構成とマージ
B. テンプレート値を強制します
C. テンプレートを参照テンプレートとして指定します
D. デバイスとネットワークのテンプレートを含める
Answer: (解答を表示する**)**

最新問題: **71**
展示を参照してください。



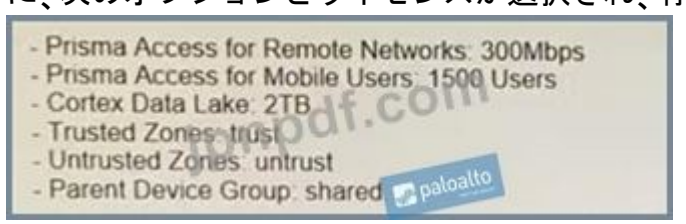
管理者はDNATを使用して、2台のサーバーを1つのパブリックIPアドレスにマップしています。トラフィックは、アプリケーションに基づいて特定のサーバーに誘導されます。ホストA（10.1.1.100）はHTTPトラフィックを受信し、ホストB（10.1.1.101）はSSHトラフィックを受信します。）この構成を実現する2つのセキュリティポリシールールはどれですか。（2つ選択してください。）
A. DMZ（10.1.1.100.10.1.1.101）、ssh、web-browsingへの信頼できない（任意）許可
B. DMZ（1.1.1.100）に対する信頼できない（任意）Webブラウジング許可
C. Untrust（Any）to Untrust（10.1.1.1）、web-browsing -Allow
D. Untrust（Any）to Untrust（10.1.1.1）、SSH -Allow
E. DMZ（1.1.1.100）への信頼できない（任意）SSH-許可
Answer: (解答を表示する**)**

説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

最新問題: **72**
展示を参照してください。

転送された信頼証明書として使用できる証明書はどれですか？
A. ドメインサブCA
B. デフォルトの信頼認証局からの証明書
C. Forward_Trust
D. ドメインルート証明書
Answer: A (メーッセージを残す**)**

最新問題: **73**
お客様が従来のリモートアクセスVPNソリューションを置き換えています。代わりにPrismaAccessが選択されました。オンボーディング中に、次のオプションとライセンスが選択され、有効になりました。



顧客は、モバイルユーザー向けのPrismaAccessに接続しているユーザーによって生成されたログをSplunkSIEMに転送したいと考えています。
お客様が構成する必要がある2つの設定はどれですか？ 2つ選択してください）
A. Splunksyslogサーバーにログを送信するようにPanoramaCollectorグループのデバイスログ転送を設定します
B. Cortex Data Lakeログ転送を構成し、Splunksyslogサーバーを追加します
C. ログ転送プロファイルを構成し、syslogチェックボックスを選択して、Splunksyslogサーバーを追加します。ログ転送プロファイルをMobiie_User_Device_Groupのすべてのセキュリティポリシールールに適用します。
D. ログ転送プロファイルを構成し、[パノラマ/皮質データレイク]チェックボックスを選択します。モバイル_ユーザー_デバイス_グループのすべてのセキュリティポリシールールにログ転送プロファイルを適用します。
Answer: (解答を表示する**)**

最新問題: **74**
パノラマをPAN-OS8.1より前のバージョンに戻すことを計画する場合、管理者は何を考慮する必要がありますか？
A. 変数がテンプレートまたはテンプレートスタックで使用されている場合、Panoramaを以前のPAN-OSリリースに戻すことはできません。
B. 管理者は、Expeditionツールを使用して、構成をPAN-OS8.1より前の状態に適合させる必要があります。
C. Panoramaが以前のPAN-OSリリースに戻されると、テンプレートまたはテンプレートスタックで使用されている変数が自動的に削除されます。
D. 管理者は、変数文字をPAN-OS8.1より前のバージョンに手動で更新する必要があります。
Answer: A (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/81/pan-os/newfeaturesguide/upgrade-to-pan- os-81 / upgradedowngrade-considerations

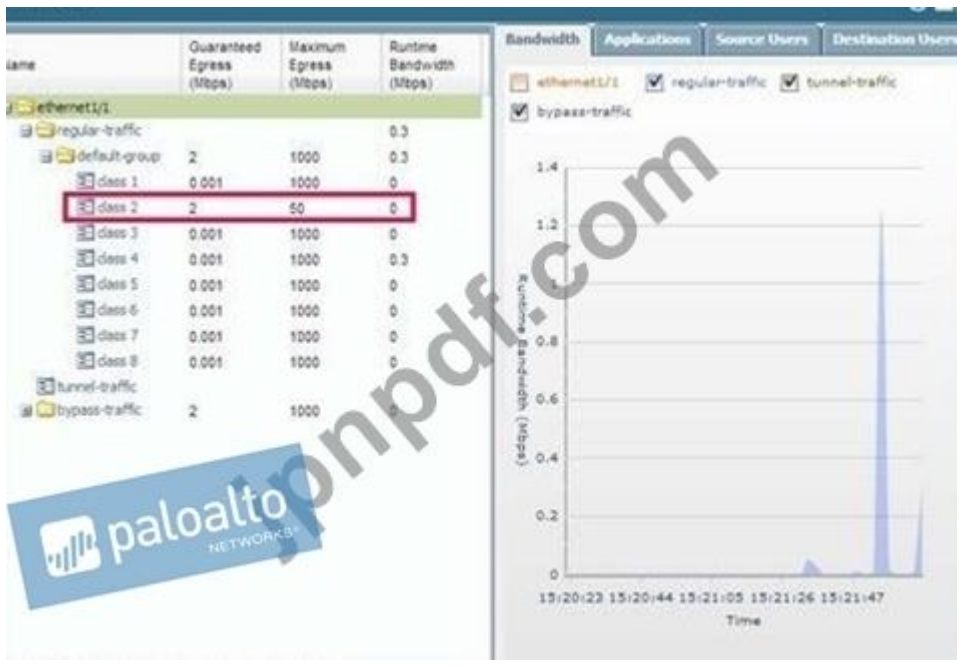
最新問題: **75**
パケットバッファ保護に関する情報はどこに記録されますか？
A. アラートエントリはアラームログにありますドロップされたトラフィック、破棄されたセッション、およびブロックされたIPアドレスのエントリは脅威ログにあります
B. すべてのエントリはシステムログにあります
C. アラートエントリはシステムログにありますドロップされたトラフィック、破棄されたセッション、およびブロックされたIPアドレスのエントリは脅威ログにあります
D. すべてのエントリはアラームログにあります
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNGFCA4

最新問題: **76**
ユーザーが誤って企業のクレデンシャルをフィッシングWebサイトに送信しないようにするには、どの機能を構成する必要がありますか？
A. URLフィルタリングプロファイル
B. ゾーン保護プロファイル
C. スパイウェア対策プロファイル
D. 脆弱性保護プロファイル
Answer: (解答を表示する**)**
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishinフィッシング攻撃防止は、URLフィルタリング機能を拡張して、クラウドを介して標的となるクレデンシャルフィッシング攻撃を積極的に検出しますベースの分析サービス、およびデバイス自体のヒューリスティックを介して。

最新問題: **77**
コンテンツ検査プロセスの一部であるオプションはどれですか？
A. SSLプロキシの再暗号化
B. パケット転送プロセス
C. パケット出力プロセス
D. IPsecトンネル暗号化
Answer: (解答を表示する**)**

最新問題: **78**
お客様は、レイヤ2イーサネットポート用にVLANインターフェイスを設定したいと考えています。
VLANインターフェイスの設定に使用される2つの必須オプションはどれですか。2つ選択してください。）
A. 仮想ルーター
B. セキュリティゾーン
C. ARPエントリ
D. Netflowプロファイル
Answer: B,D (メーッセージを残す**)**
説明/参照：
参照 :https ://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/ network-interfaces / pa-7000-series-layer-2-interface＃idd2bcaacc-54b9-4ec9- a1dd-8064499f5b9d

最新問題: **79**
IT部門は、営業スタッフが電話をかけたり受けたりしているときに、VoIP通話のジッターに関する苦情を受けています。QoSはすべてのファイアウォールインターフェイスで有効になっていますが、ルールベースに記述されたQoSポリシーはありません。IT管理者は、ユーザーがジッターを報告したときに、どのトラフィックがジッターを引き起こしているかをリアルタイムで調べたいと考えています。
最も帯域幅を使用しているアプリケーションをリアルタイムで識別するために使用できる機能はどれですか？
A. QoS統計
B. アプリケーションレポート
C. アプリケーションコマンドセンター ACC）
D. QoSログ
Answer: A (メーッセージを残す**)**
[ネットワーク]>[QoS]を選択して[QoSポリシー]ページを表示し、[統計]リンクをクリックして、QoS帯域幅、選択したQoSノードまたはクラスのアクティブなセッション、および選択したQoSノードまたはクラスのアクティブなアプリケーションを表示します。
たとえば、QoSが有効になっているイーサネット1/1の統計を参照してください。



https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/quality-of-service/configure- qos

最新問題**: 80**
管理者は、ワームやトロイの木馬に対する保護を提供するためにPalo AltoNetworksNGFWを構成するように求められました。
ワームやトロイの木馬から保護するセキュリティプロファイルの種類はどれですか？
A. スパイウェア対策
B. 命令防止
C. アンチウイルス
D. ファイルのブロック
Answer: C (メーッセージを残す**)**

最新問題**: 81**
基本的なWildFireサービスの一部として分析のためにWildFireに転送できる3つのファイルタイプはどれですか？
（3つ選択してください。）
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar
Answer: D,E,F (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

最新問題**: 82**
WebサーバーはDMZでホストされ、サーバーはTCPポート443で着信接続をリッスンするように構成されています。信頼ゾーンからDMZゾーンへのアクセスを許可するセキュリティポリシールールは、Webブラウジングアクセスを許可するように構成する必要がありま

す。Webサーバーは、そのコンテンツをHTTP（S）経由でホストします。信頼からDMZへのトラフィックは、転送プロキシルールで復号化されています。
tcp / 443でこのサーバーへのクリアテキストのWebブラウジングトラフィックを許可するには、サービスとアプリケーションのどの組み合わせ、およびセキュリティポリシールールの順序を構成する必要があります。
A. ルール#1 :アプリケーション :ウェブブラウジング; サービス :サービス-https アクション :ルール#2を許可する :アプリケーション :ssl; サービス :アプリケーションデフォルト; アクション：許可する
B. ルール#1 :アプリケーション :ウェブブラウジング; サービス :アプリケーションデフォルト; アクション :ルール#2を許可する :アプリケーション :ssl; サービス :アプリケーションデフォルト; アクション：許可する
C. ルール#1 :アプリケーション :Webブラウジング; サービス :サービス-http アクション :ルール#2を許可する :アプリケーション :ssl; サービス :アプリケーションデフォルト; アクション：許可する
D. ルール#1 :アプリケーション :ssl; サービス :アプリケーションデフォルト; アクション :ルール#2を許可する :アプリケーション :Webブラウジング; サービス :アプリケーションデフォルト; アクション：許可する
Answer: (解答を表示する**)**

最新問題**: 83**
管理者は、WildFire分析のために新しく見つかったスパイウェアを提出しました。スパイウェアは、ユーザーの知らないうちに動作を受動的に監視します。
WildFireから予想される評決は何ですか？
A. マルウェア
B. 灰色の陶器
C. フィッシング
D. スパイウェア
Answer: (解答を表示する**)**

最新問題**: 84**
GlobalProtect設定画面のキャプチャを表示します。

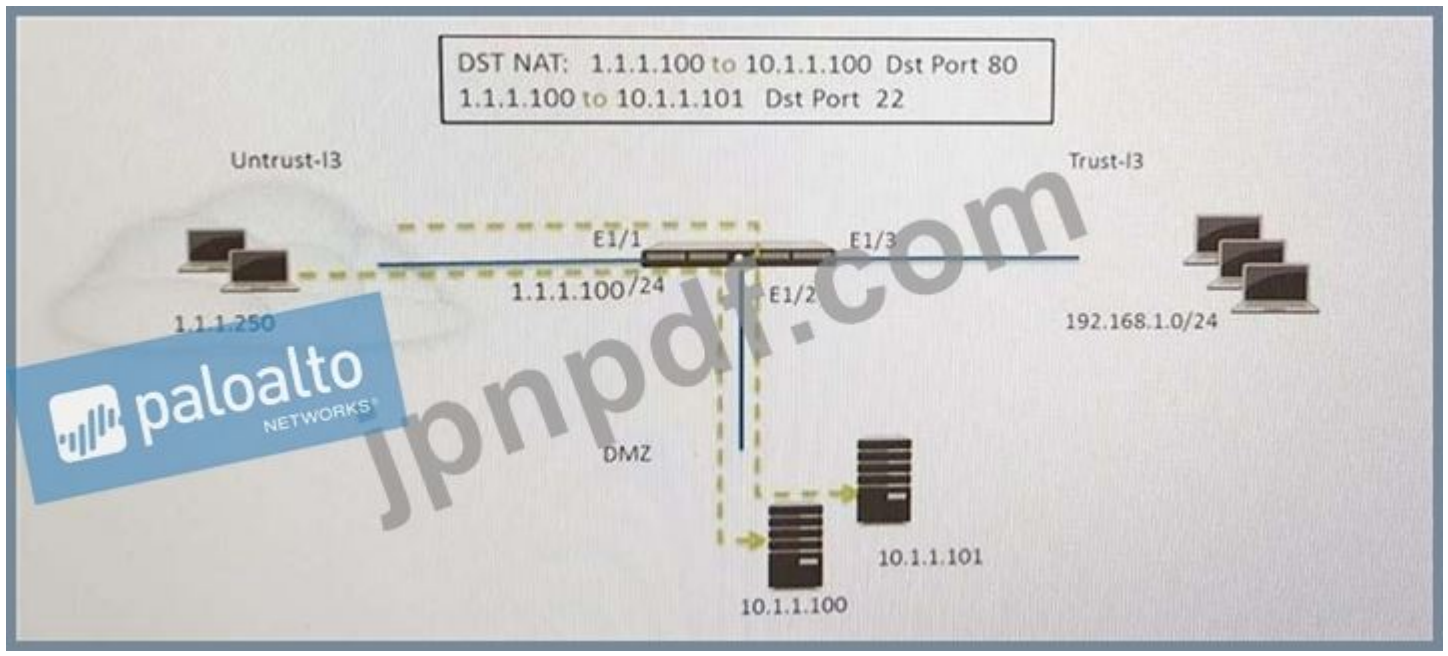
この構成の目的は何ですか？
A. すべての内部クライアントのトンネルアドレスを192.168.10.1から始まるIPアドレス範囲に設定します。
B. 内部クライアントを強制的にIPアドレス192.168.10.1の内部ゲートウェイに接続します。
C. クライアントが192.168.10.1で逆DNSルックアップを実行して、それが内部クライアントであることを検出できるようにします。
D. ファイアウォールに動的DNS更新を実行させ、内部ゲートウェイのホスト名とIPアドレスをDNSサーバーに追加します。
Answer: C (メーッセージを残す**)**
参照：

https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-por the-globalprotect-client-authentication-configurations / define-the-globalprotect-agent-configurations
「このオプションを選択すると、GlobalProtectエージェントがエンタープライズネットワーク内にあるかどうかを判断できます。このオプションは、内部ゲートウェイと通信するように構成されているエンドポイントにのみ適用されます。ユーザーがログインしようとすると、エージェントは指定されたホスト名を指定されたIPアドレスに使用する内部ホスト。ホストは、エンドポイントがエンタープライズネットワーク内にある場合に到達可能な参照ポイントとして機能します。エージェントがホストを検出した場合、エンドポイントはネットワーク内にあり、エージェントはに接続します。内部ゲートウェイ。エージェントが内部ホストを見つけられなかった場合、エンドポイントはネットワークの外部にあり、エージェントは外部ゲートウェイの1つへのトンネルを確立します。」

最新問題: **85**
ネットワークセキュリティエンジニアは、ファイアウォールで返品承認（RMA）を実行するように求められます。Panoramaを使用している交換用ファイアウォールにファイルのどの部分をインポートして戻す必要がありますか？
A. デバイスの状態とライセンスファイル
B. 構成ファイルと統計ファイル
C. 構成および大規模VPN（LSVPN）セットアップファイル
D. 構成およびシリアル番号ファイル
Answer: (解答を表示する**)**

最新問題: **86**
Wildfireのサブスクリプションに基づいて、WildFireに送信できる1日あたりのサンプルの最大数はどれですか。
A. 15,000
B. 10,000
C. 75,00
D. 5,000
Answer: B (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/submit-files-for-wildfire-analysis/manually-uploa
「WildFireAPIは、1日に最大1,000件のファイル送信と最大10,000件のクエリをサポートします。」
https://docs.paloaltonetworks.com/wildfire/9-0/wildfire-admin/wildfire-overview/wildfire-subscription
https://docs.paloaltonetworks.com/wildfire/10-0/wildfire-admin/submit-files-for-wildfire-analysis/manually-uplo

最新問題: **87**
展示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アドレスにマップしています。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誘導されます。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2つのセキュリティポリシールールはどれですか。（2つ選択してください。）

A. DMZ（10.1.1.100.10.1.1.101）、ssh、web-browsingへの信頼できない（任意）許可

B. DMZ（10.1.1.1）に対する信頼できない（任意）ssh -Allow

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

D. DMZ（10.1.1.1）に対する信頼できない（任意）Webブラウジング許可

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

Answer: (解答を表示する)

最新問題**: 88**

WebサーバーはDMZでホストされ、サーバーはTCPポート443で着信接続をリッスンするように構成されています。信頼ゾーンからDMZゾーンへのアクセスを許可するセキュリティポリシールールは、Webブラウジングアクセスを許可するように構成する必要があります。Webサーバーは、そのコンテンツをHTTP（S）経由でホストします。信頼からDMZへのトラフィックは、転送プロキシルールで復号化されています。

tcp / 443でこのサーバーへのクリアテキストWebブラウジングトラフィックを許可するには、サービスとアプリケーションのどの組み合わせ、およびセキュリティポリシールールの順序を構成する必要があります。

A. ルール#1 :アプリケーション :ssl; サービス :アプリケーション-デフォルト; アクション :ルール#2を許可する :アプリケーション :Webブラウジング; サービス :アプリケーション-デフォルト; アクション：許可する

B. ルール#1 :アプリケーション :ウェブブラウジング; サービス :サービス-https; アクション :ルール#2を許可する :アプリケーション :ssl; サービス :アプリケーション-デフォルト; アクション：許可する

C. ルール#1 :アプリケーション :ウェブブラウジング; サービス :サービス-http; アクション :ルール#2を許可する :アプリケーション :ssl; サービス :アプリケーション-デフォルト; アクション：許可する

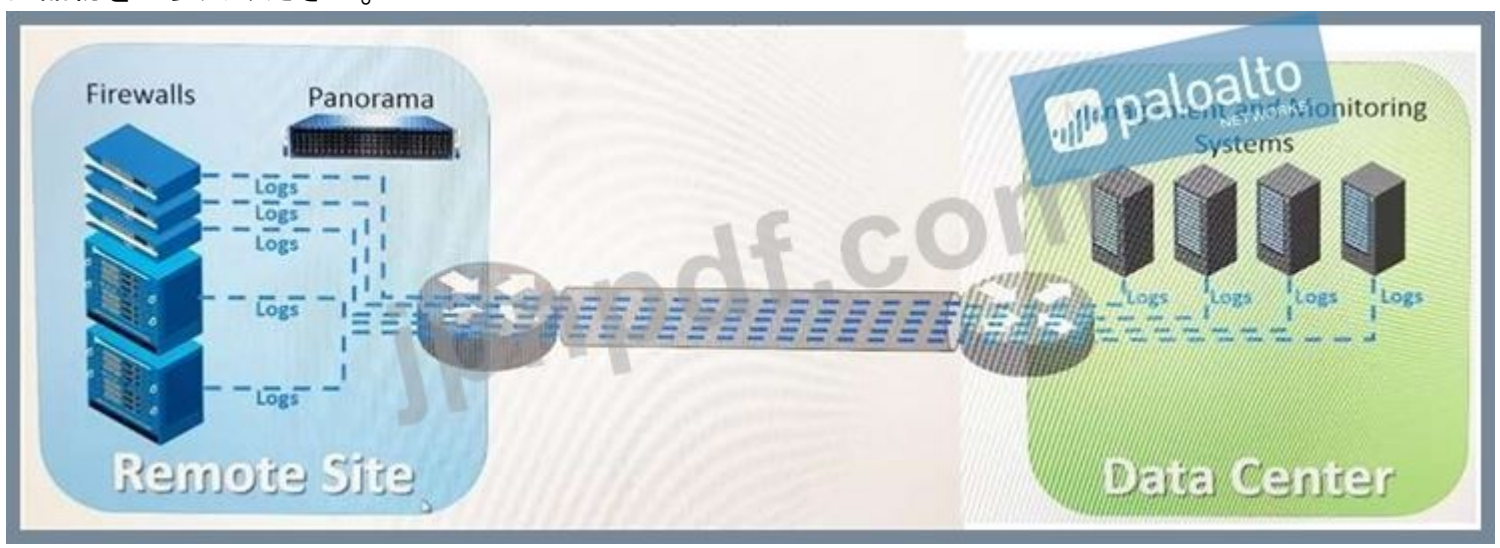
D. ルール#1 :アプリケーション :ウェブブラウジング; サービス :アプリケーション-デフォルト; アクション :ルール#2を許可する：アプリケーション :ssl; サービス :アプリケーション-デフォルト; アクション：許可する

Answer: (解答を表示する)

最新問題: **89**
新規および変更されたApp-IDを組み込むための2つのベストプラクティスは何ですか？ 2つ選択してください。）
A. サポートされているリリースツリーで最新のPAN-OSバージョンを実行して、新しいApp-IDのパフォーマンスを最高にします。
B. ネットワーク全体に影響を与える可能性のある新しいApp-IDを許可するようにセキュリティポリシールールを構成します
C. ベストプラクティス評価を実行して、新規または変更されたApp-IDの影響を評価します
D. リリースノートを調べて、影響が少ないと判断された場合は新しいApp-IDをインストールします
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: **90**
管理者には750のファイアウォールがあります管理者の中央管理Panoramaインスタンスは、動的更新をファイアウォールに展開します管理者は、Panoramaが動的更新スケジュールの構成を管理対象ファイアウォールにプッシュした場合、Panoramaからの動的更新が一部のファイアウォールに表示されないことに気付きます。構成が表示されない根本的な原因は何ですか？
A. ファイアウォール上にパロアルトネットワークス更新サーバーへのサービスルートが構成されていません
B. パノラマには動的更新をプッシュするための有効なライセンスがありません
C. パノラマはパロアルトネットワークスの更新サーバーに接続していません
D. ローカルで定義された動的更新設定は、Panoramaがプッシュした設定よりも優先されます
Answer: D (メーッセージを残す**)**

最新問題: **91**
出品物をご参照ください。



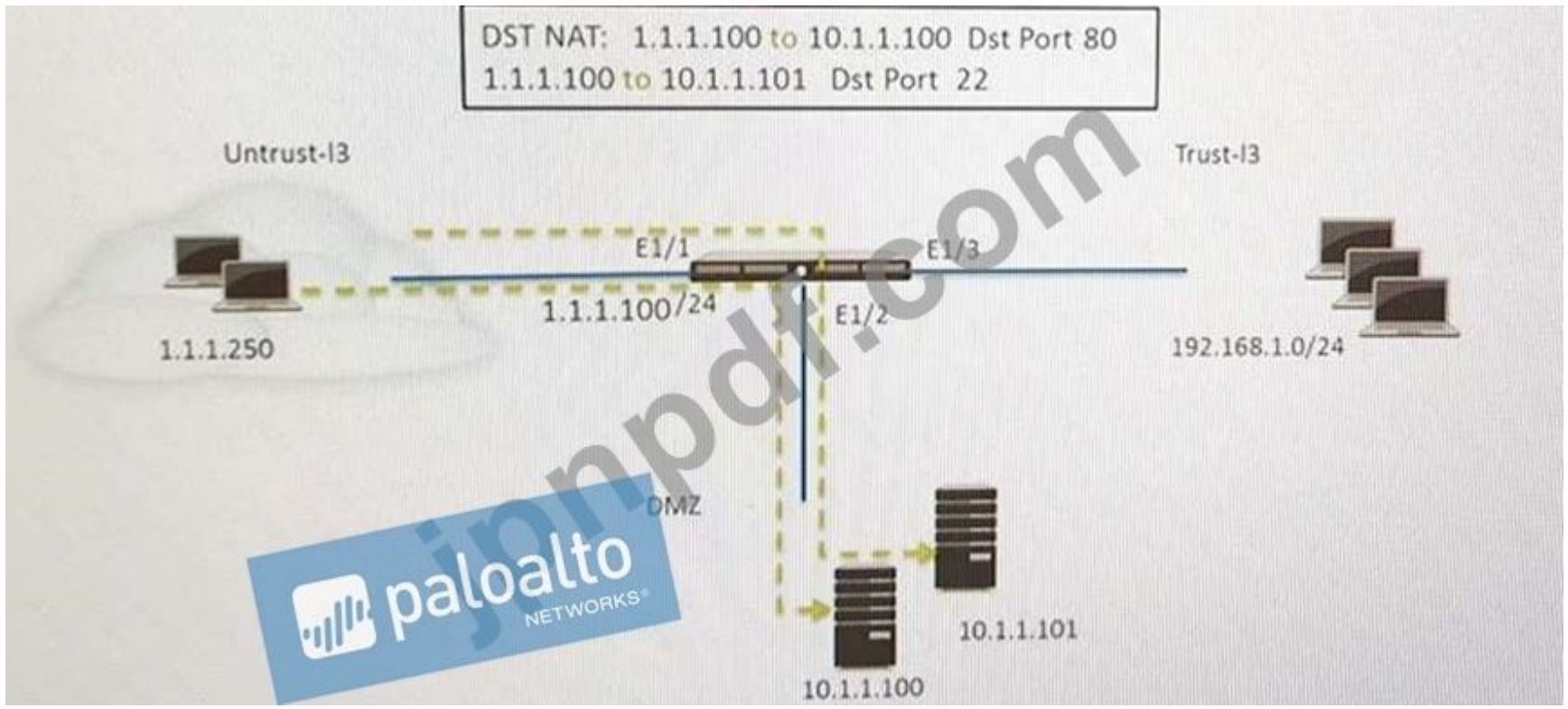
組織には、リモート監視およびセキュリティ管理プラットフォームにログを送信するパロアルトネットワークスNGFWがあります。ネットワークチームは、企業WANでの過剰なトラフィックを報告しました。
パロアルトネットワークスのNGFW管理者は、既存のすべての監視/セキュリティプラットフォームのサポートを維持しながら、WANトラフィックをどのように削減できますか？
A. 相関のために外部ソースからPanoramaにログを転送し、PanoramaからログをNGFWに送信します。
B. ファイアウォールからPanoramaにのみログを転送し、Panoramaが他の外部サービスにログを転送するようにします。
C. すべてのリモートファイアウォールでログ圧縮および最適化機能を構成します。

D. M-500の構成は、不十分な帯域幅の問題に対処します。
Answer: B (メーッセージを残す**)**

最新問題**: 92**
Palo Alto Networks NGFWにユーザー名とロール名の両方を提供するために変更できる3つのユーザー認証サービスはどれですか？ 3つ選択してください。）
A. TACACS +
B. Kerberos
C. PAP
D. LDAP
E. SAML
F. RADIUS
Answer: B,D,E (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat

最新問題**: 93**
PAN-OS®ソフトウェアがアプリケーションを識別するために使用する2つの機能はどれですか？ 2つ選択してください）
A. ポート番号
B. セッション番号
C. トランザクション特性
D. アプリケーション層のペイロード
Answer: A,D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/app-id/application-level-gateways#

最新問題**: 94**
展示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アドレスにマップしています。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誘導されます。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2つのセキュリティポリシールールはどれですか？（2つ選択してください）
A. DMZ（1.1.1.100）への信頼できない（任意）Webブラウジング許可
B. 信頼できない（任意）から信頼できない（10.1.1.1）Webブラウジング許可
C. Untrust（Any）to Untrust（10.1.1.1）Ssh-Allow
D. DMZ（1.1.1.100）への信頼できない（任意）Ssh-許可
Answer: (解答を表示する**)**

最新問題**: 95**
セキュリティプロファイルを作成するときに使用できる3つのオプションはどれですか？（3つ選択してください）
A. マルウェア対策
B. ファイルのブロック
C. URLフィルタリング
D. IDS / ISP
E. 脅威の防止
F. アンチウイルス
Answer: B,C,F (メーッセージを残す**)**
URLカテゴリを一致基準として使用すると、URLカテゴリごとにセキュリティプロファイル（ウイルス対策、スパイウェア対策、脆弱性、ファイルブロッキング、データフィルタリング、およびDoS）をカスタマイズできます。

最新問題**: 96**

管理者は、Palo AltoNetworksNGFWを最新バージョンのPAN-OS®ソフトウェアにアップグレードする必要があります。ファイアウォールにはイーサネットインターフェイスを介したインターネット接続がありますが、管理インターフェイスからのインターネット接続はありません。セキュリティポリシーには、デフォルトのセキュリティルールと、任意のゾーンから任意のゾーンへのすべてのWebブラウジングトラフィックを許可するルールがあります。PAN-OS®ソフトウェアをアップグレードできるように、管理者は何を構成する必要がありますか？

A. CRL
B. スケジューラ
C. サービスルート
D. セキュリティポリシールール
Answer: D (メーッセージを残す**)**

最新問題**: 97**
ブートストラップUSBフラッシュドライブは、以前にラボで使用されていたPalo Alto Networksファイアウォールの初期構成をロードするために、Windowsワークステーションを使用して準備されています。USBフラッシュドライブはファイルシステムFAT32を使用してフォーマットされ、初期構成はinit-cfgtxtという名前のファイルに保存されます。ファイアウォールは現在PAN-OS10.0を実行しており、ラボ構成を使用しています。USBフラッシュドライブのinit-cfgtxiの内容は次のとおりです。

USBフラッシュドライブがファイアウォールのUSBポートに挿入され、次のコマンドを使用してファイアウォールが再起動されました。> request Resort system再起動時に、ファイアウォールはブートストラッププロセスの開始に失敗します。失敗の原因は

A. ファイアウォールは工場出荷時のデフォルト状態であるか、ブートストラップのためにすべてのプライベートデータを削除する必要があります
B. ホスト名は必須パラメーターですが、init-cfgtxtにありません
C. USBはext3ファイルシステムを使用してフォーマットする必要があります。FAT32はサポートされていません
D. PANOSのバージョンは少なくとも91.xである必要がありますが、ファイアウォールは10.0.xを実行しています
E. bootstrap.xmlファイルは必須ファイルですが、欠落しています
Answer: C (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootst

最新問題: **98**
スリータブデモを成功させるための3つの重要な要素は何ですか？（正解を3つ選択してください。）
A. パロアルトネットワークスのファイアウォールがアプリケーションの可視性とそれらのアプリケーションの制御をどのように提供するかを示します
B. [ネットワーク]タブと[デバイス]タブに情報を表示する
C. 最近発生した脅威を可視化し、それらの脅威をブロックする方法を示します
D. [オブジェクト]タブで一致基準を設定した後、そのデータがログにどのように表示されるかを示します
E. どのユーザーがどのアプリケーションを実行しているかを示し、ユーザーによるアプリケーションアクセスを制御する方法を提供します
Answer: A,C,E (メーッセージを残す**)**

最新問題: **99**
マシン証明書の配布と使用が必要なGlobalProtectクライアント接続方法はどれですか？
A. オンデマンド
B. ユーザーログオン（常時オン）
C. 起動時
D. ログオン前
Answer: D (メーッセージを残す**)**

最新問題: **100**
Webサイトhttps://www.microsoft.comからの復号化されたパケットは、トラフィックログ内のどのアプリケーションとサービスとして表示されますか？
A. ウェブブラウジングと443
B. SSLおよび80
C. SSLおよび443
D. ウェブブラウジングと80
Answer: A (メーッセージを残す**)**
説明
SSL復号化により、暗号化されていないトラフィックを可視化できるはずです。
したがって、復号化されたトラフィックは、SSLとしてではなく、Webブラウジング、Facebookベースなどの基盤となるアプリケーションとして識別されると予想されます。

最新問題: **101**
管理者は、パロアルトネットワークスNGFWと中央管理パノラマバージョンのアップグレードを検討しています
このシナリオのベストプラクティスと見なされるものは何ですか？
A. パノラマとファイアウォールのアップグレードを同時に実行します
B. デバイスの状態をエクスポートして更新を実行してから、デバイスの状態をインポートします
C. ファイアウォールをアップグレードするには、最初に少なくとも24時間待ってから、Panoramaバージョンをアップグレードします
D. パノラマをターゲットファイアウォールバージョン以上のバージョンにアップグレードします

Answer: (解答を表示する)

最新問題: **102**
次の画像に表示されている証明書情報は、どのタイプの証明書ですか？

A. パブリックCA署名付き証明書
B. Webサーバー証明書
C. 転送信頼証明書
D. 自己署名ルートCA証明書
Answer: D (メーッセージを残す)

最新問題: **103**
出品物をご参照ください。

組織には、リモート監視およびセキュリティ管理プラットフォームにログを送信するパロアルトネットワークスNGFWがあります。ネットワークチームは、企業WANでの過剰なトラフィックを報告しました。
パロアルトネットワークスのNGFW管理者は、既存のすべての監視/セキュリティプラットフォームのサポートを維持しながら、WANトラフィックをどのように削減できますか？
A. ファイアウォールからPanoramaにのみログを転送し、Panoramaが他の外部サービスにログを転送するようにします。
B. 相関のために外部ソースからPanoramaにログを転送し、PanoramaからログをNGFWに送信します。
C. すべてのリモートファイアウォールでログ圧縮および最適化機能を構成します。
D. M-500の構成は、不十分な帯域幅の問題に対処します。
Answer: A (メーッセージを残す)
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and-reporting
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKFCA0
帯域幅が制限されているWANリンクを介してこれを行う必要がある場合は、リンクを介して送信されるログストリームの数を減らすことを検討する必要があります」この構成では、ファイアウォールは、ログ転送がファイアウォールで正しく構成されています。ログはsyslogサーバーに転送されるため、ログストリームの数が大幅に削減されます。」

最新問題: **104**
セキュリティポリシーの一致のためにサービスを使用することとアプリケーションを使用することの違いは何ですか？
A. 「サービス」を使用すると、ファイアウォールはポート番号に基づいて最初に監視されたパケットに対して即座にアクションを実行できます。「アプリケーション」を使用すると、使用されているポートがアプリケーションの標準ポートリストのメンバーである場合、ファイアウォールは即座にアクションを実行できます。
B. 「サービス」と「アプリケーション」に違いはありません。「アプリケーション」を使用すると、ポート番号の代わりにわかりやすいアプリケーション名を使用できるようになるため、構成が簡素化されます。
C. 「サービス」を使用すると、ファイアウォールはポート番号に基づいて最初に監視されたパケットに対して即座にアクションを実行できます。「アプリケーション」を使用すると、使用されているポートに関係なく、十分なパケットがApp-IDの識別を可能にした後、ファイアウォールがアクションを実行できます。
D. 「サービス」を使用すると、十分なパケットがApp-IDの識別を可能にした後、ファイアウォールがアクションを実行できるようになります
Answer: A (メーッセージを残す)

説明/参照：

最新問題: **105**
M-100アプライアンスをログコレクターとして構成するには、どの2つのオプションが必要ですか？ 2つ選択してください）
A. パノラマGUIの[パノラマ]タブから[ログコレクターモード]を選択し、変更をコミットします
B. コマンドリクエストシステムシステムモードロガーを入力し、Yを入力してログコレクターモードへの変更を確認します。
C. パノラマGUIの[デバイス]タブから[ログコレクターモード]を選択し、変更をコミットします。
D. コマンドlogger-modeを入力し、Yを入力して、ログコレクターモードへの変更を確認します。
E. 専用のログコレクターのPanoramaCLIにログインします
Answer: (解答を表示する)
（https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up- panorama / set-up-the-m-100-appliance）

最新問題: **106**
ethernetl / 8に接続されている物理メディアを表示するCLIコマンドはどれですか？
A. >システム状態フィルターを表示かなりsys.si.p8.stats
B. > show interface ethernetl / 8
C. >システム状態フィルターを表示かなりsys.sl.p8.phy
D. >システム状態フィルターを表示かなりsys.si.p8.med
Answer: D (メーッセージを残す)
説明
出力例：
>システム状態フィルターを表示かなりsys.s1.p1.phy
sys.s1.p1.phy :{
リンクパートナー :{}、
メディア :CAT5、
タイプ :イーサネット、
}
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC

最新問題: **107**
ファイアウォールがパケットフローシーケンスの一部としてパケットを破棄する理由は2つありますか？ 2つ選択してください）
A. 等コストマルチパス
B. 入力処理エラー

C. アクション 「許可」とのルールー致
D. アクション 「拒否」とのルールー致
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0トラフィックを拒否すると、パケットが破棄されます。フレーム、データグラム、またはパケットの形式が正しくないか正しくないために、パケットが破棄されることもあります。

最新問題**: 108**
ファイアウォールがパケットフローシーケンスの一部としてパケットを破棄する理由は2つありますか？ 2つ選択してください）
A. 等コストマルチパス
B. 入力処理エラー
C. アクション 「許可」とのルールー致
D. アクション 「拒否」とのルールー致
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0トラフィックを拒否すると、パケットが破棄されます。フレーム、データグラム、またはパケットの形式が正しくないか正しくないために、パケットが破棄されることもあります。

最新問題**: 109**
管理者は、アクティブな脅威防止サブスクリプションを備えたPA-820ファイアウォールを持っています。管理者は、WildFireサブスクリプションの追加を検討しています。WildFireサブスクリプションを追加すると、組織のセキュリティ体制がどのように改善されますか1。
A. WildFireとThreat Preventionを組み合わせて、ファイアウォールに最大限のセキュリティ体制を提供します
B. WildFireとThreat Preventionを組み合わせて、攻撃対象領域を最小限に抑えます
C. 24時間後、WildFireシグネチャがウイルス対策アップデートに含まれます
D. 未知のマルウェアに対する保護をほぼリアルタイムで提供できます
Answer: B (メーッセージを残す**)**

最新問題**: 110**
ブートストラップUSBフラッシュドライブは、以前にラボで使用されていたPalo Alto Networksファイアウォールの初期構成をロードするために、Windowsワークステーションを使用して準備されています。USBフラッシュドライブはファイルシステムFAT32を使用してフォーマットされ、初期構成はinit-cfgtxtという名前のファイルに保存されます。ファイアウォールは現在PAN-OS10.0を実行しており、ラボ構成を使用しています。USBフラッシュドライブのinit-cfgtxiの内容は次のとおりです。

USBフラッシュドライブがファイアウォールのUSBポートに挿入され、次のコマンドを使用してファイアウォールが再起動されました。> request Resort system再起動時に、ファイアウォールはブートストラッププロセスの開始に失敗します。失敗の原因は

A. ファイアウォールは工場出荷時のデフォルト状態であるか、ブートストラップのためにすべてのプライベートデータを削除する必要があります

B. ホスト名は必須パラメーターですが、init-cfgtxtにありません

C. USBはext3ファイルシステムを使用してフォーマットする必要があります。FAT32はサポートされていません

D. PANOSのバージョンは少なくとも91.xである必要がありますが、ファイアウォールは10.0.xを実行しています

E. bootstrap.xmlファイルは必須ファイルですが、欠落しています

Answer: C (メーッセージを残す**)**

https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/bootstrap-the-firewall/bootstrap-a-firewall-using-a-usb-flash-drive。html#id8378007f-d6e5-4f2d-84a4-5d50b0b3ad7d

最新問題**: 111**

pcapフィルターに含めることができる3つのフィールドはどれですか？ 3つ選択してください）

A. 出力インターフェース

B. ソースIP

C. ルール番号

D. 宛先IP

E. 入力インターフェース

Answer: (解答を表示する**)**

説明

（https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069）

最新問題**: 112**

ICMPパケットの送信元アドレスは何になりますか？

A. 10.30.0.93

B. 10.46.72.93

C. 192.168.93.1

D. 10.46.64.94

Answer: D (メーッセージを残す)

最新問題: **113**

企業は、ファイアウォールを事前に構成して、最小量のリモートサイトに送信する必要があります。

事前設定。導入後、各ファイアウォールは複数の地域に戻る安全なトンネルを確立する必要があります

将来の地域データセンターを含むデータセンター。

将来のサイトに展開するときに、どのVPN構成が変更に適応しますか？

A. 事前設定されたGlobalProtectクライアント

B. 事前設定されたGlobalProtect衛星

C. 事前設定されたPPTPトンネル

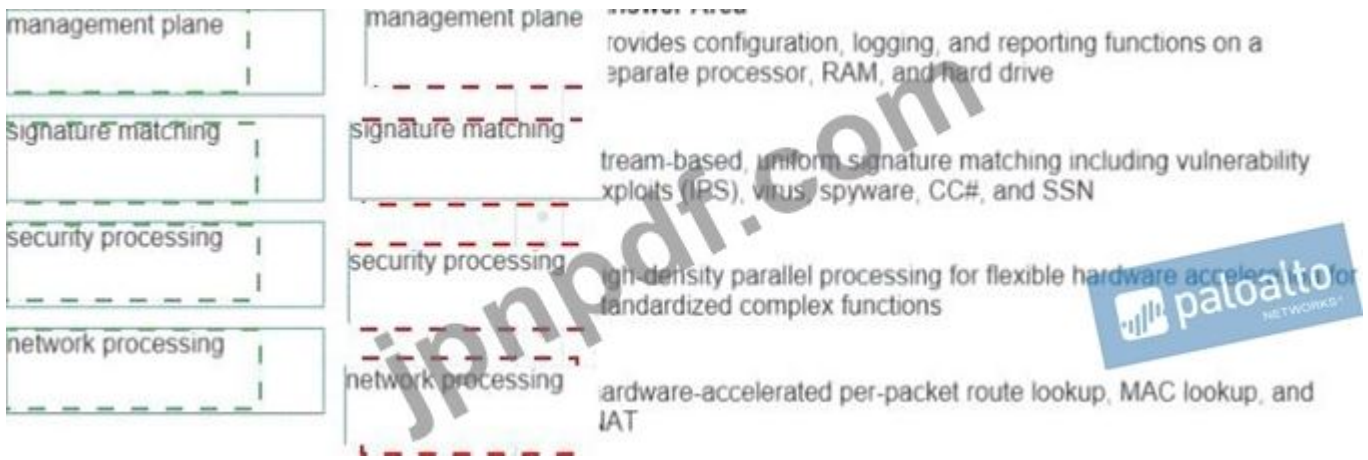
D. 事前設定されたIPsecトンネル

Answer: B (メーッセージを残す)

最新問題: **114**

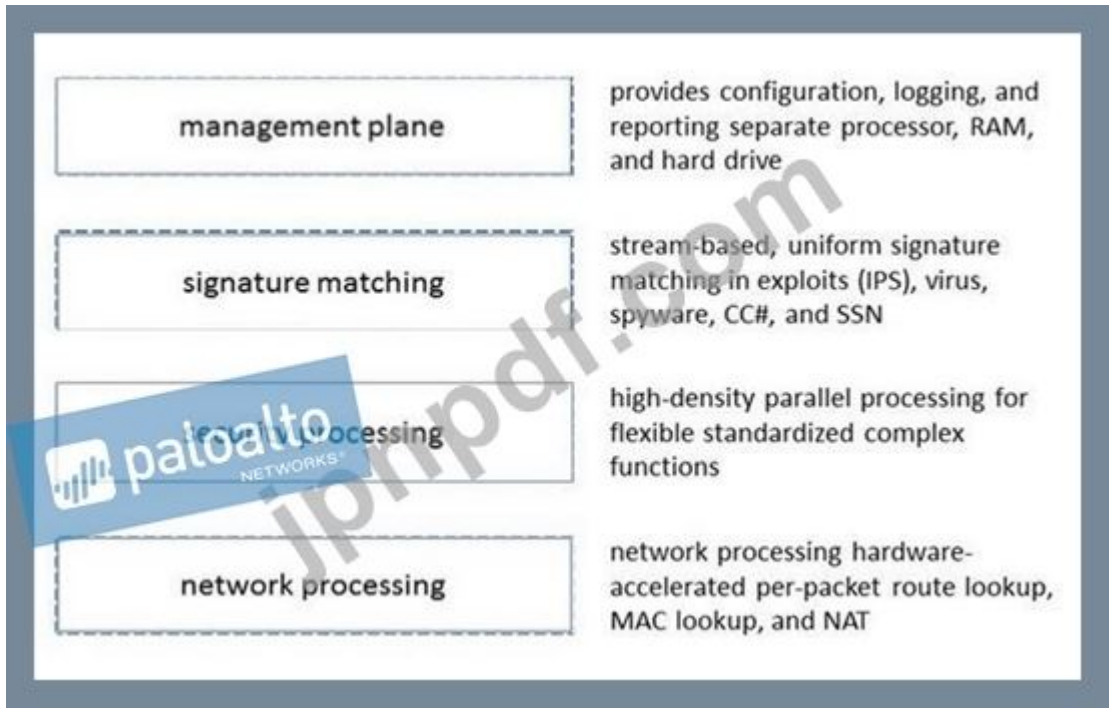
用語を対応する定義と一致させてください。

Answer:



説明

中程度の信頼度で自動生成されたグラフィカルユーザーインターフェイスの説明



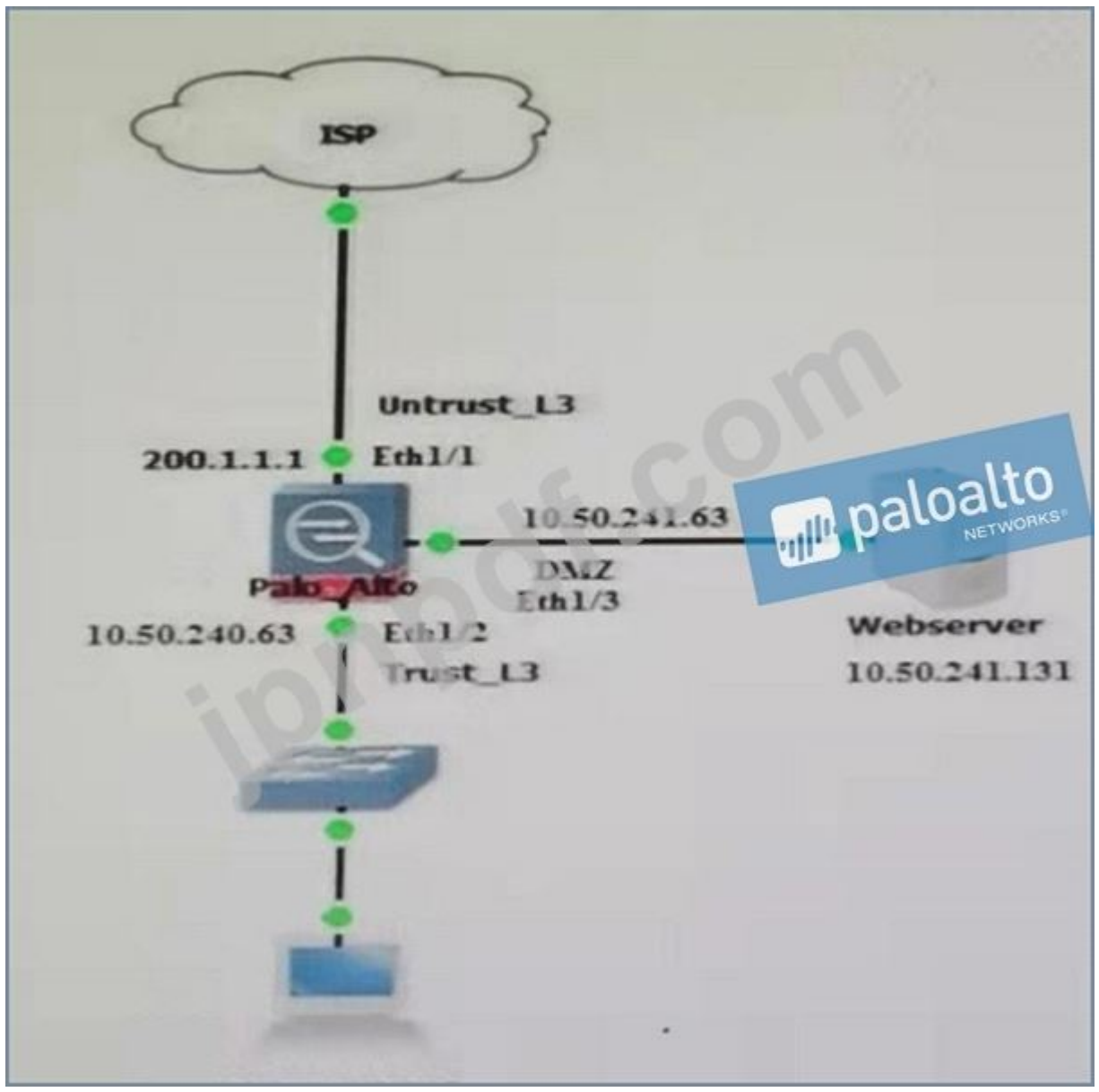
最新問題: 115

セキュリティポリシーの優先度を最高にするには、管理者はデバイスグループ階層でセキュリティポリシーをどのように構成する必要がありますか？
A. 共有デバイスグループにポリシーを事前ルールとして追加します
B. ターゲットデバイスグループ内のターゲットデバイスのテンプレートを参照します
C. ポリシーをターゲットデバイスグループに追加し、マスターデバイスをデバイスグループに適用します
D. セキュリティポリシーのクローンを作成し、他のデバイスグループに追加します
Answer: A (メーッセージを残す)
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy.html

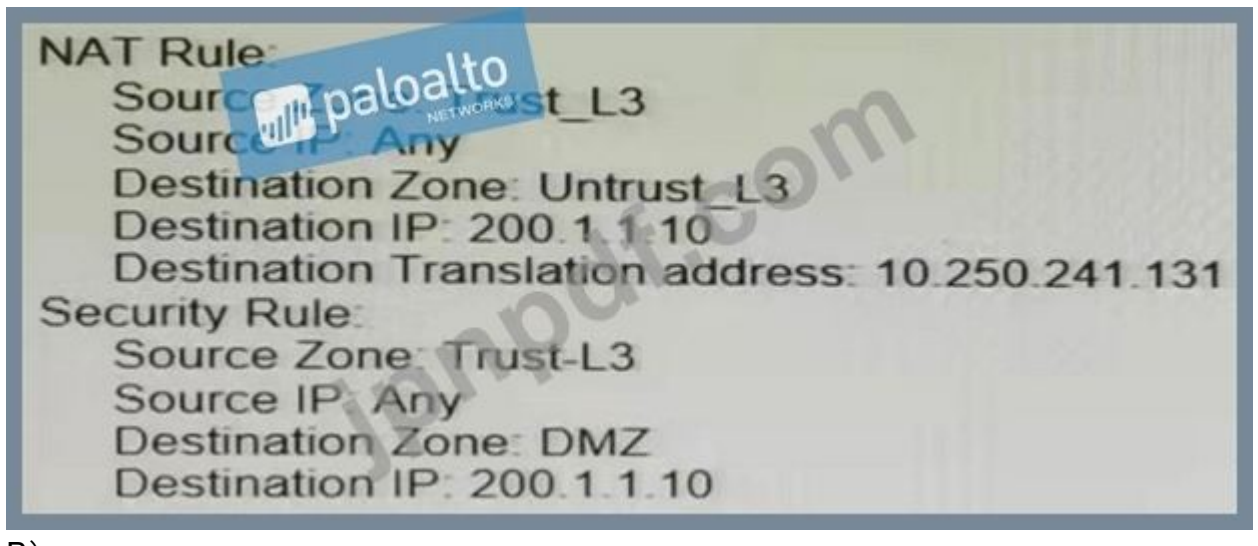
最新問題**: 116**
SAML SLOは、どの2つのファイアウォール機能でサポートされていますか？ 2つ選択してください。）
A. GlobalProtectポータル
B. キャプティブポータル
C. WebUI
D. CLI
Answer: A,B (メーッセージを残す)
説明
SSOは、Webインターフェイスにアクセスする管理者、およびGlobalProtectまたはキャプティブポータルを介してアプリケーションにアクセスするエンドユーザーが利用できます。SLOは、管理者とGlobalProtectエンドユーザーが利用できますが、キャプティブポータルのエンドユーザーは利用できません。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/authentication-types/saml
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/device/device-server-profiles-saml-ide

最新問題**: 117**
HA Liteでサポートされている3つのオプションはどれですか？ 3つ選択してください。）
A. 仮想リンク
B. アクティブ/パッシブ展開
C. IPsecセキュリティアソシエーションの同期
D. 構成の同期
E. セッションの同期
Answer: B,C,D (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-high-availability

最新問題**: 118**
内部システムのユーザーは、でプライベートIPが10 250241131のWebサーバーをDNSサーバーに照会します。DNSサーバーは、Webサーバーのパブリックアドレス200.1.1.10のアドレスを返します。
Webサーバーにアクセスするには、ファイアウォールでどのセキュリティルールとUターンNATルールを構成する必要がありますか？


ISP
Untrust_L3
200.1.1.1
Eth1/1
10.50.241.63
DMZ
Eth1/3
Palo_Alto
10.50.240.63
Eth1/2
Trust_L3
Webserver
10.50.241.131

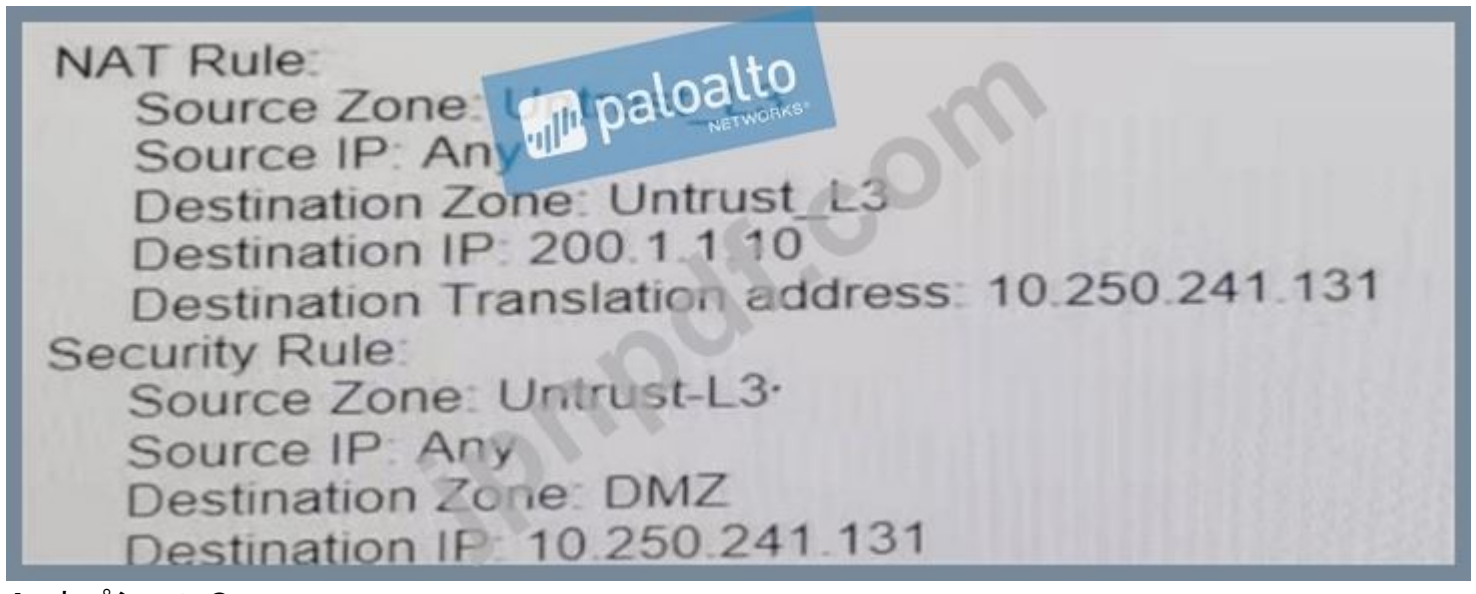
A)


NAT Rule:
Source Zone: Trust_L3
Source IP: Any
Destination Zone: Untrust_L3
Destination IP: 200.1.1.10
Destination Translation address: 10.250.241.131
Security Rule:
Source Zone: Trust-L3
Source IP: Any
Destination Zone: DMZ
Destination IP: 200.1.1.10

B)

C)

D)



A. オプションC

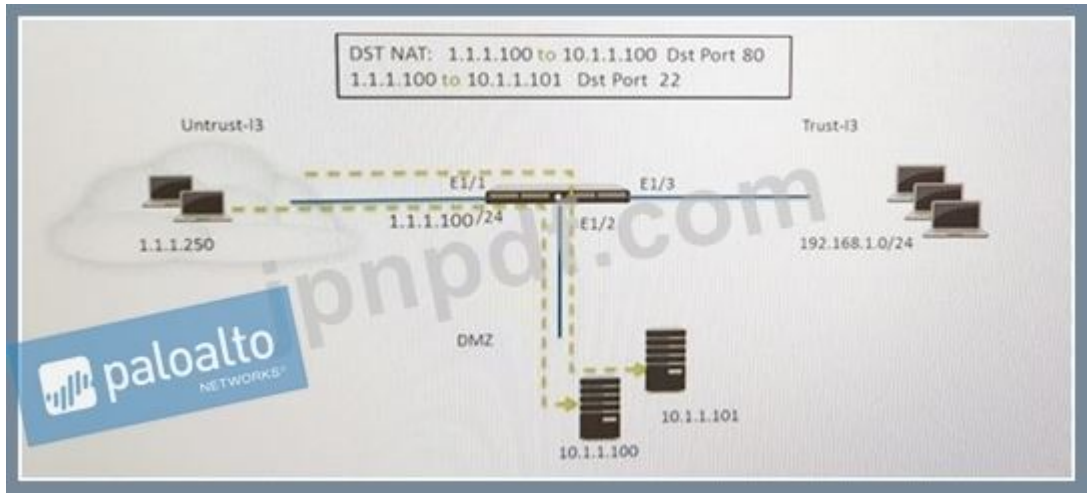
B. オプションB

C. オプションD

D. オプションA

Answer: D (メーッセージを残す**)**

最新問題: **119**
展示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アドレスにマップしています。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誘導されます。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2つのセキュリティポリシールールはどれですか。（2つ選択してください。）

A. Untrust（Any）to Untrust（10.1.1.1）、web-browsing -Allow

B. Untrust（Any）to Untrust（10.1.1.1）、ssh -Allow

C. DMZ（10.1.1.1）に対する信頼できない（任意）Webブラウジング許可

D. DMZ（10.1.1.1）に対する信頼できない（任意）ssh -Allow

E. DMZ（10.1.1.100.10.1.1.101）、ssh、web-browsingへの信頼できない（任意）許可

Answer: C,D (メーッセージを残す)

https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-many-mapping#

最新問題: **120**
管理者は、WildFire分析のために新しく見つかったスパイウェアを提出しました。スパイウェアは、ユーザーの知らないうちに動作を監視します。
WildFireから予想される評決は何ですか？

A. マルウェア

B. グレイウェア

C. フィッシング

D. スパイウェア

Answer: (解答を表示する)

説明/参照：

最新問題: **121**
ネットワークセキュリティエンジニアがMicrosoftAzureでブートストラップパッケージを構成しようとしましたが、仮想マシンのプロビジョニングプロセスが失敗しました。ブートストラップパッケージを確認したところ、エンジニアは次のディレクトリしか持っていませんでした：/ config、/licenseおよび/software AzureのVM-Seriesファイアウォールでブートストラッププロセスが失敗したのはなぜですか？

A. ブートストラップパッケージに/contentフォルダーがありません
B. VM-SeriesファイアウォールがPanoramaに事前登録されておらず、ブートストラッププロセスが正常に完了できませんでした
C. /configまたは/softwareフォルダーには、正常にブートストラップするための必須ファイルがありませんでした
D. すべてのパブリッククラウド展開では、適切なファイアウォールネイティブ統合をサポートするために/pluginsフォルダーが必要です
Answer: A (メーッセージを残す**)**

最新問題: **122**
ターミナルサーバーを介して接続しているユーザーのユーザー名にIPアドレスをマップするには、どのユーザーID方式を構成する必要がありますか？
A. ポートマッピング
B. サーバー監視
C. クライアントプロービング
D. XFFヘッダー
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/user-id/map-ip-addresses-to-users/configure-user-mapping-for-terminal-server-ユーザー

最新問題: **123**
管理者がアプリケーションオーバーライドポリシーを使用すると、どのイベントが発生しますか？
A. 脅威IDの処理時間が短縮されます。
B. Palo Alto Networks NGFWは、レイヤー4でApp-ID処理を停止します。
C. セキュリティルールによってトラフィックに割り当てられたアプリケーション名がトラフィックログに書き込まれます。
D. App-IDの処理時間が長くなります。
Answer: (解答を表示する**)**
参照：
https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#

最新問題: **124**
ローカルファイアウォールで対応する管理者アカウントを定義せずに、管理者がPalo Alto Networks NGFWに対して管理者を認証するために使用できる3つの認証サービスはどれですか？ 3つ選択してください。）
A. PAP
B. SAML

C. RADIUS
D. LDAP
E. TACACS +
F. Kerberos
Answer: B,D,F (メーッセージを残す)

最新問題**: 125**
外部Webサイトへのエンドユーザー SSLトラフィックを制御するルールタイプはどれですか？
A. SSL転送プロキシ
B. SSLインバウンド検査
C. SSLアウトバウンドプロキシレス検査
D. SSHプロキシ
Answer: B (メーッセージを残す)

最新問題**: 126**
PAN-OSバージョン9.1以降、アプリケーションの依存関係情報がどの新しい場所で報告されるようになりましたか？ 2つ選択してください。）
A. [コミットステータス]ウィンドウの[アプリの依存関係]タブ
B. セキュリティポリシールール作成ウィンドウの[アプリケーション]タブ
C. オブジェクト>アプリケーションブラウザページ
D. ポリシーオプティマイザの[ルールの使用法]ページ
Answer: A,B (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-app

最新問題**: 127**
パノラマテンプレートでは、どの3種類のオブジェクトを構成できますか？ 3つ選択してください）
A. セキュリティプロファイル
B. 証明書プロファイル
C. QoSプロファイル
D. インターフェース管理プロファイル
E. HIPオブジェクト
Answer: B,C,D (メーッセージを残す)

最新問題**: 128**
アクセスルート、宛先ドメイン、およびアプリケーションによるスプリットトンネリングを有効にするには、どのGlobalProtectゲートウェイ設定が必要ですか？
A. ローカルネットワークへの直接アクセスなし
B. 衛星モード
C. トンネルモード

D. IPSecモード
Answer: A (メーッセージを残す**)**
https://docs.paloaltonetworks.com/globalprotect/9-1/globalprotect-admin/globalprotect-gateways/split-tunnel-traffic-on-globalprotect-gateways/configure-a-split-tunnel-based-on-the- access-route.html

最新問題**: 129**
パロアルトネットワークスNGFWは、分析のためにファイルをWildFireに送信しました。の5分のウィンドウを想定します
分析。ファイアウォールは、5分ごとに判定をチェックするように構成されています。
ファイアウォールはどのくらいの速さで評決を受け取りますか？
A. 5分
B. 10〜15分
C. 5〜10分
D. 15分以上
Answer: (解答を表示する**)**

最新問題**: 130**
イーサネット1/4に接続されているホストは、デフォルトゲートウェイにpingを実行できません。ダッシュボードのウィジェットには、イーサネット1/1とイーサネット1/4が緑色で表示されます。
イーサネット1/1のIPアドレスは192.168.1.7で、イーサネット1/4のIPアドレスは10.1.1.7です。デフォルトゲートウェイはイーサネット1/1に接続されています。デフォルトルートは適切に設定されています。
この問題の原因は何でしょうか？
A. イーサネット1/4にゾーンが設定されていません。
B. DNSがホストで正しく構成されていません。
C. DNSがファイアウォールで適切に構成されていません。
D. インターフェイスイーサネット1/1は仮想ワイヤモードです。
Answer: A (メーッセージを残す**)**

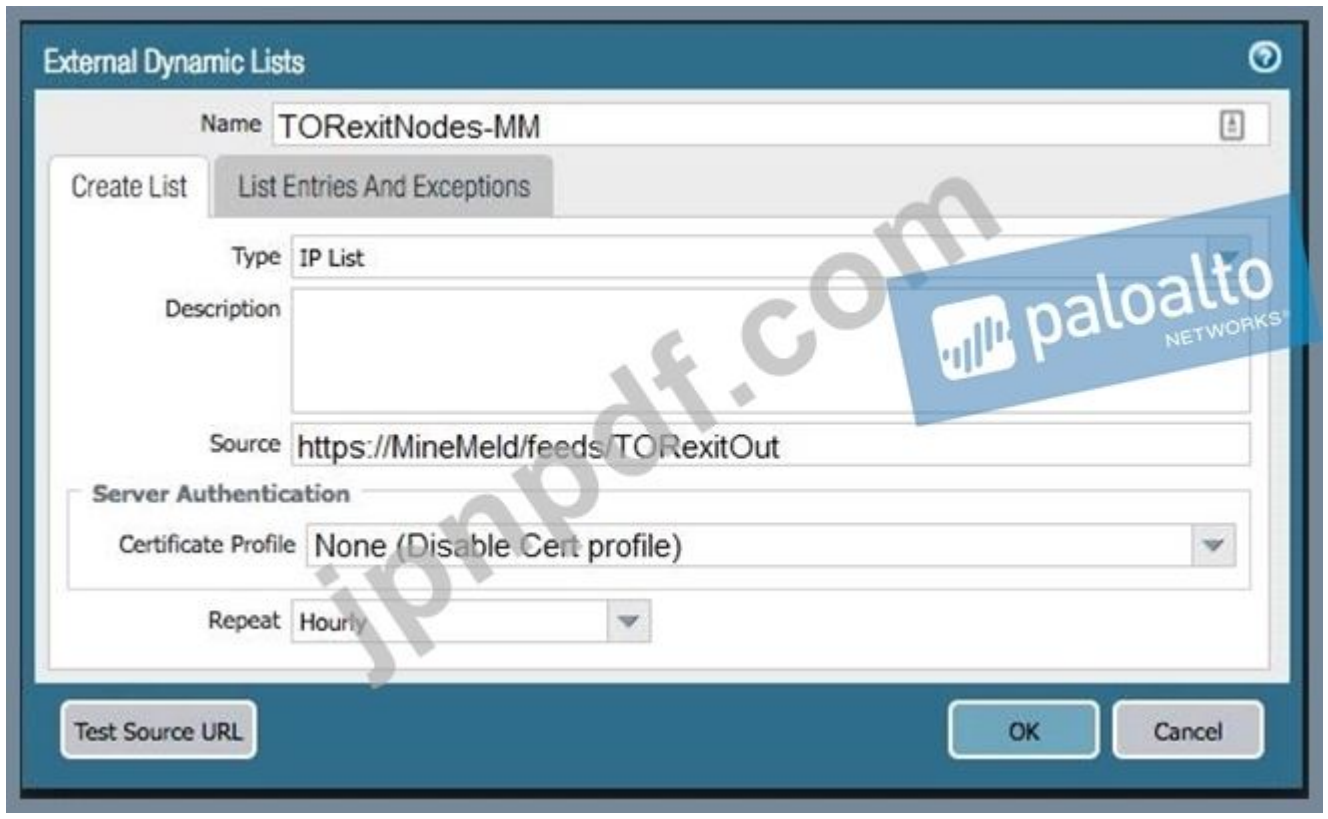
最新問題**: 131**
HAペアの構成をPanoramaにインポートする場合、インポートが進行中のトラフィックに影響を与えるのをどのように防止しますか？
A. HA2リンクを無効にする
B. パッシブリンク状態を'shutdownに設定します。-
C. HAを無効にする
D. 構成同期を無効にする
Answer: D (メーッセージを残す**)**

最新問題**: 132**
速度/デュプレックスネゴシエーションの不一致は、パロアルトネットワークスの管理ポートとそれが接続するスイッチポートの間にあります。
管理者はインターフェイスを1Gbpsにどのように構成しますか？
A. deviceconfig interfacespeed-duplex1Gbps-full-duplexを設定します

B. deviceconfigシステムの速度を設定デュプレックス1Gbps-デュプレックス
C. deviceconfig systemspeed-duplex1Gbps-full-duplexを設定します
D. setdeviceconfigインターフェイスの速度デュプレックス1Gbps-ハーフデュプレックス
Answer: (解答を表示する**)**
説明/参照 :https ://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex- of-the-Management-Port / ta-p / 59034

最新問題**: 133**
特定の宛先IPアドレスに到達できるかどうかを決定する仮想ルーター機能はどれですか？
A. 心拍数の監視
B. フェイルオーバー
C. パスモニタリング
D. Ping-Path
Answer: C (メーッセージを残す**)**
説明/参照：
参照 :https ://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based-forwarding/pbf/path-monitoring-for-pbf

最新問題**: 134**
ファイアウォールはMineMeldからIPアドレスをダウンロードしていません。画像に基づいて、最も可能性の高いものは何が間違っていますか？



A. クライアント証明書を含む証明書プロファイルを選択する必要があります。
B. 送信元アドレスは、ftp :// <address/file>でホストされているファイルのみをサポートします。
C. 外部動的リストはSSL接続をサポートしていません。
D. CA証明書を含む証明書プロファイルを選択する必要があります。

Answer: D (メーッセージを残す)
『リストソースがSSLで保護されている場合（つまり、HTTPS URLのリスト）、サーバー認証を有効にします。証明書プロファイルを選択するか、リストをホストするサーバーを認証するための新しい証明書プロファイルを作成します。選択する証明書プロファイルにはルート証明書が必要です。認証しているサーバーにインストールされている証明書と一致するURL（Authority）および中間CA証明書。」

最新問題: **135**
展示を参照してください。

DMZ内のWebサーバーは、DNATを介してパブリックアドレスにマップされています。
トラフィックがWebサーバーに流れることを許可するセキュリティポリシールールはどれですか？
A. Untrust（any）からUntrust（10. 1.1。100）、Webブラウジング許可
B. 信頼できない（任意から信頼できない（1. 1. 1. 100）、Webブラウジング許可
C. DMZ（1. 1. 1. 100）への信頼（任意）Webブラウジング許可
D. DMZ（10. 1. 1. 100）、Webブラウジングへの信頼（任意）許可
Answer: C (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

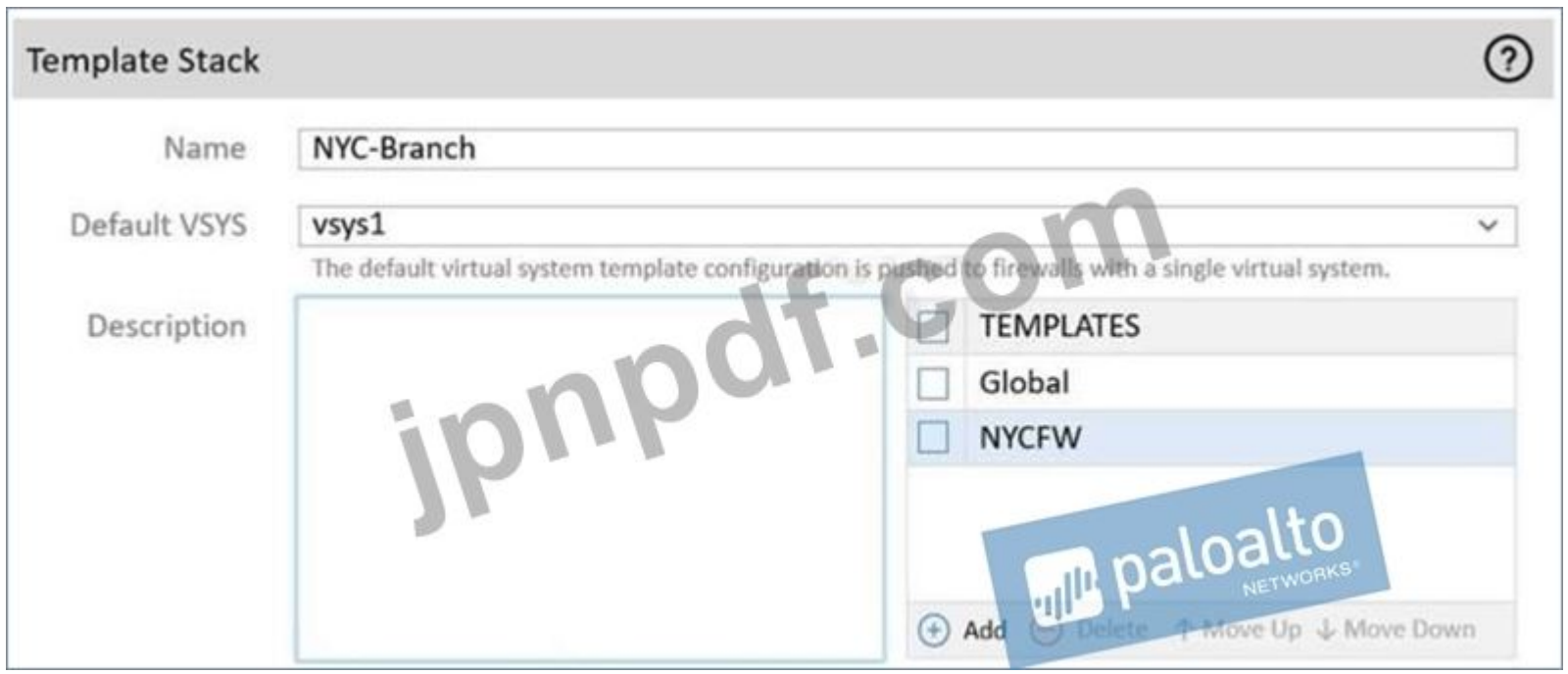
最新問題: **136**
管理者がゾーン保護を有効にしたい
その前に、管理者は何を考慮する必要がありますか？
A. ゾーン保護プロファイルは、そのゾーン内のすべてのインターフェースに適用されます
B. 帯域幅を増やすには、1つのゾーンに接続するファイアウォールインターフェースを1つだけにする必要があります
C. ゾーン保護サブスクリプションをアクティブ化します。
D. セキュリティポリシールールは、ゾーン間のトラフィックの横方向の移動を防止しません

Answer: (解答を表示する**)**

最新問題: **137**
インストールされたセッションがアプリケーションの不完全なタグで識別できる3つの理由は何ですか？
（3つ選択してください。）
A. アプリケーションデータを特定せずにTCP接続を終了しました
B. クライアントはPUSHフラグが設定されたTCPセグメントを送信しました
C. TCP接続が確立された後、十分なアプリケーションデータがありません
D. TCP接続が完全に確立されませんでした
E. TCP接続が確立された後、アプリケーションデータはありませんでした
Answer: A,D,E (メーッセージを残す**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

最新問題: **138**
グローバルな企業オフィスには、ユーザーIDエージェントが1つしかない大規模なネットワークがあり、ユーザーIDエージェントサーバーの近くにボトルネックが生じます。
この場合、PAN-OSソフトウェアのどのソリューションが役立ちますか？
A. アプリケーションのオーバーライド
B. 仮想ワイヤーモード
C. コンテンツ検査
D. ユーザーマッピングの再配布
Answer: D (メーッセージを残す**)**
参照 :https ://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy- user-id-in-a-large-scale-network

最新問題: **139**
画像を参照してください。



管理者は、グローバルテンプレートNTPサーバーを使用できないファイアウォールのNTPサービス構成を修正する必要があります。管理者は、IPアドレスをこのテンプレートスタックに適したサーバーに変更する必要がありますが、他のテンプレートスタックに影響を与えることはできません。

どうすれば問題を修正できますか？

A. NYCFWテンプレートの値を上書きします。

B. テンプレートスタック変数を使用してテンプレート値をオーバーライドします。

C. グローバルテンプレートの値を上書きします。

D. パノラマ設定で 粗先で定義されたオブジェクトが優先される」を有効にします。

Answer: B (メーッセージを残す)

説明

テンプレートとテンプレートスタックの両方が変数をサポートします。変数を使用すると、構成のニーズに基づいて、テンプレートまたはテンプレートスタックで指定された値を使用してプレースホルダーオブジェクトを作成できます。テンプレートまたはテンプレートスタック変数を作成して、構成内のIPアドレス、グループID、およびインターフェイスを置き換えます。

https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-tem

最新問題**: 140**

NGFWで、秘密鍵を生成してエクスポートをブロックし、セキュリティ体制を強化して、不正な管理者やその他の悪意のある人物が鍵を悪用するのを防ぐにはどうすればよいでしょうか。

A. 1.[デバイス]>[証明書の管理]>[証明書]>[デバイス]>[証明書]を選択します

2.証明書をインポートします

3.[秘密鍵のインポート]を選択します

4. [生成]をクリックして、新しい証明書を生成します

B. 1.[デバイス]>[証明書]を選択します

2.証明書プロファイルを選択します

3.証明書を生成します

4.[秘密鍵のエクスポートをブロックする]を選択します

C. 1.[デバイス]>[証明書の管理]>[証明書]>[デバイス]>[証明書]を選択します
2.証明書を生成します
3.[秘密鍵のエクスポートをブロックする]を選択します
4. [生成]をクリックして、新しい証明書を生成します
D. 1.[デバイス]>[証明書]を選択します
2.証明書プロファイルを選択します
3.証明書を生成します
4.[秘密鍵のエクスポートをブロックする]を選択します
Answer: C (メーッセージを残す**)**
説明/参照 :https ://docs.paloaltonetworks.com/pan-os/10-0/pan-os-new-features/decryption-features/block- export-of-private-keys.html

最新問題**: 141**
GlobalProtectのどのバージョンが、宛先ドメイン、クライアントプロセス、およびHTTP / HTTPSビデオストリーミングアプリケーションに基づくスプリットトンネリングをサポートしていますか？
A. PAN-OS8.0を搭載したGlobalProtectバージョン4.0
B. PAN-OS8.0を搭載したGlobalProtectバージョン4.1
C. PAN-OS8.1を搭載したGlobalProtectバージョン4.0
D. PAN-OS8.1を搭載したGlobalProtectバージョン4.1
Answer: (解答を表示する**)**

最新問題**: 142**
管理者は、任意のポートでSSLセッションを復号化するSSL復号化ポリシールールを作成しました。
管理者は、セッションが復号化されていることを確認するためにどのログエントリを使用できますか？
A. 脅威ログエントリの詳細
B. データフィルタリングログ
C. トラフィックログエントリの詳細
D. 復号化ログ
Answer: C (メーッセージを残す**)**

最新問題**: 143**
NGFWについて。秘密鍵を生成してエクスポートをブロックし、セキュリティ体制を強化して、不正な管理者やその他の悪意のある人物が鍵を悪用するのを防ぐにはどうすればよいでしょうか。
A. 1。[デバイス]>[証明書管理]>[証明書]>[デバイス]>[証明書]を選択します
2.証明書をインポートします。
3[秘密鍵のインポート]を選択します
4 [生成]をクリックして、新しい証明書を生成します
B. 1[デバイス]>[証明書]を選択します
2証明書プロファイルを選択します
3証明書を生成します
4[秘密鍵のエクスポートをブロックする]を選択します。

C. 1[デバイス]>[証明書の管理]>[証明書]>[デバイス]>[証明書]を選択します
2証明書を生成します
3[秘密鍵のエクスポートをブロックする]を選択します
4 Genet aleをクリックして、新しい証明書を生成します。
D. 1[デバイス]>[証明書]を選択します
2[証明書プロファイル]を選択します。
3証明書を生成します
4[秘密鍵のエクスポートをブロックする]を選択します
Answer: (解答を表示する**)**

最新問題**: 144**
company.comは、アプリケーションの上書きを有効にしたいと考えています。次のスクリーンショットを考えます。

ソーストラフィックと宛先トラフィックがアプリケーションオーバーライドポリシーに一致する場合、正しい2つのステートメントはどれですか。（2つ選択してください）
A. 「ftp-base」に一致するトラフィックは、App-IDおよびContent-IDエンジンをバイパスします。
B. UDPポート16384を利用するトラフィックは、「ftp-base」として識別されるようになります。
C. トラフィックはUDPポート16384を介して動作するように強制されます。
D. UDPポート16384を利用するトラフィックは、App-IDおよびContent-IDエンジンをバイパスします。
Answer: A,B (メーッセージを残す**)**

最新問題**: 145**
会社は、複数のWANリンクにまたがるActiveDirectoryドメインコントローラーを使用する必要があります。すべてのユーザーがActiveDirectoryに対して認証されます。各リンクには、すべてのミッションクリティカルなアプリケーションをサポートするための十分なネットワーク帯域幅があります。ファイアウォール管理プレーンは非常に利用されています。
このシナリオを考えると、どのタイプのユーザーIDエージェントがパロアルトネットワークスによってベストプラクティスと見なされますか？
A. キャプティブポータル
B. スタンドアロンサーバー上のWindowsベースのユーザーIDエージェント
C. 適切なデータプレーンリソースを備えたCitrixターミナルサーバーエージェント

D. PAN-OS統合エージェント
Answer: C (メーッセージを残す**)**

最新問題**: 146**
管理者は、トラストゾーンのユーザーが特定のWebサイトにアクセスできない理由を特定する必要があります。利用可能な唯一の情報は、次の画像に示されています。管理者はどの構成変更を行う必要がありますか？
A：

Detailed Log View

General

Session ID	567
Action	block-url
Application	web-browsing
Rule	AllowTrafficOut
Virtual System	
Device SN	
IP Protocol	tcp
Log Action	
Category	gambling
Generated Time	2017/05/23 21:22:27
Receive Time	2017/05/23 21:22:27
Tunnel Type	N/A

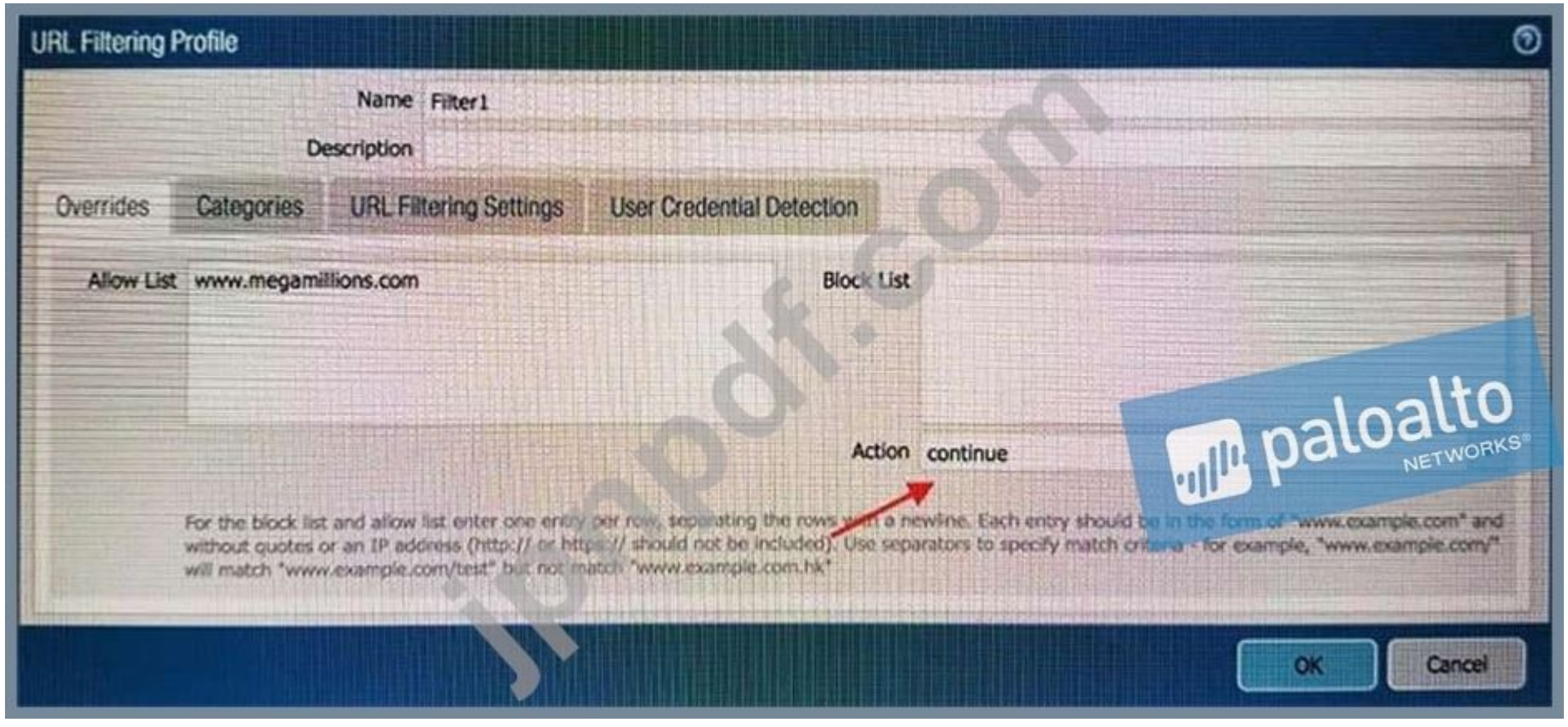
B :


URL Filtering Profile
Name Filter1
Description
Overrides
Categories
paloalto NETWORKS
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel

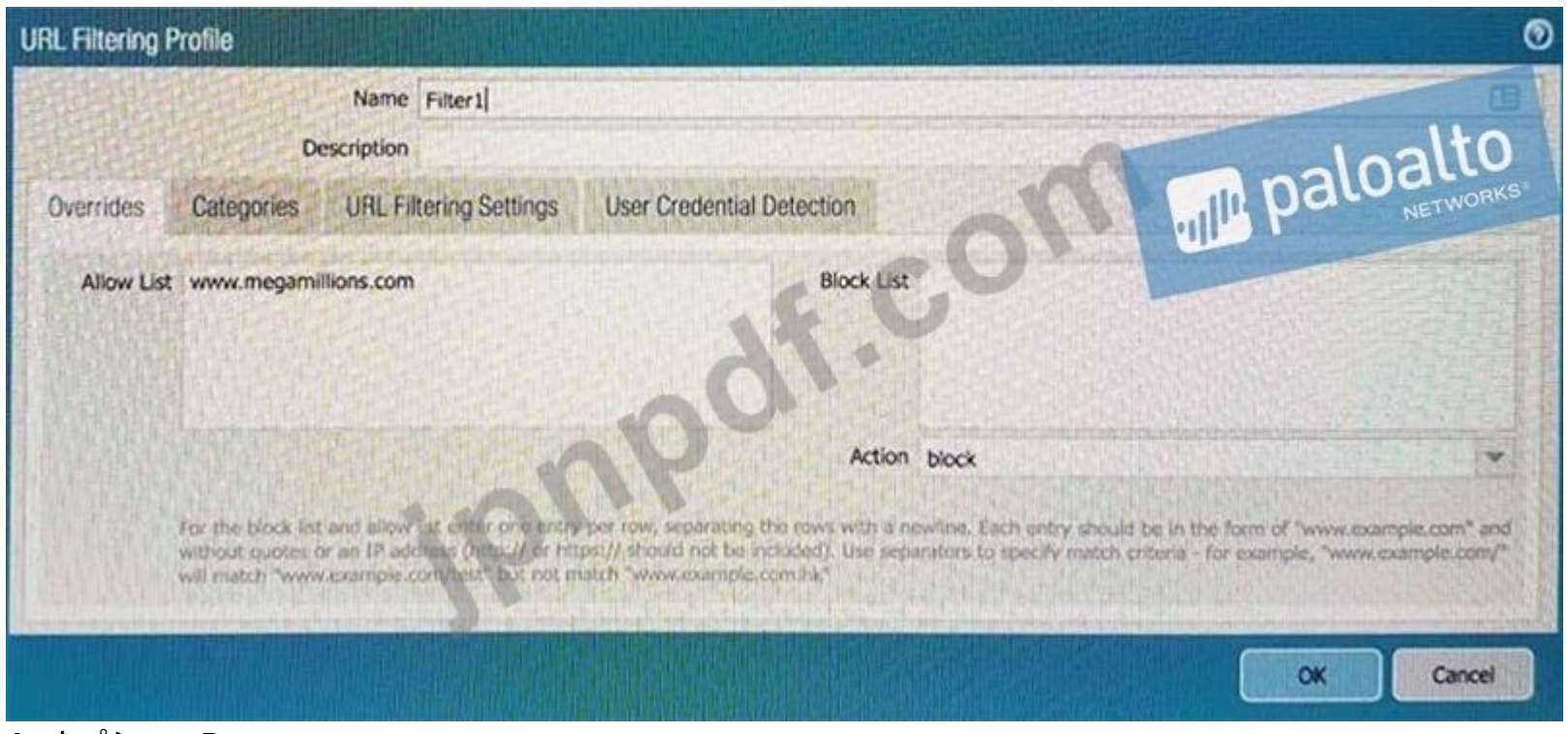
C :


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Name www.megamillions.com
Rule Type universal (default)
Description
Tags
paloalto NETWORKS
OK
Cancel

D :



と：



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

最新問題: **147**
管理者のPaloAltoNetworks NGFWを対象としたVPNトラフィックが悪意を持って傍受され、インターセプターによって再送信されています。VPNトンネルを作成する場合、この悪意のある動作を防ぐためにどの保護プロファイルを有効にできますか？
A. ゾーン保護
B. リプレイ
C. Webアプリケーション
D. DoS保護
Answer: A (メーッセージを残す**)**
説明/参照：

最新問題: **148**
HA2リンクを介して何が交換されますか？
A. こんにちはハートビート
B. ユーザーID情報
C. セッションの同期
D. HA状態情報
Answer: C (メーッセージを残す**)**
参照：https ://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

最新問題: **149**
基本的なWildFireサービスの一部として分析のためにWildFireに転送できる3つのファイルタイプはどれですか？
（3つ選択してください。）
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar
Answer: D,E,F (メーッセージを残す**)**
説明/参照：https ://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire- file-type-support

最新問題: **150**
ファイアウォールは、人気のあるアプリケーションをunknown-tcpとして識別します。
アプリケーションを識別するために使用できる2つのオプションはどれですか？（2つ選択してください。）
A. カスタムアプリケーションを作成します。
B. カスタムアプリケーションサーバーのカスタムオブジェクトを作成して、カスタムアプリケーションを識別します。
C. Apple-IDリクエストをパロアルトネットワークスに送信します。
D. カスタムアプリケーションを識別するためのセキュリティポリシーを作成します。
Answer: A,D (メーッセージを残す**)**

説明
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applica

最新問題: **151**
Company.comには、PaloAltoNetworksデバイスが正しく識別しない社内アプリケーションがあります。脅威管理チームのメンバーは、この社内アプリケーションは非常に機密性が高く、識別されるすべてのトラフィックをContent-IDエンジンで検査する必要があると述べています。
company.comは、パロアルトネットワークスデバイスでこのトラフィックにすぐに対処するためにどの方法を使用する必要がありますか？
A. 署名なしでカスタムアプリケーションを作成してから、トラフィックの送信元、宛先、宛先ポート/プロトコル、およびカスタムアプリケーションを含むアプリケーションオーバーライドポリシーを作成します。
B. 社内アプリケーションのニーズを満たすために、最も近い参照アプリケーションのセッションタイマー設定を変更します
C. 社内アプリケーショントラフィックの一意の識別子と一致する署名を使用してカスタムアプリケーションを作成します
D. パロアルトネットワークスから公式のアプリケーション署名が提供されるまで待ちます。
Answer: C (メーッセージを残す)

最新問題: **152**
PAN-OS 8.0で追加された認証方式のサポートは？
A. RADIUS
B. LDAP
C. 直径
D. TACACS +
Answer: D (メーッセージを残す)
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

最新問題: **153**
ユーザーマッピングの再配布を説明するデータフローはどれですか？
A. ファイアウォールへのユーザーIDエージェント
B. ファイアウォールからファイアウォールへ
C. ドメインコントローラーからユーザーIDエージェントへ
D. パノラマへのユーザーIDエージェント
Answer: B (メーッセージを残す)
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redistribute-user-mapping-information

最新問題: **154**
ネットワークセキュリティエンジニアが、ブロックのアクションを使用してファイルブロックプロファイルをルールに適用しました。LinuxCLIオペレーティングシステムのユーザーがチケットを開きました。チケットには、TARファイルをダウンロードしようとしたときに、ユーザーがファイアウォールによってブロックされていることが示されています。ユーザーはシステムでエラー応答を受け取りません。
ファイアウォールがユーザーのTARファイルをブロックしているかどうかを検証するのに最適な場所はどこですか？
A. データフィルタリングログ
B. URLフィルタリングログ
C. WildFire送信ログ
D. 脅威ログ
Answer: (解答を表示する**)**

最新問題: **155**
グローバルな企業オフィスには、ユーザーIDエージェントが1つしかない大規模なネットワークがあり、ユーザーIDエージェントサーバーの近くにボトルネックが生じます。
この場合、PAN-OS®ソフトウェアのどのソリューションが役立ちますか？
A. コンテンツ検査
B. ユーザーマッピングの再配布
C. 仮想ワイヤーモード
D. アプリケーションのオーバーライド
Answer: B (メーッセージを残す**)**

最新問題: **156**
GlobalProtectポータルを設定する場合、認証プロファイルを指定する目的は何ですか？
A. ポータルへのゲートウェイ認証を有効にするには
B. ゲートウェイへのポータル認証を有効にするには
C. ポータルへのユーザー認証を有効にする
D. ポータルへのクライアントマシン認証を有効にする
Answer: (解答を表示する**)**
説明
ブラウザとサテライトの追加オプションを使用すると、特定のシナリオで使用する認証プロファイルを指定できます。「ブラウザー」を選択して、GlobalProtectエージェント（WindowsおよびMac）をダウンロードする目的でWebブラウザーからポータルにアクセスするユーザーを認証するために使用する認証プロファイルを指定します。
[衛星]を選択して、衛星の認証に使用する認証プロファイルを指定します。
参照
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalpr

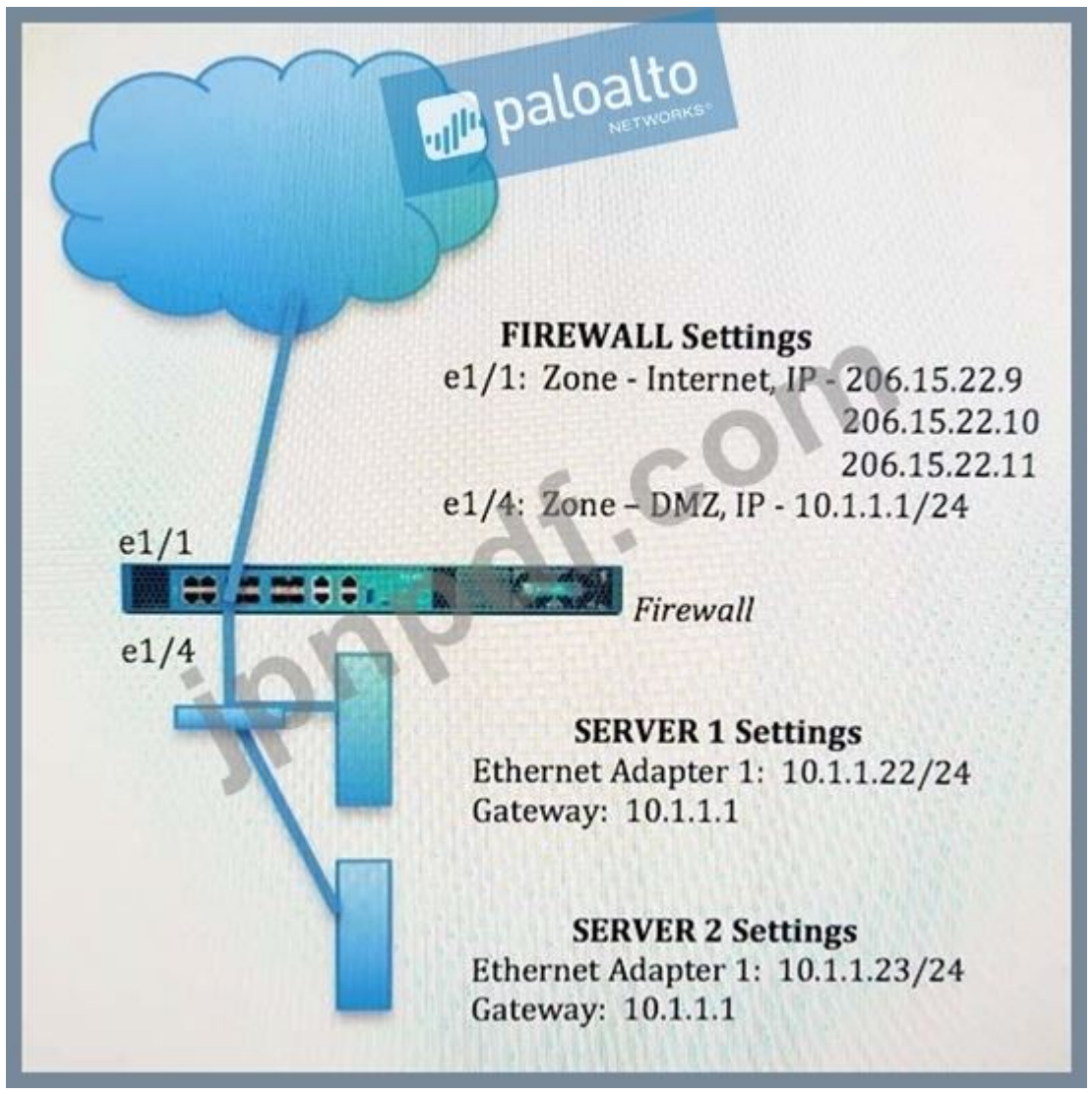
最新問題: **157**
管理者がインバウンド復号化で問題に遭遇しました。管理者はトリアージの一部としてどのオプションを調査する必要がありますか？

A. ターゲットサーバーへのSSLを許可するセキュリティポリシールール
B. CRLへのファイアウォール接続
C. 「信頼」が有効になっているファイアウォールにインポートされたルート証明書
D. HSMからの証明書のインポート
Answer: A (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

最新問題**: 158**
パノラマでポリシーを定義するときに使用できる3つのルールタイプはどれですか？ （3つ選択してください。）
A. クリーンアップルール
B. ステルスルール
C. 投稿ルール
D. 事前ルール
E. デフォルトのルール
Answer: C,D,E (メーッセージを残す)
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-firewalls/manage-the-rule-hierarchy

最新問題**: 159**
こぼれた脳のシナリオをアクティブ/パッシブ高可用性（HA）ペアで防ぐのに役立つ2つのメカニズムはどれですか？（2つ選択してください）
A. 管理インターフェースをHA3バックアップとして構成します
B. イーサネット1/1をHA2バックアップとして構成します
C. イーサネット1/1をHA1バックアップとして構成します
D. 管理インターフェースをHA2バックアップとして構成します
E. ethernet1 / 1をHA3バックアップとして構成します
F. 管理インターフェースをHA1バックアップとして構成します
Answer: C,F (メーッセージを残す)

最新問題**: 160**
管理者は、DMZ内の複数のWebサーバーがインターネットから開始された接続を受信することを望んでいます。
206.15.22.9ポート80/TCP宛てのトラフィックは、10.1.1.22のサーバーに転送する必要があります。画像に示されている情報に基づいて、どのNATルールがWebブラウジングトラフィックを正しく転送しますか？



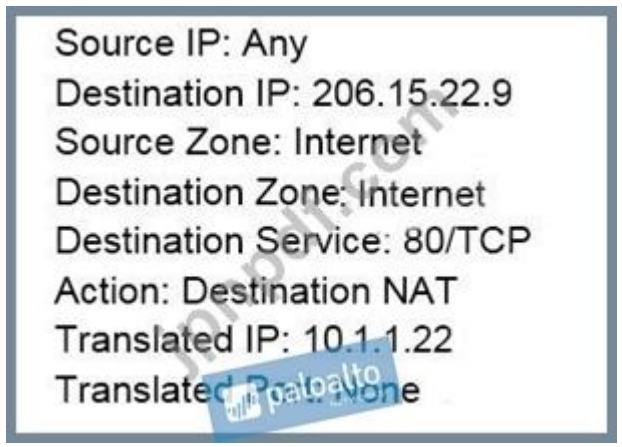
A :

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B :

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C：

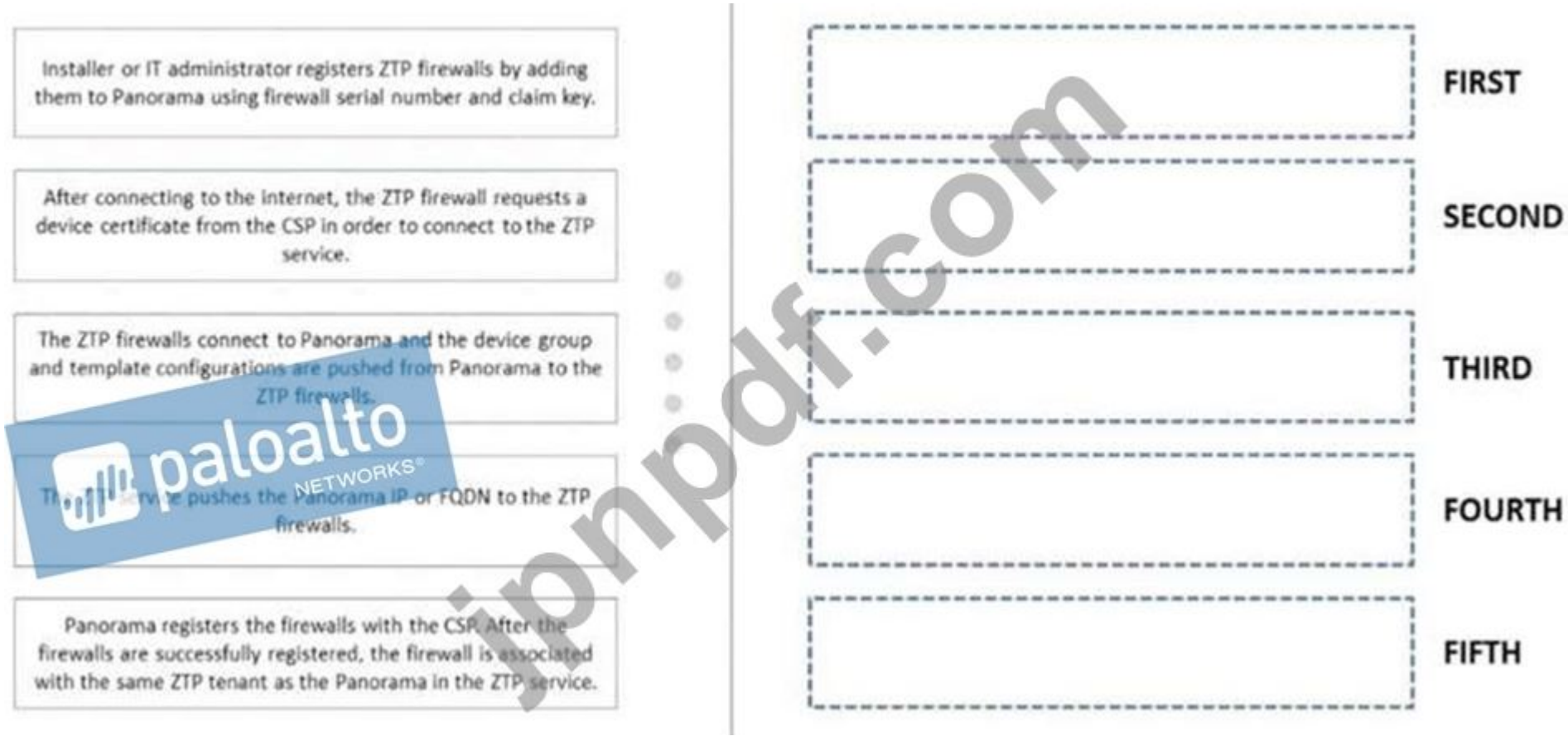


D：

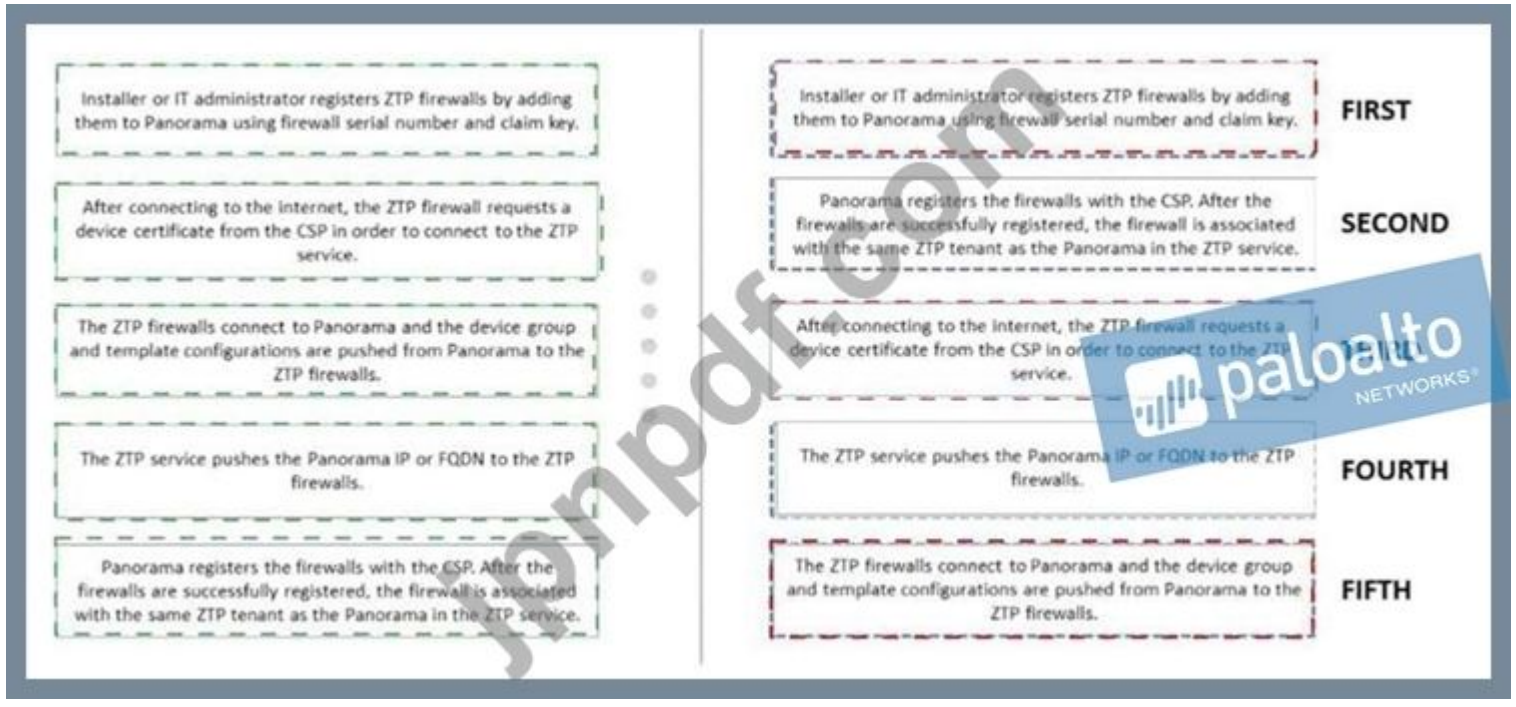
A. オプションD
B. オプションB
C. オプションC
D. オプションA
Answer: C (メーッセージを残す**)**

最新問題**: 161**
HA4 Keep-Alive Threshold（ms）の最も良い説明は何ですか？
A. 別のクラスターメンバーがクラスターの完全な同期を妨げている場合に、ローカルファイアウォールがアクティブ状態になるまで待機する時間枠。
B. 他のファイアウォールのHA機能が動作していることを確認するために送信されるhelloパケット間の最大間隔。
C. パッシブまたはアクティブ-セカンダリファイアウォールがアクティブまたはアクティブ-プライマリファイアウォールとして引き継ぐ前に待機する時間
D. ファイアウォールがクラスターメンバーからキープアライブを受信して、クラスターメンバーが機能していることを確認する必要がある時間枠。
Answer: D (メーッセージを残す**)**

最新問題**: 162**
ZTPファイアウォールをPanorama/CSP/ZTP-Serviceにオンボードする手順を正しい順序で配置します。

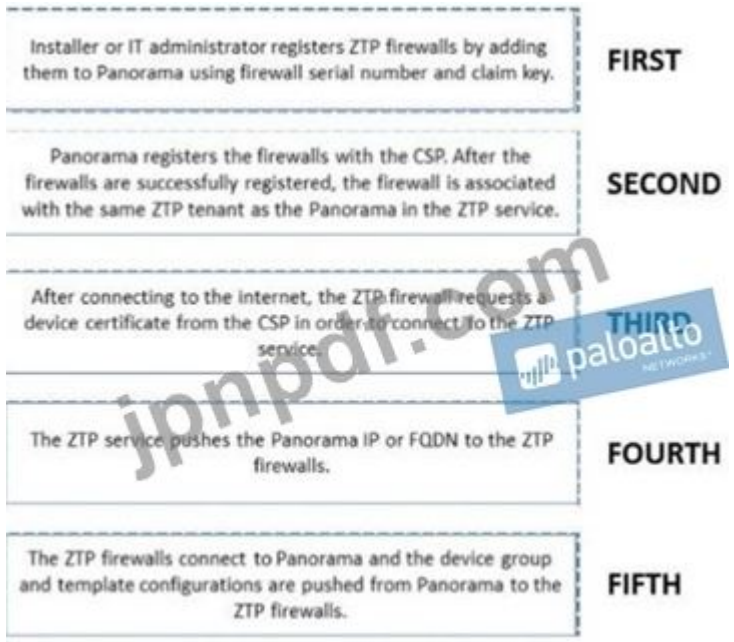


Answer:



説明

グラフィカルユーザーインターフェイス、テキスト、アプリケーション、電子メール説明が自動的に生成されます



https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/set-up-zero-touch-provisio

最新問題: **163**
管理者は、ローカルのオンプレミスラボ環境（「クラウド」ではない）に100個の仮想ファイアウォールを作成するように依頼されました。
ブートストラップは、このタスクを実行するための最も便利な方法です。
オンプレミス仮想環境でのブートストラップパッケージの展開を説明するオプションはどれですか？
A. USBスティックでconfig-driveを使用します。
B. ISOでS3バケットを使用します。
C. 仮想ハードディスク（VHD）を作成して接続します。
D. ISO付きの仮想CD-ROMを使用します。
Answer: D (メーッセージを残す**)**
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapping-firewalls-for-rapid-deployment.html

最新問題: **164**
次のパノラマの画像で、一部の値が赤で表示されているのはなぜですか？

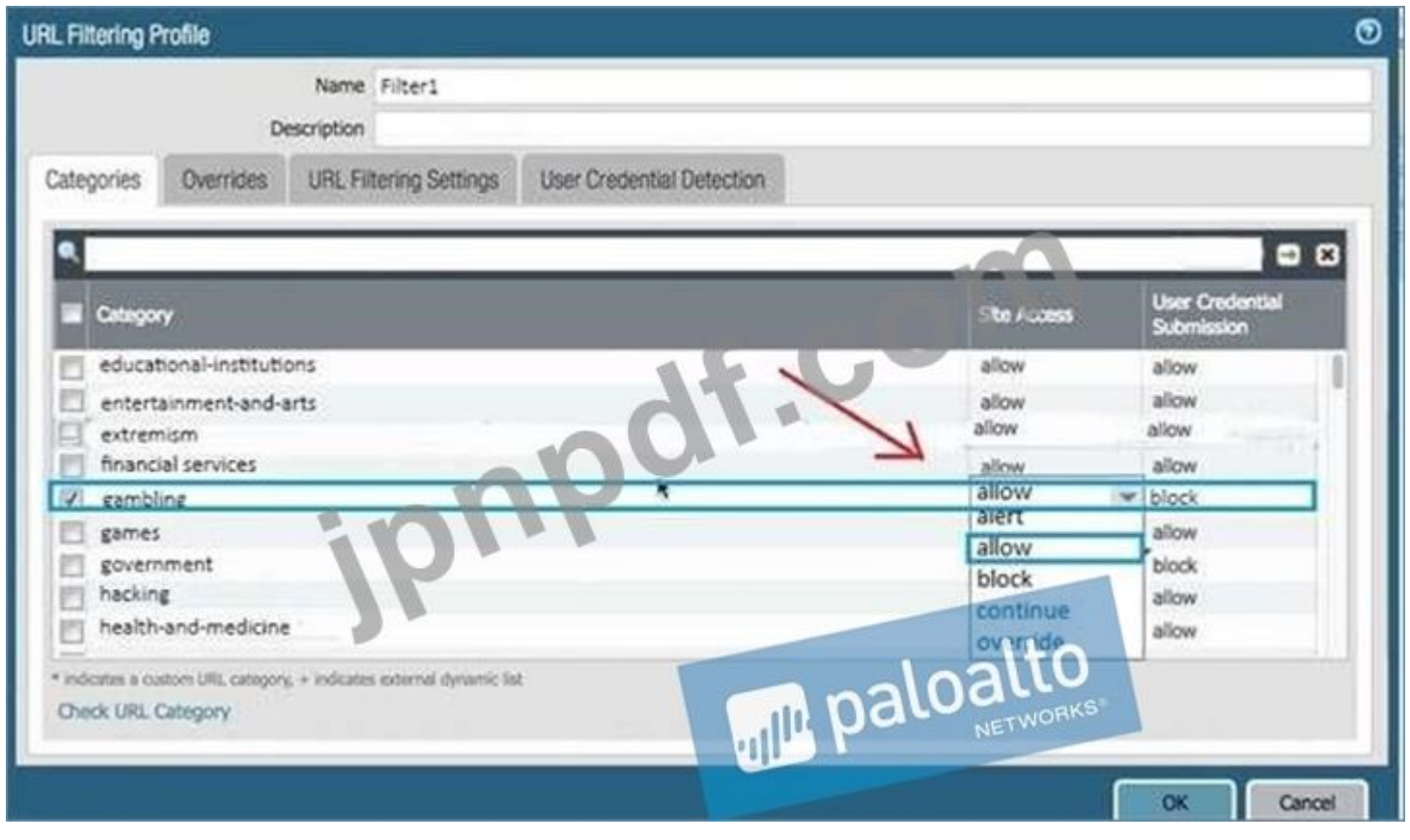
Device Name	Logging Rate (Log/sec)	Device Throughput (KB/sec)	Session Count (Sessions)
uk3	781	209	40221
sg2	0	953	170
us3	291	0	67455

A. us3のログレートは、管理者が設定したしきい値から外れています。
B. sg2セッション数は、他の管理対象デバイスと比較して最も少なくなっています。

C. sg2のセッションしきい値が正しく構成されていません。
D. uk3のログレートは、7日間の計算されたベースラインから外れています。
Answer: D (メーッセージを残す)

最新問題**: 165**
管理者がインバウンド復号化で問題に遭遇しました。管理者はトリアージの一部としてどのオプションを調査する必要がありますか？
A. ターゲットサーバーへのSSLを許可するセキュリティポリシールール
B. CRLへのファイアウォール接続
C. 「信頼」が有効になっているファイアウォールにインポートされたルート証明書
D. HSMからの証明書のインポート
Answer: A (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html

最新問題**: 166**
管理者は、トラストゾーンのユーザーが特定のWebサイトにアクセスできない理由を特定する必要があります。利用可能な唯一の情報は、次の画像に示されています。
管理者はどの構成変更を行う必要がありますか？
A.



B.


Security Policy Rule
General
Source
User
Destination
Application
Service/URL Category
Actions
Target
Name
www.megamillions.com
Rule Type
universal (default)
Description
Tags
OK
Cancel

C.


Detailed Log View
General
Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A

D. 

E. 

Answer: A (メーッセージを残す)

最新問題: **167**
PAN-OSバージョン9.1以降、アプリケーションの依存関係情報がどの新しい場所で報告されるようになりましたか？ 2つ選択してください。）

A. [コミットステータス]ウィンドウの[アプリの依存関係]タブ
B. セキュリティポリシールール作成ウィンドウの[アプリケーション]タブ
C. オブジェクト>アプリケーションブラウザページ
D. ポリシーオプティマイザの[ルールの使用法]ページ
Answer: A,B (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/resolve-application-dependencies.html

最新問題**: 168**
ファイアウォールにリンク監視構成がある場合、フェイルオーバーの原因は何ですか？

A. ethernet1/3とethernet1/6がダウン
B. ethernet1/3がダウン
C. ethernet1/3またはEthernet1/6がダウン
D. ethernet1/6がダウン
Answer: A (メーッセージを残す**)**

最新問題**: 169**
管理者は、Palo AltoNetworksNGFWを最新バージョンのPAN-OS®ソフトウェアにアップグレードする必要があります。ファイアウォールにはイーサネットインターフェイスを介したインターネット接続がありますが、管理インターフェイスからのインターネット接続はありません。セキュリティポリシーには、デフォルトのセキュリティルールと、任意のゾーンから任意のゾーンへのすべてのWebブラウジングトラフィックを許可するルールがあります。PAN-OS®ソフトウェアをアップグレードできるように、管理者は何を構成する必要がありますか？
A. CRL
B. スケジューラ
C. セキュリティポリシールール
D. サービスルート
Answer: D (メーッセージを残す**)**

最新問題: **170**
SD-WANは、どの2つのネットワークトポロジタイプをサポートするように設計されていますか？ 2つ選択してください。）
A. リング
B. ポイントツーポイント
C. ハブアンドスポーク
D. フルメッシュ
Answer: (解答を表示する**)**
説明
https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-s
https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/g

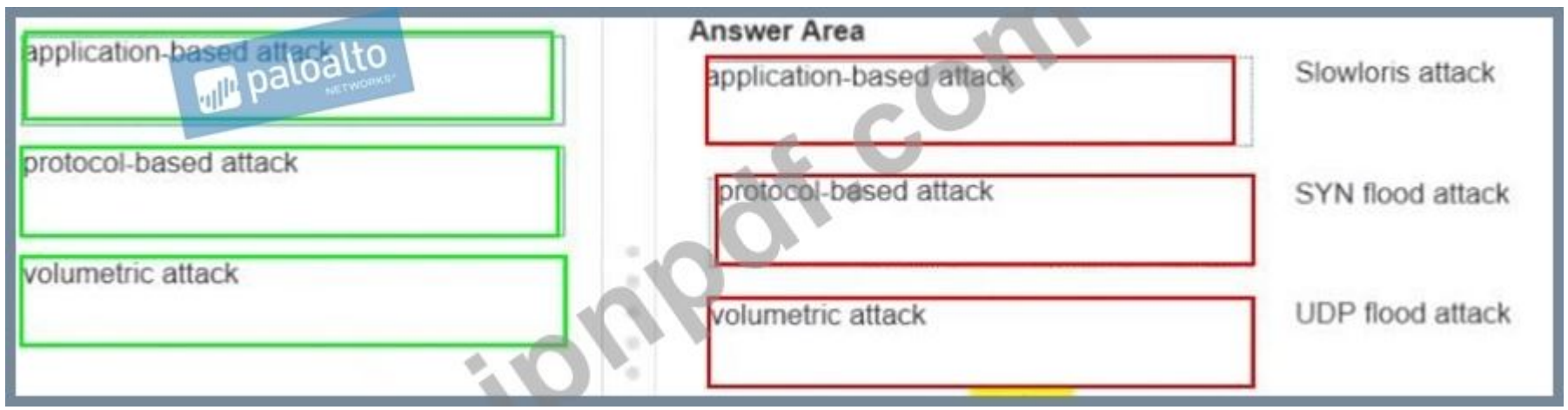
最新問題: **171**
ゾーン保護プロファイルでのみ使用できる保護機能はどれですか？
A. SYNフラッドCookieを使用したSYNフラッド保護
B. ICMPフラッドプロテクション
C. ポートスキャン保護
D. UDPフラッド保護
Answer: C (メーッセージを残す**)**
対応する偵察の試行に応答してファイアウォールが実行する次の偵察保護アクションのいずれかを構成します。許可-ファイアウォールは、ポートスキャンまたはホストスイープ偵察の続行を許可します。
SYNフラッドCookieはDoS保護プロファイルでも利用できます。答えは のみ」です。DoS保護プロファイルは、SYN、UDP、ICMP、ICMPv6、およびその他のIPフラッド攻撃から特定のデバイス（分類されたプロファイル）およびデバイスのグループ（集約プロファイル）を保護します。
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-zone-protection/reconnaissance-protection。html#ida0512c75-ed54-4b31-8d2c-9f459466d4d2
ポートスキャン保護=偵察保護
これは、ゾーン保護プロファイルでのみ実行できます。これは、攻撃対象領域全体を保護するために、外部に面したインターフェイスで構成することを目的としています。
DOS保護プロファイルは、SYNフラッドを含むフラッド攻撃から特定のサーバーまたはサーバーのグループを保護するために、内部に面したインターフェイスで構成することを目的としています。
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/zone-protection-and-dos-protection/configure-zone-protection-to-increase-network-security/configure-偵察保護

最新問題: **172**
PAN-OS 7.0で追加された認証方式のサポートは？
A. RADIUS
B. LDAP
C. 直径
D. TACACS +
Answer: D (メーッセージを残す**)**

デバイスは、管理ユーザーを認証するためのターミナルアクセスコントローラアクセス制御システムプラス（TACACS +）プロトコルをサポートするようになりました。TACACS +は、（パスワードだけでなく）ユーザー名とパスワードを暗号化するという点でRADIUSよりも優れたセキュリティを提供し、信頼性も高くなります（UDPの代わりにTCPを使用します）。
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os-release-notes/pan-os-7-0- release-information / authentication-features #91847

最新問題: 173
各タイプのDoS攻撃を、そのタイプの攻撃の例に一致させます

Answer:



最新問題: 174
各GlobalProtectコンポーネントをそのコンポーネントの目的に一致させます

Answer:

最新問題**: 175**

パノラマ管理者が ‟祖先で定義されたオブジェクトが優先されます」という設定を選択すると、どの処理順序が有効になりますか？

A. 子孫オブジェクトは他の子孫オブジェクトよりも優先されます。

B. 子孫オブジェクトは、祖先オブジェクトよりも優先されます。

C. 祖先オブジェクトは子孫オブジェクトよりも優先されます。

D. 祖先オブジェクトは他の祖先オブジェクトよりも優先されます。

Answer: (解答を表示する)

説明/参照：

参照：https ://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-setup-management

最新問題**: 176**

展示を参照してください。

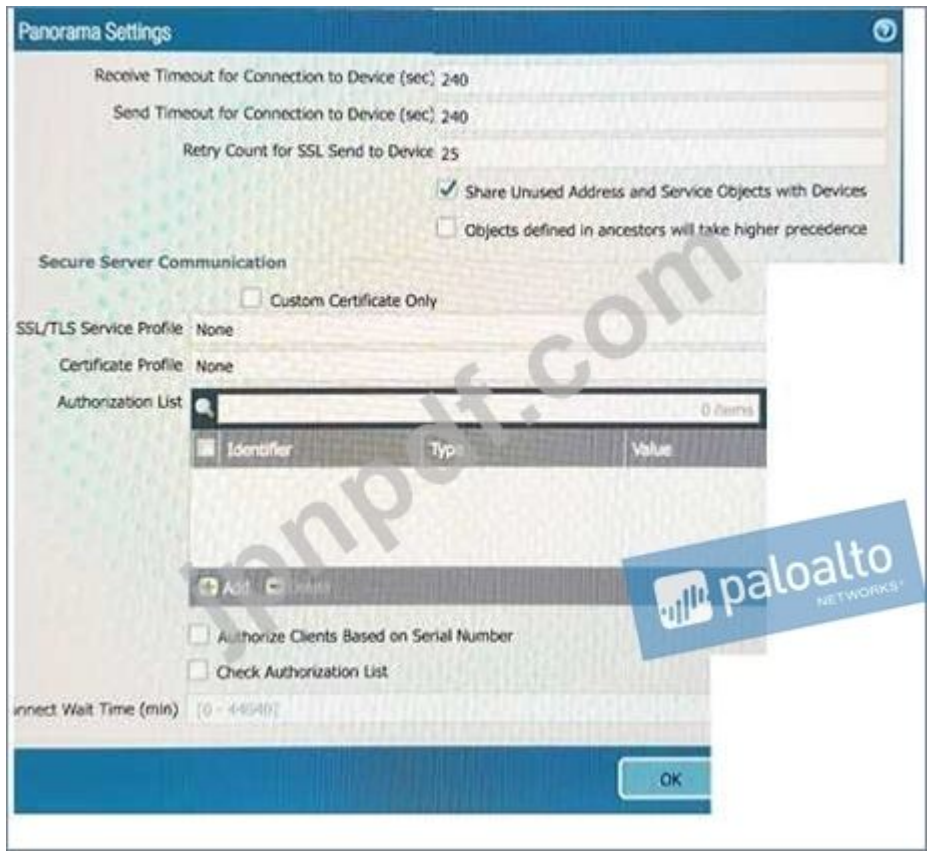
管理者は、PanoramaのPalo AltoNetworksNGFWからのトラフィックログを確認できません。
構成の問題はファイアウォール側にあるようです。構成が正しいかどうかを確認するために、パロアルトネットワークスNGFWのどこが最適ですか？

A :オプション

B :オプション

C :オプション

D :オプション



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

最新問題**: 177**
自動コミット回復機能の動作を説明するオプションはどれですか？
A. アプリケーションの依存関係エラーが見つかった場合、ファイアウォールが以前の構成に戻ることができます。
B. ルールのシャドウイングが検出された場合、ファイアウォールが以前の構成に戻ることができます。
C. コミットによってPanorama接続障害が発生した場合、ファイアウォールが以前の構成に戻ることができます。
D. コミットによってHAパートナーの接続障害が発生した場合に、ファイアウォールを以前の構成に戻すことができます。
Answer: C (メーッセージを残す**)**

最新問題**: 178**
画像に示されている時間内に、トラフィックの入力インターフェイスが192.168.111.3から宛先10.46.41.113へのethernet1 / 6ソーシングである場合、出力インターフェイスはどうなりますか？

```
admin@Lab33-111-PA-3060(active)> show clock

Thu Jun  8 12:49:55 PDT 2017
######################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
test-pbf {
  action {
    forward {
      egress-interface ethernet1/5;
    }
  }
  from {
    zone L3-Trust;
  }
  enforce-symmetric-return {
    enabled no;
  }
  source 192.168.111.3;
  destination 10.46.41.113;
  source-user any;
  application any;
  service any;
  schedule schedule-pbf;
}
######################
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
schedule-pbf {
  schedule-type {
    recurring {
      daily 16:00-21:00;
    }
  }
}
######################
admin@Lab33-111-PA-3060(active)> show routing fib
id      destination           nexthop            flags  interface          mtu
--------------------------------------------------------------------------------
47      0.0.0.0/0             10.46.40.1         ug     ethernet1/3        1500
67      10.10.20.0/24         0.0.0.0            u      ethernet1/7        1500
66      10.10.20.111/32       0.0.0.0            uh     ethernet1/7        1500
46      10.46.40.0/23         0.0.0.0            u      ethernet1/3        1500
49      10.46.44.0/23         0.0.0.0            u      ethernet1/5        1500
45      10.46.41.111/32       0.0.0.0            uh     ethernet1/3        1500
70      10.46.41.113/32       10.46.40.1         ug     ethernet1/3        1500
48      10.46.45.1/32         0.0.0.0            uh     ethernet1/5        1500
51      192.168.111.0/24      0.0.0.0            u      ethernet1/6        1500
50      192.168.111.2/32      0.0.0.0            uh     ethernet1/6        1500
--------------------------------------------------------------------------------
```


A. ethernet1 / 6
B. ethernet1 / 3
C. ethernet1 / 5
D. ethernet1 / 7
Answer: (解答を表示する**)**

最新問題**: 179**
お客様は、リンクアグリゲーションを使用して、複数のイーサネットインターフェイスを単一の仮想インターフェイスに結合したいと考えています。集約インターフェースの命名に適した2つの形式はどれですか？ 2つ選択してください。）
A. ae.8
B. aggregate.1
C. ae.1
D. aggregate.8

Answer: A,C (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html

最新問題: **180**
HA4 Keep-Alive Threshold（ms）の最も良い説明は何ですか？
A. 他のファイアウォールのHA機能が動作していることを確認するために送信されるhelloパケット間の最大間隔。
B. パッシブまたはアクティブ-セカンダリファイアウォールがアクティブまたはアクティブ-プライマリファイアウォールとして引き継ぐ前に待機する時間
C. 別のクラスターメンバーがクラスターの完全な同期を妨げているときに、ローカルファイアウォールがアクティブ状態になるまで待機する時間枠。
D. ファイアウォールがクラスターメンバーからキープアライブを受信して、クラスターメンバーが機能していることを確認する必要がある時間枠。
Answer: A (メーッセージを残す)

最新問題: **181**
セキュリティポリシールールは、脆弱性保護プロファイルと「拒否」アクションで構成されます。
これにより、一致したトラフィックの構成が発生するアクションはどれですか。
A. 設定が無効です。アクションが「拒否」に設定されている場合、「プロファイル設定」セクションはグレー表示されます。
B. 脆弱性が検出されない限り、構成は一致したセッションを許可します。「拒否」アクションは、関連する脆弱性保護プロファイルで定義された重大度ごとに定義されたアクションに優先します。
C. 構成が無効です。これにより、ファイアウォールはこのセキュリティポリシールールをスキップします。コミット中に警告が表示されます。
D. 構成は有効です。これにより、ファイアウォールは一致したセッションを拒否します。セキュリティポリシールールのアクションが「拒否」に設定されている場合、構成されたセキュリティプロファイルは効果がありません。
Answer: D (メーッセージを残す)
「セキュリティプロファイルは、トラフィックフローの一致基準では使用されません。セキュリティプロファイルは、アプリケーションまたはカテゴリがセキュリティポリシーで許可された後、トラフィックをスキャンするために適用されます。」
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#

最新問題: **182**

パロアルトネットワークNGFWを通過するユーザートラフィックは、http // wwwcompanycomに到達する場合があります。それ以外の場合はセッションがタイムアウトします。それ以外の場合、セッションがタイムアウトします。NGFWは、http ://www.company.comにアクセスするとユーザートラフィックが一致するPBFルールで構成されています。http :// wwwcompanycomにアクセスします。ファイアウォールを構成するにはどうすればよいですか。ネクストホップがダウンした場合、PBFルールを自動的に無効にしますか？
A. 仮想ルーターのデフォルトルートでネクストホップゲートウェイのパス監視を構成します
B. ファイアウォールの外部インターフェイスのリンク監視プロファイルを有効にして構成します
C. 問題のPBFルールで待機回復アクションを使用してモニタープロファイルを作成および追加します
D. 問題のPBFルールでフェイルオーバーのアクションを持つモニタープロファイルを作成して追加します
Answer: D (メーッセージを残す**)**

最新問題**: 183**
次の表を考えます。

ファイアウォールのどの構成変更により、192.168.93.0 / 30ネットワークのネクストホップとして10.66.24.88が使用されますか？
A. RIPの管理距離をOSPFExtの管理距離よりも大きくなるように構成します。
B. RIPのメトリックをOSPFIntのメトリックよりも高くなるように構成します。
C. RIPのメトリックをそのOSPFExtより低くなるように構成します。
D. RIPの管理距離をOSPFIntの管理距離よりも短くなるように構成します。
Answer: D (メーッセージを残す**)**

最新問題**: 184**
ファイアウォール復号化ブローカーの目的は何ですか？
A. SSLトラフィックを復号化し、クリアテキストとして検査ツールのセキュリティチェーンに送信します
B. これまで知られていなかった暗号スイートの強制復号化
C. SSLトラフィックをより弱い暗号に減らしてから、検査ツールのセキュリティチェーンに送信します
D. IPsecトンネル内の検査トラフィック
Answer: B (メーッセージを残す**)**

最新問題: **185**
クライアントは、DNSサーバーに対するサービス拒否攻撃によるリソースの枯渇を懸念しています。
個々のサーバーを保護するオプションはどれですか？
A. ゾーン保護プロファイルでパケットバッファ保護を有効にします。
B. DNSシンクホールを使用してスパイウェア対策プロファイルを適用します。
C. DNSApp-IDをapplication-defaultとともに使用します。
D. 分類されたDoS保護プロファイルを適用します。
Answer: D (メーッセージを残す**)**
「パケットバッファ保護」は確かにリソースの枯渇から保護する方法ですが、DOS保護プロファイル」では構成されていません。ZONESで直接有効になります。

最新問題: **186**
どのURLフィルタリングセキュリティプロファイルアクションがURLフィルタリングカテゴリをURLフィルタリングログに切り替えますか？
A. アラート
B. デフォルト
C. ログ
D. 許可する
Answer: A (メーッセージを残す**)**

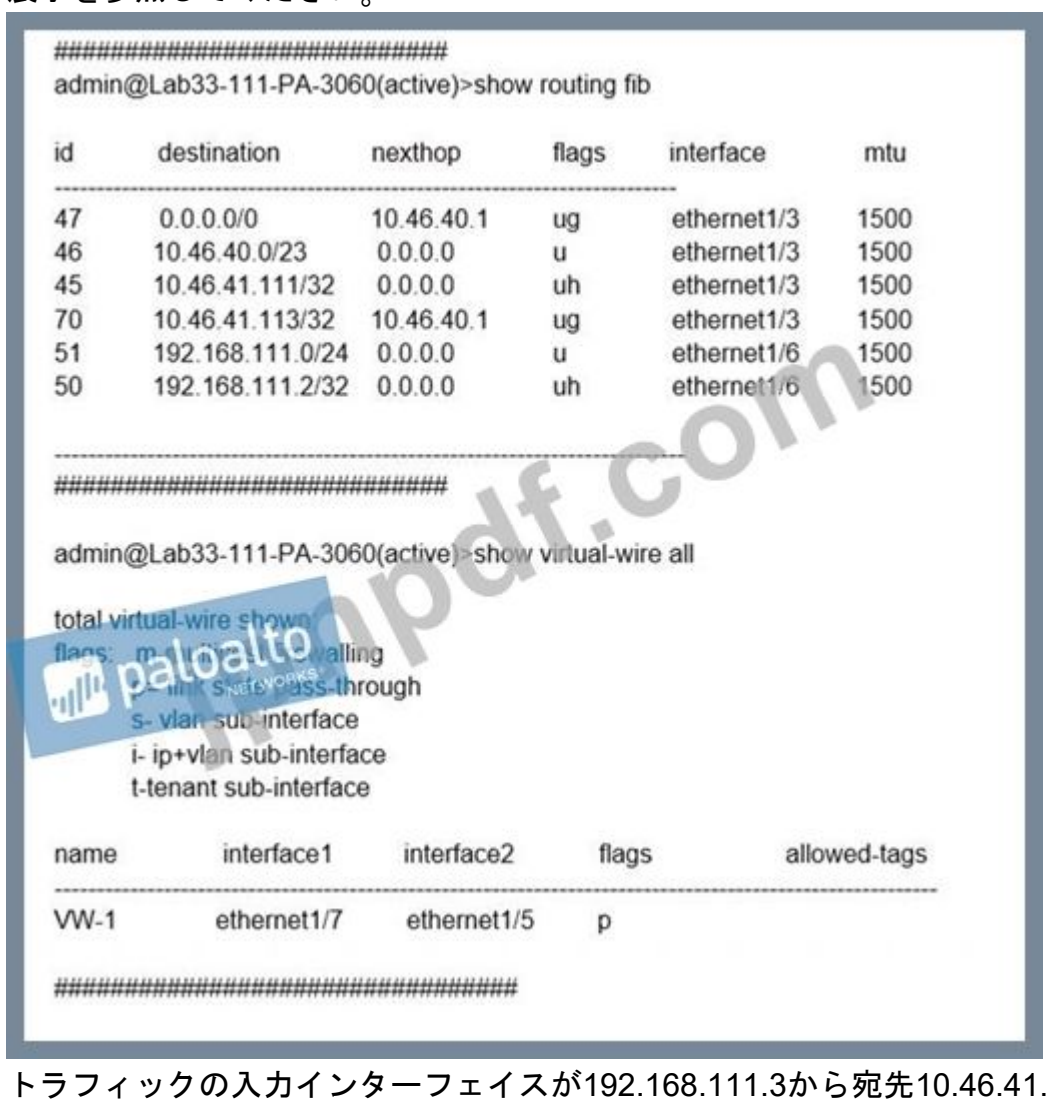
最新問題: **187**
Webサイトフォームへの企業ログイン情報の送信を妨げる機能はどれですか？
A. データフィルタリング
B. ユーザーID
C. ファイルのブロック
D. クレデンシャルフィッシングの防止
Answer: D (メーッセージを残す**)**
参照：
https://www.paloaltonetworks.com/cyberpedia/how-the-next-generation-security-platform-contributes-to-gdpr-co
「クレデンシャルフィッシング防止は、Webサイトへのユーザー名とパスワードの送信をスキャンし、それらの送信を有効な企業のクレデンシャルと比較することで機能します。WebサイトのURLカテゴリに基づいて、企業のクレデンシャルの送信を許可、アラート、またはブロックするWebサイトを選択できます。または、特定のURLカテゴリに分類されたサイトに資格情報を送信しないようにユーザーに警告するページを表示することもできます。これにより、正当なフィッシング以外のサイトであっても、企業の資格情報を再利用しないようにユーザーを教育する機会が得られます。が侵害された場合、この機能を使用すると、クレデンシャルを送信したユーザーを識別して、修正することができます。」

最新問題: **188**
管理者がデータプレーンのCPU使用率を確認できるCLIコマンドはどれですか。
A. デバッグデータプレーンdp-cpu
B. 実行中のリソースモニターを表示します

C. 実行中のリソースをデバッグします
D. システムリソースを表示する
Answer: (解答を表示する**)**

最新問題**: 189**
ファイアウォールを通過するトラフィックをシミュレートし、トラフィックによってトリガーされるセキュリティポリシールール、NAT変換、静的ルート、またはPBFルールを決定するために使用されるCLIコマンドはどれですか。
A. チェック
B. 検索
C. テスト
D. シム
Answer: (解答を表示する**)**
説明/参照：
参照：http ://www.shanekillen.com/2014/02/palo-alto-useful-cli-commands.html

最新問題**: 190**
展示を参照してください。

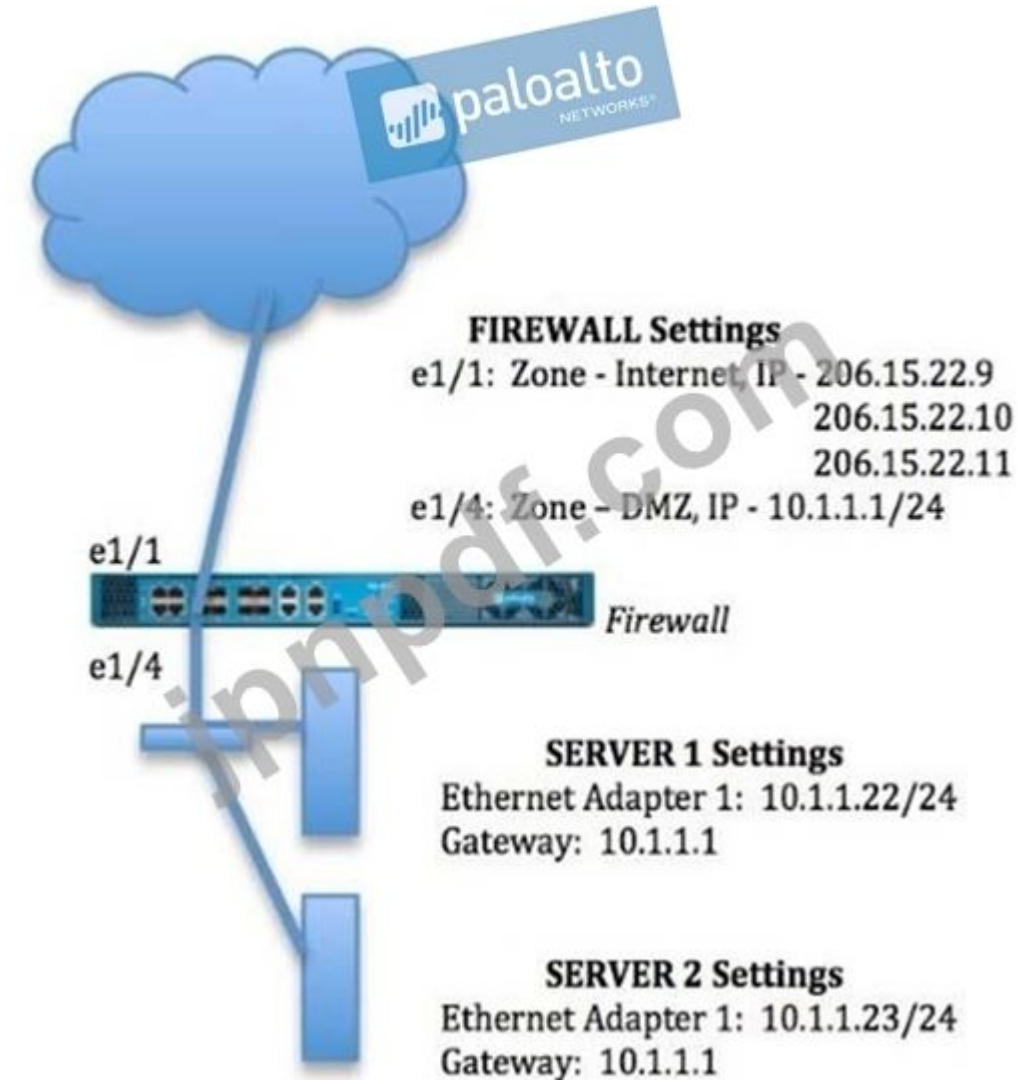


トラフィックの入力インターフェイスが192.168.111.3から宛先10.46.41.113へのイーサネット1/7ソーシングである場合、どちらが出力インターフェイスになりますか？

A. ethernet1 / 6
B. ethernet1 / 3
C. ethernet1 / 7
D. ethernet1 / 5
Answer: (解答を表示する**)**
説明
PBFはe1/5ですが、現在の時刻はタイムスケジュールに含まれていません。通常のルーティングはe1/3になります

最新問題**: 191**
顧客は、トンネルインターフェイスを使用してサイト間VPNを設定したいと考えています。
トンネルインターフェースの命名に適した2つの形式はどれですか？ 2つ選択してください。）
A. tunnel.1
B. vpn-tunnel.1
C. tunnel.1025
D. vpn-tunnel.1024
Answer: (解答を表示する**)**
説明/参照：

最新問題**: 192**
管理者は、DMZ内の複数のWebサーバーがインターネットから開始された接続を受信することを望んでいます。
206.15.22.9ポート80/TCP宛てのトラフィックは、10.1.1.22のサーバーに転送する必要があります。
画像に示されている情報に基づいて、どのNATルールがWebブラウジングトラフィックを正しく転送しますか？



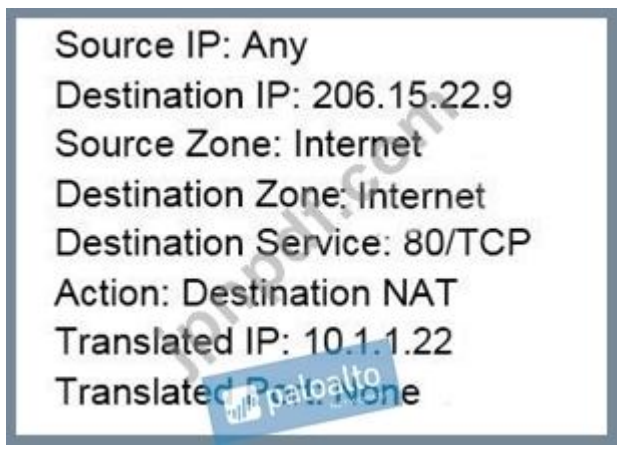
A :

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B :

Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: Internet
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.1.1.22
Translated Port: 53/UDP

C :



D :

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

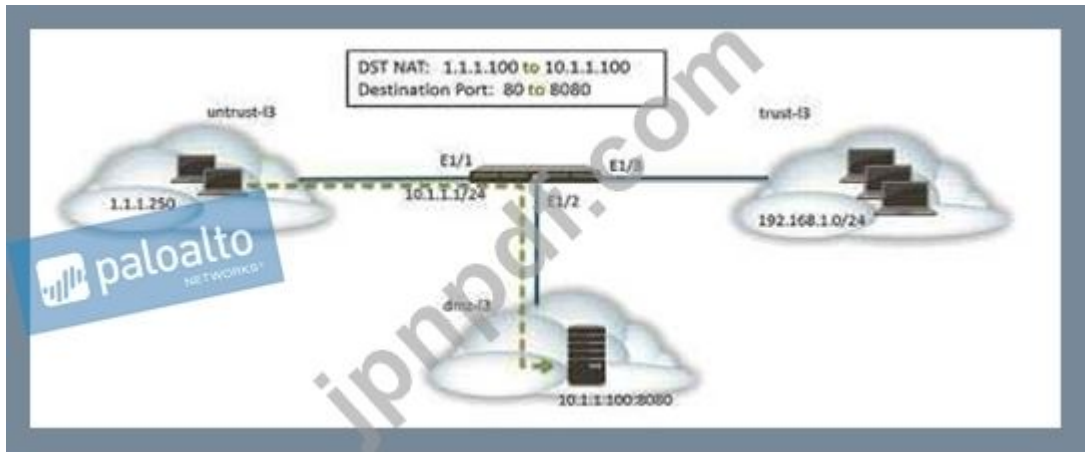
最新問題**: 193**
どのパロアルトネットワークスVMシリーズファイアウォールが有効ですか？
A. VM-25
B. VM-800
C. VM-50
D. VM-400
Answer: C (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

最新問題**: 194**
サイトAとサイトBは、VPN接続を確立するためにIKEv2を使用する必要があります。サイトAは、パブリックIPアドレスを使用してインターネットに直接接続します。サイトBは、ISPルーターの背後にあるプライベートIPアドレスを使用してインターネットに接続します。
サイトAとサイトBの間でVPN接続を確立するには、NATトラバーサルをどのように実装する必要がありますか？

A. サイトBでのみ有効にする
B. パッシブモードでのみサイトBで有効にする
C. サイトAでのみ有効
D. サイトAとサイトBで有効にする
Answer: (解答を表示する**)**

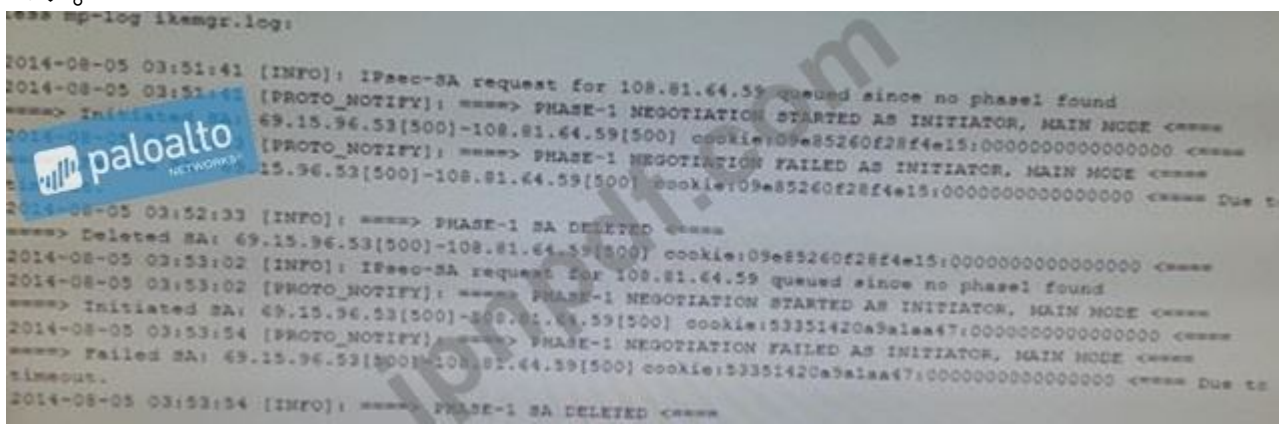
最新問題**: 195**
組織は、Palo Alto Networks VM-SeriesファイアウォールをAWSテナントにデプロイするためのブートストラップパッケージを構築しています。ブートストラップパッケージの内容に関して正しい2つのステートメントはどれですか？ 2つ選択してください）
A. init-cfg txtファイルとbootstrap.xmlファイルは、どちらも/configフォルダーのオプションの構成アイテムです。
B. ディレクトリ構造には、/ config / content、/ software、および/licenseフォルダが含まれている必要があります
C. ブートストラップxmlファイルを使用すると、完全なネットワークおよびポリシー構成でVM-Senesファイアウォールを自動展開できます。
D. ブートストラップパッケージは、AFS共有または個別のコンテナファイルバケットに保存されます
E. / config /contentフォルダーと/softwareフォルダーは必須ですが、/licenseフォルダーと/pluginフォルダーはオプションです。
Answer: A,C (メーッセージを残す**)**

最新問題**: 196**
Webサーバーは、ポート8080でHTTPトラフィックをリッスンするように構成されています。クライアントは、TCPポート80でIPアドレス1.1.1.100を使用してWebサーバーにアクセスします。宛先NATルールは、IPアドレスとレポートの両方を10.1.1.100に変換するように構成されています。TCPポート8080。



ファイアウォールで構成する必要があるNATおよびセキュリティルールはどれですか？ 2つ選択してください）
A. service-httpサービスを使用して、送信元がuntrust-l3ゾーンから宛先がuntrust-l3ゾーンの1.1.1.100までのNATルール。
B. Webブラウジングアプリケーションを使用して、untrust-l3ゾーンからdmz-l3ゾーンの宛先1.1.100までのいずれかのソースを持つセキュリティポリシー。
C. untrust-l3ゾーンから、service-httpサービスを使用したdmz-zoneの宛先10.1.1.100までのいずれかの送信元を持つNATルール。
D. Webブラウジングアプリケーションを使用して、untrust-l3ゾーンからdmz-l3ゾーンの宛先10.1.1.100までのいずれかのソースを持つセキュリティポリシー
Answer: (解答を表示する**)**

最新問題: **197**
管理者が管理者の自宅でCiscoASAへのIPSecVPNを設定していて、接続の完了で問題が発生しています。コマンドからの出力は次のとおりです。



この問題の原因は何でしょうか？
A. Palo AltoNetworksFirewallのプロキシIDがASAの設定と一致しません。
B. 共有シークレットがPalo AltoNetworksFirewallとASAの間で一致しません。
C. デッドピア検出設定がPalo AltoNetworksFirewallとASAの間で一致していません。
D. パブリックIPアドレスは、パロアルトネットワークファイアウォールとASAの両方で一致しません。
Answer: D (メーッセージを残す**)**

最新問題: **198**
ファイアウォールにリンク監視構成がある場合、フェイルオーバーの原因は何ですか？

A. ethernet1/3またはEthernet1/6がダウン
B. ethernet1/6がダウン
C. ethernet1/3がダウン
D. ethernet1/3とethernet1/6がダウン
Answer: D (メーッセージを残す)

最新問題**: 199**
管理者がPaloAltoNetworks NGFWにログインし、WebUIに[ポリシー]タブがないことを報告します。
[ポリシー]タブが表示されない原因はどのプロファイルですか？
A. 管理者の役割
B. WebUI
C. 承認
D. 認証
Answer: A (メーッセージを残す)

最新問題**: 200**
すでにユーザーを認証しているWebプロキシを介して接続しているユーザーのユーザー名にIPアドレスをマップするユーザーIDの方法はどれですか？
A. クライアントプロービング
B. ポートマッピング
C. サーバーの監視
D. Syslogリスニング
Answer: D (メーッセージを残す)
説明
ユーザーを認証する既存のネットワークサービス（ワイヤレスコントローラーなど）からユーザーマッピングを取得するには、802.1xデバイス、Apple Open Directoryサーバー、プロキシサーバー、またはその他のネットワークアクセス制御（NAC）メカニズムユーザーマッピング用にSyslog送信者を監視するようにユーザーIDを構成します。WindowsエージェントまたはPAN-OS統合ユーザーのいずれかを構成できます。ネットワークサービスからの認証syslogメッセージをリッスンするファイアウォール上のIDエージェント。PAN-OS統合エージェントのみがTLSを介したsyslogリスニングをサポートしているため、これが推奨される構成です。

最新問題**: 201**
Palo Alto Networks NGFWにユーザー名とロール名の両方を提供するために変更できる3つのユーザー認証サービスはどれですか？（3つ選択してください。）
A. TACACS +
B. Kerberos
C. PAP
D. LDAP
E. SAML
F. RADIUS
Answer: A,E,F (メーッセージを残す)

説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat

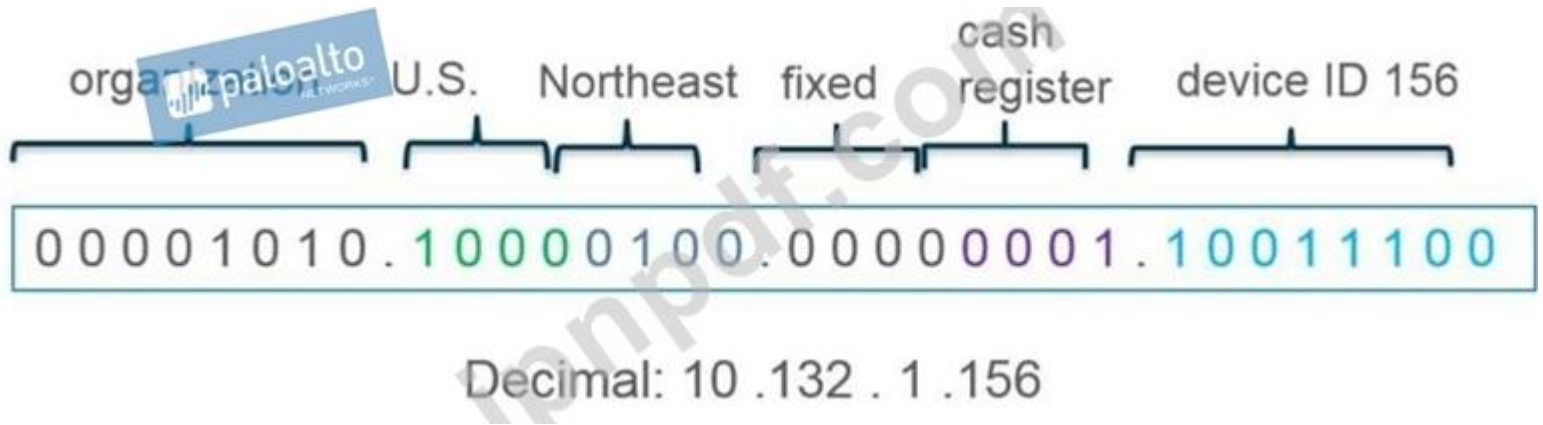
最新問題: 202
展示を参照してください。

```
##################################
admin@Lab33-111-PA-3060(active)>show routing fib

id        destination      nexthop     flags      interface          mtu
--------------------------------------------------------------------------
47        0.0.0.0/0        10.46.40.1  ug         ethernet1/3        1500
46        10.46.40.0/23    0.0.0.0     u          ethernet1/3        1500
45        10.46.41.111/32  0.0.0.0     uh         ethernet1/3        1500
70        10.46.41.113/32  10.46.40.1  ug         ethernet1/3        1500
51        192.168.111.0/24 0.0.0.0     u          ethernet1/6        1500
50        192.168.111.2/32 0.0.0.0     uh         ethernet1/6        1500

--------------------------------------------------------------------------
##################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1       interface2       flags              allowed-tags
--------------------------------------------------------------------------------
VW-1          ethernet1/7      ethernet1/5      p

######################################
```

トラフィックの入力インターフェイスが192.168.111.3から宛先10.46.41.113へのイーサネット1/7ソーシングである場合、どちらが出力インターフェイスになりますか？

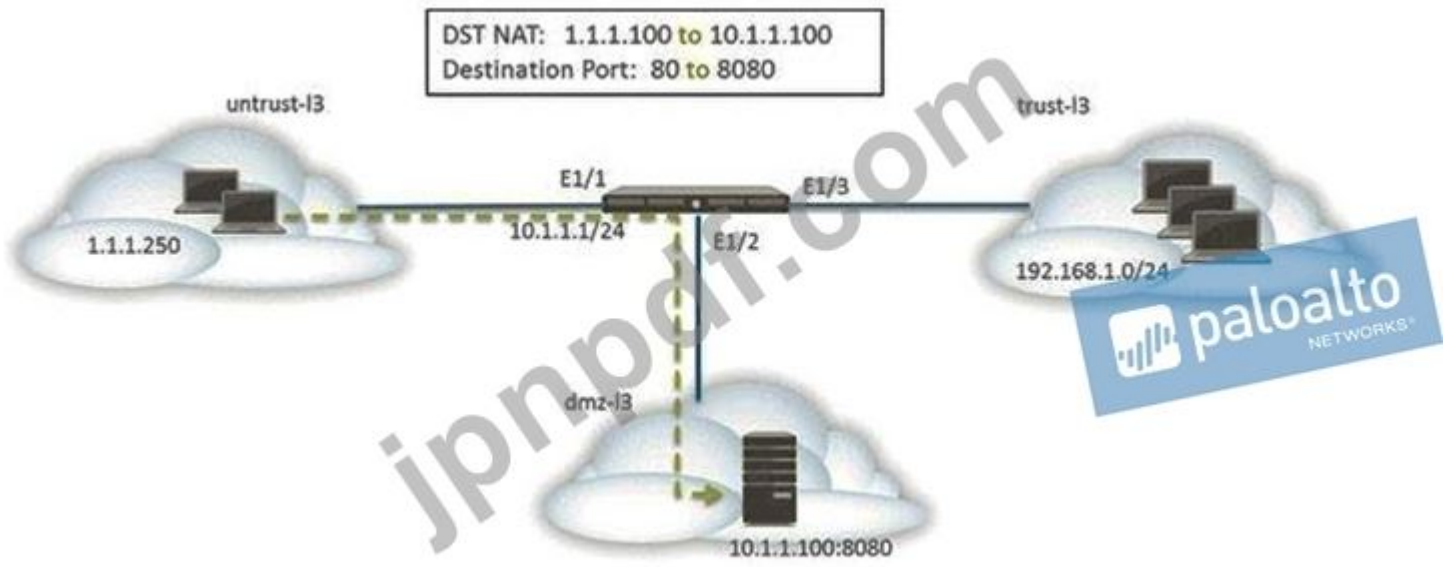
A. ethernet1 / 5
B. ethernet1 / 6
C. ethernet1 / 3
D. ethernet1 / 7
Answer: A (メーッセージを残す**)**

最新問題: **203**
図に示すように、アドレス指定構造がアドレスの特定のビットに意味を割り当てる内部デバイスには、どのタイプのアドレスオブジェクトが役立ちますか？



A. IPネットマスク
B. IPワイルドカードマスク
C. IPアドレス
D. IP範囲
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/networking-features/wildcard-address

最新問題: **204**
Webサーバーは、ポート8080でHTTPトラフィックをリッスンするように構成されています。クライアントは、TCPポート80でIPアドレス1.1.1.100を使用してWebサーバーにアクセスします。宛先NATルールは、IPアドレスとレポートの両方を10.1.1.100に変換するように構成されています。TCPポート8080。



ファイアウォールで構成する必要があるNATおよびセキュリティルールはどれですか？ 2つ選択してください）
A. Webブラウジングアプリケーションを使用して、untrust-l3ゾーンからdmz-l3ゾーンの1.1.100の宛先までのいずれかのソースを持つセキュリティポリシー。
B. service-httpサービスを使用して、送信元がuntrust-l3ゾーンから宛先がuntrust-l3ゾーンの1.1.1.100までのNATルール。

C. Webブラウジングアプリケーションを使用して、untrust-l3ゾーンからdmz-l3ゾーンの宛先10.1.1.100までのいずれかのソースを持つセキュリティポリシー
D. untrust-l3ゾーンから、service-httpサービスを使用したdmz-zoneの宛先10.1.1.100までのいずれかの送信元を持つNATルール。
Answer: A,D (メーッセージを残す)

最新問題**: 205**
テンプレートとテンプレートスラックをより簡単に再利用するために、構成内のファイアウォール固有およびアプライアンス固有のIPリテラルの代わりにタームプレート変数を作成できます。正しい構成はどれですか。
A. @Panorama
B. #パンクラマ
C. &Panorama
D. $ Panorama
Answer: D (メーッセージを残す)
オブジェクトの変数名を使用して、テンプレートとテンプレートスタックを作成します。変数名はドル記号（"$"）で始まる必要があります。たとえば、複数の管理対象ファイアウォールおよびアプライアンスで構成するパノラマIPアドレスの変数として$Panoramaを使用できます。
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama-features/configuration-reusability-for-templates-and-template-stacks.html

最新問題**: 206**
クライアントのデータセンターには機密性の高いアプリケーションサーバーがあり、分散型サービス拒否攻撃によるリソースの枯渇を特に懸念しています。
複数のIPアドレス（DDoS攻撃）に起因するリソースの枯渇からこのサーバーを具体的に保護するように、パロアルトネットワークスNGFWをどのように構成できますか？
A. セッション数が定義されたDoS保護プロファイルを追加します。
B. 着信要求を抑制するためにQoSプロファイルを追加します。
C. 脆弱性保護プロファイルを追加して、攻撃をブロックします。
D. カスタムApp-IDを定義して、正当なアプリケーショントラフィックのみがサーバーに到達するようにします。
Answer: A (メーッセージを残す)

最新問題**: 207**
ファイアウォール管理者は、パロアルトネットワークスファイアウォールを通過するトラフィックの問題のトラブルシューティングを行っています。適切なパケットフィルタを設定した後、トラフィックに関連付けられたグローバルカウンタを表示する方法はどれですか。
A. GUIから、[モニター]タブの下の[グローバルカウンターの表示]を選択します。
B. CLIから、show counter global filterpacket-filteryesコマンドを発行します。
C. CLIから、入力インターフェイスに対してshowcounterinterfaceコマンドを発行します。
D. CLIから、show counter global filterpcapyesコマンドを発行します。
Answer: B (メーッセージを残す)

最新問題**: 208**

管理者は、トラフィックログでunknown-tcpとして識別されたいくつかのインバウンドセッションを確認します。管理者は、これらのセッションが会社独自の会計アプリケーションにアクセスする外部ユーザーからのものであると判断します。管理者は、このトラフィックをアカウンティングアプリケーションとして確実に識別し、このトラフィックをスキャンして脅威を検出したいと考えています。
どのオプションがこの結果を達成しますか？
A. カスタムApp-IDを作成し、[詳細設定]タブでスキャンを有効にします。
B. アプリケーションオーバーライドポリシーを作成します。
C. カスタムApp-IDを作成し、[注文条件]チェックボックスを使用します。
D. アプリケーションのアプリケーションオーバーライドポリシーとカスタム脅威シグネチャを作成します。
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

最新問題**: 209**
GlobalProtectポータルを設定する場合、認証プロファイルを指定する目的は何ですか？
A. ポータルへのゲートウェイ認証を有効にするには
B. ゲートウェイへのポータル認証を有効にするには
C. ポータルへのユーザー認証を有効にする
D. ポータルへのクライアントマシン認証を有効にする
Answer: (解答を表示する**)**
ブラウザとサテライトの追加オプションを使用すると、特定のシナリオで使用する認証プロファイルを指定できます。「ブラウザー」を選択して、GlobalProtectエージェント（WindowsおよびMac）をダウンロードする目的でWebブラウザーからポータルにアクセスするユーザーを認証するために使用する認証プロファイルを指定します。[衛星]を選択して、衛星の認証に使用する認証プロファイルを指定します。
参照：https ://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals