PaloAltoNetworks.PCNSE-JPN.v2022-01-01.q127

試験コード：	PCNSE-JPN
試験名称：	Palo Alto Networks Certified Network Security Engineer Exam (PCNSE日本語版)
認証ベンダー：	Palo Alto Networks
無料問題の数：	127
バージョン：	v2022-01-01
ページの閲覧量：	476
問題集の閲覧量：	20187

https://www.jpnshiken.com/shiken/PaloAltoNetworks.PCNSE-JPN.v2022-01-01.q127.html

質問: **1**
どのオプションがコンテンツ検査プロセスの一部ですか？
A. Packet forwarding process
B. SSL Proxy re-encrypt
C. IPsec tunnel encryption
D. Packet egress process
正解: **(**正解を表示します**)**
Explanation
http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

質問: **2**
PanoramaをPAN-OS 8.1より前のバージョンに戻す場合、管理者は何を考慮する必要がありますか？
A. 管理者はExpeditionツールを使用して、構成をPAN-OS 8.1より前の状態に調整する必要があります。
B. 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。
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た変数は自動的に削除されます。
D. 管理者は、PAN-OS 8.1より前のバージョンで使用されているものに手動で可変文字を更新する必要があります。
正解: **B (**コメントを発表する**)**

質問: **3**
変数名はどの記号で始まる必要がありますか？
A. $
B. &

C. !
D. #
正解: **(**正解を表示します**)**
Explanation
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-firewalls/manage-templates-and-temp

質問: **4**
どのセッティングが、DOS保護プロフィールをソースIPアドレスから最大の並列のセッションを制限させます？
A. タイプを集約に設定し、 ₧セッション」ボックスをチェックし、最大同時セッション数を4000に設定します。
B. タイプをClassifiedに設定し、セッションのボックスをクリアし、最大同時セッション数を4000に設定します。
C. 分類済み」タイプを設定し、 ₧セッション」ボックスをチェックし、最大同時セッション数を4000に設定します。
D. タイプをAggregateに設定し、セッションのボックスをクリアし、最大同時セッション数を4000に設定します。
正解: **(**正解を表示します**)**

質問: **5**
UDP-4501プロトコルポートは、どの2つのGlobalProtectコンポーネント間で使用されますか？
A. GlobalProtectアプリとGlobalProtectゲートウェイ
B. GlobalProtectアプリとGlobalProtectポータル
C. GlobalProtectアプリとGlobalProtect衛星
D. GlobalProtectポータルとGlobalProtectゲートウェイ
正解: **(**正解を表示します**)**

質問: **6**
仮想ルータでは、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
正解: **B (**コメントを発表する**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/virtual-routers

質問: **7**

管理者は、トラフィックログでunknown-tcpと識別された複数の受信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、会社の専有会計アプリケーションにアクセスする外部ユーザーのフォーム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、このトラフィックで脅威をスキャンする必要があります。
この結果を達成するオプションはどれですか？
A. カスタムApp-IDを作成し、詳細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、 順序付けられた条件」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の署名を作成します。
正解: **(**正解を表示します**)**
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRoCAK

質問: **8**
フォワードUntrust証明書はどのように使用されていますか？
A. Webサーバーがクライアント証明書を要求するときに使用されます。
B. 接続先のサーバーがファイアウォールによって信頼されていない認証局によって署名されている場合、クライアントに提示されます。
C. クライアントが復号化されたサイトに接続しようとすると、Untrustセキュリティゾーンで発生した証明書が発行されます。
D. これは、キャプティブポータルが不明なユーザーを識別するために使用されます。
正解: **(**正解を表示します**)**

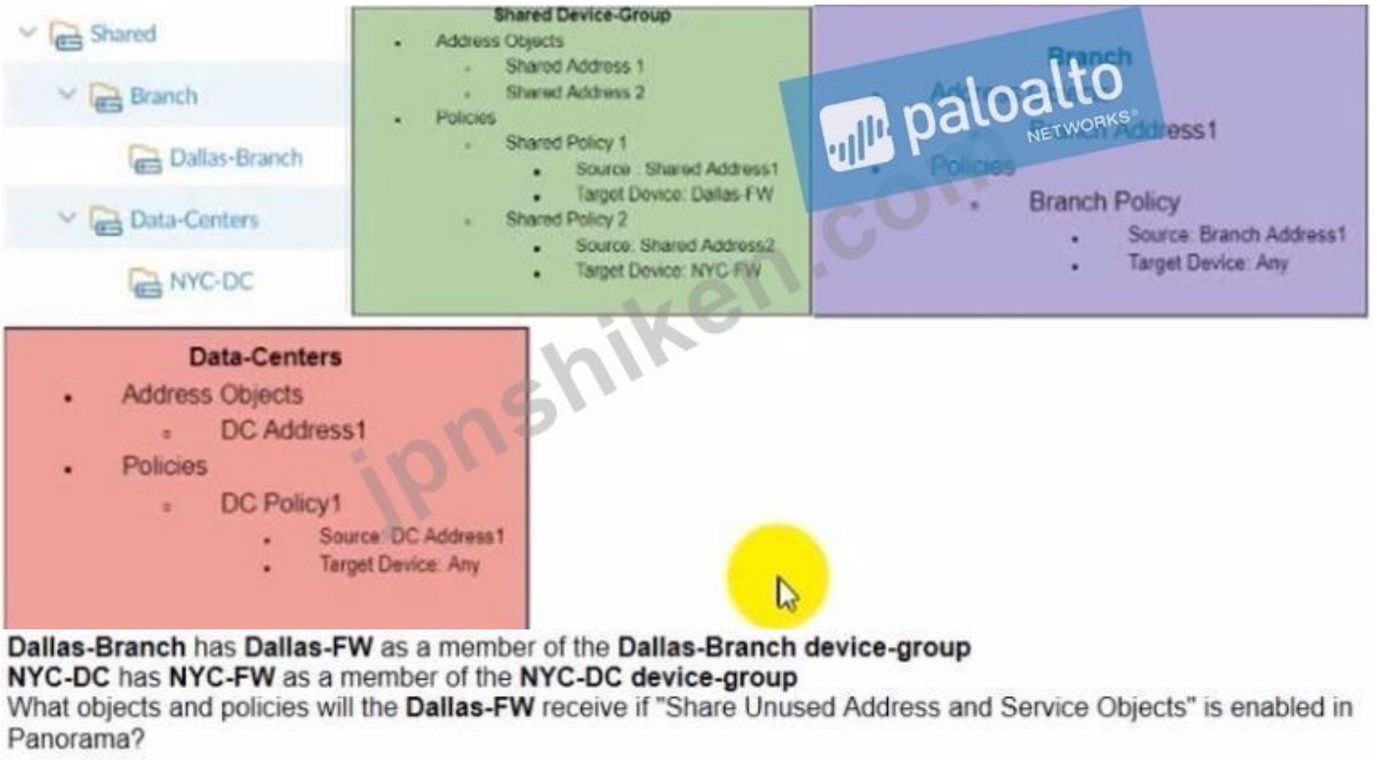
質問: **9**
ネットワーク技術者は、ファイアウォール上でvr1を通じて98.139.183.24に達する問題のレポートを復活させました。このファイアウォールのルーティングテーブルは、広範かつ複雑です。
どのCLIコマンドが、問題を識別するのに役立つか？
A. show routing interface
B. test routing fib virtual-router vr1
C. test routing fib-lookup ip 98.139.183.24 virtual-router vr1
D. show routing route type static destination 98.139.183.24
正解: **C (**コメントを発表する**)**

質問: **10**
管理者は、QoSポリシールールと、YouTubeアプリケーションの最大許容帯域幅を制限するQoSプロファイルを設定しました。ただし、YouTubeは最大帯域幅割り当てよりも多くを消費しています。
QoSを有効にするためにはどの設定ステップを設定する必要がありますか？
A. QoSデータフィルタリングプロファイルを有効にする

B. QoSモニタを有効にする
C. Qosインターフェイスを有効にする
D. インターフェイスの管理プロファイルでQosを有効にします。
正解: **C** (コメントを発表する)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-qos/qos-interface-sett

質問: **11**
エンタープライズ展開では、ネットワークセキュリティエンジニアは、ファイアウォールにローカル管理者アカウントを作成せずに、管理者グループに割り当てる必要があります。
どの認証方法を使用する必要がありますか？
A. LDAP
B. RADIUS with Vendor-Specific Attributes
C. Certification based authentication
D. Kerberos
正解: (正解を表示します)

質問: **12**
次のオブジェクトとポリシーは、デバイスグループ階層で定義されています



A)

B)


C)
アドレスオブジェクト
-共有アドレス1
-支店住所2
ポリシー共有Polic1
l-ブランチポリシーl
D)
アドレスオブジェクト共有アドレス1-共有アドレス2-ブランチアドレスポリシー共有ポリシー1-共有ポリシー2-ブランチポリシーl
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
正解: **(**正解を表示します**)**

質問: **13**
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
正解: **D,E,F (**コメントを発表する**)**
Explanation

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

質問: **14**
エンジニアは、復号化ブローカー機能を構成する必要があります
どのDecryptionBrokerセキュリティチェーンが双方向のトラフィックフローをサポートしていますか？
A. レイヤー2セキュリティチェーン
B. レイヤー3セキュリティチェーン
C. トランスペアレントブリッジセキュリティチェーン
D. 透過プロキシセキュリティチェーン
正解: **(**正解を表示します**)**
Explanation
Together, the primary and secondary interfaces form a pair of decryption forwarding interfaces. Only interfaces that you have enabled to be Decrypt Forward interfaces are displayed here. Your security chain type (Layer 3 or Transparent Bridge) and the traffic flow direction (unidirectional or bidirectional) determine which of the two interfaces forwards allowed, clear text traffic to the security chain, and which interface receives the traffic back from the security chain after it has undergone additional enforcement.

質問: **15**
インストールされたセッションがアプリケーションで識別できる3つの理由は何ですか
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. 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
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. 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
正解: **(**正解を表示します**)**

質問: **16**
どの方法でパロアルトネットワークNGFWにタグを動的に登録しますか？
A. ファイアウォール上またはユーザーIDエージェントまたは読み取り専用ドメインコントローラー（RODC）上のRestful APIまたはVMWare API
B. ファイアウォールまたはUser-IDエージェント上のRestful APIまたはVMware API
C. ファイアウォールまたはUser-IDエージェントまたはCLI上のXML-APIまたはVMware API
D. NGFWまたはUser-IDエージェント上のXML APIまたはVMモニタリングエージェント
正解: **D (**コメントを発表する**)**
Reference:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/policy/monitor-changes-in-the-virtual-environmen

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu
875問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
復号化ポリシールールの一致に有効な3つの修飾子は何ですか？ （3つ選択してください）
A. カスタムURLカテゴリ
B. ユーザーID
C. 宛先ゾーン
D. ソースインターフェイス
E. アプリID
正解: **B,C,D** (コメントを発表する)

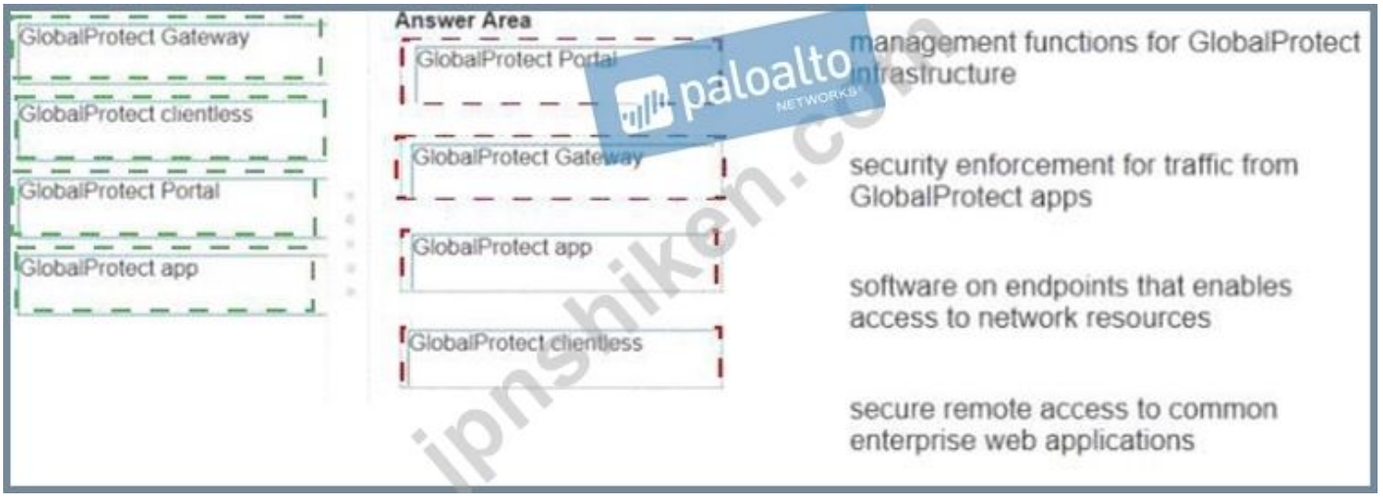
質問: **18**
ファイル共有アプリケーションが許されて、誰も、何でそれのためにこのアプリケーションが使われるかを知らない。
このアプリケーションはどのようにブロックする必要がありますか？
A. レイヤ4およびレイヤ7攻撃をブロックするWildFire Analysisプロファイルを作成する
B. すべての既知の内部カスタムアプリケーションをブロックする
C. セキュリティポリシーを使用して、未承認のアプリケーションをすべてブロックする
D. レイヤ4およびレイヤ7攻撃をブロックするファイルブロックプロファイルを作成する
正解: (正解を表示します)

質問: **19**
管理者は、すべての非ネイティブMFAプラットフォームをPAN-OSソフトウェアに統合するためにどの方法を使用しますか？
A. オクタ
B. DUO
C. RADIUS
D. PingID
正解: **C** (コメントを発表する)
Explanation
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-auth

質問: **20**

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

正解:



Explanation

The GlobalProtect portal provides the management functions for your GlobalProtect infrastructure The GlobalProtect gateways provide security enforcement for traffic from GlobalProtect apps The GlobalProtect app software runs on endpoints and enables access to your network resources

質問: **21**

ユーザーが誤って企業の資格情報をフィッシングサイトに送信しないようにするには、どの機能を設定する必要がありますか？

A. URL Filtering profile

B. Zone Protection profile

C. Anti-Spyware profile

D. Vulnerability Protection profile

正解: **(**正解を表示します**)**

Reference:

https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishin

質問: **22**
globalProtectゲートウェイでは、どの3つのスプリットトンネル方式がサポートされていますか？（3つ選んでください。）
A. クライアント申請プロセス
B. ビデオストリーミングアプリケーション
C. 宛先ユーザー/グループ
D. ソースドメイン
E. 宛先ドメイン
F. URLカテゴリ
正解: **(**正解を表示します**)**

質問: **23**
管理者は、ポリシーマットが展開されることを検証する必要があります。devce-oroup階層の適切なルールと一致します。管理者は、ポリシー作成ロジックを確認し、不要なトラフィックが許可されていないことを確認するためにどのツールを使用できますか？
A. テストポリシーの一致
B. 管理対象デバイスの状態
C. ポリシーオプティマイザー
D. 変更のプレビュー
正解: **A (**コメントを発表する**)**

質問: **24**
いくつかのオフィスは、静的IPV4ルートを使用してVPNに接続されています。管理者は、静的ルーティングを置き換えるためにOSPFを実装することが任されています。
この目標を達成するためにはどのステップが必要ですか？
A. 個々のサイトで個々のトンネルインタフェースのIPアドレスを割り当てなさい
B. すべてのイーサネットおよびトンネルインターフェイスにOSPFエリアID 0.0.0.0を割り当てます
C. 個々のトンネルインタフェースのOSPFv3を可能にし、エリアID0.0.0.0を使いなさい
D. 各サイトで新しいVPNゾーンを作成して各VPN接続を終了する
正解: **(**正解を表示します**)**

質問: **25**
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

正解:

Explanation

Plan to defend your network against different types of DoS attacks:

* Application-Based Attacks

-Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it.

An example of this is the Slowloris attack.

* Protocol-Based Attacks

-Also known as state-exhaustion attacks, these attacks target protocol weaknesses. A common example is a SYN flood attack.

* Volumetric Attacks

-High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing those resources.

An example of this is a UDP flood attack.

https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/zone-protection-and-dos-protection/zone-defense.ht

質問: **26**

ファイアウォールが再起動されたときの[未使用ルールの強調表示]と[ルール使用状況ヒット]カウンタの2つの動作の違いは何ですか？ 2つ選んでください。）

A. ルール使用ヒットカウンターはリセットされません

B. ルールの使用法ヒットカウンタがリセットされます。

C. 未使用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. 未使用ルールを強調表示すると、ゼロルールが強調表示されます。

正解: **(正解を表示します)**

質問: **27**
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.Webブラウジングアクセスを許可するようにTrust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を構成する必要があります。Webサーバーは HTTP ⑤でコンテンツをホストします。トラストからDMZへのトラフィックは、フォワード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ように、サービスとアプリケーションの組み合わせとセキュリティポリシールールの順序を設定する必要があります。
A. Rule #1: application: web-browsing; service: application-default; action: allowRule #2: application: ssl; service: application-default; action: allow
B. Rule #1: application: web-browsing; service: service-https; action: allowRule #2: application: ssl; service: application-default; action: allow
C. Rule # 1: application: ssl; service: application-default; action: allowRule #2: application: web-browsing; service: application-default; action: allow
D. Rule #1: application: web-browsing; service: service-http; action: allowRule #2: application: ssl; service: application-default; action: allow
正解: **(**正解を表示します**)**
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEyCAK

質問: **28**
どの3つのファイアウォール状態が有効ですか？ ③つ選択してください）
A. Active
B. Functional
C. Pending
D. Passive
E. Suspended
正解: **(**正解を表示します**)**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

質問: **29**
トンネルインターフェイスを使用してサイトツーサイトVPNを設定する場合
どの2つのフォーマットがトンネルインターフェースの名前付けに適していますか？ ②つを選択してください）
A. tunnel 1025
B. tunnel. 1
C. vpn-tunne.1

D. Vpn-tunnel.1024
正解: **(**正解を表示します**)**

質問: **30**
新しいパロアルトネットワークのファイアウォールをプロビジョニングするときに、ライセンスをアクティブにする必要があるのはいつですか？
A. 証明書プロファイルを設定するとき
B. ユーザーアクティビティレポートを構成するとき
C. ウイルス対策動的更新を構成するとき
D. GlobalProtectポータルを設定する場合
正解: **C (**コメントを発表する**)**

質問: **31**
レイヤ3インターフェイスを設定する場合、必須の手順は何ですか。
A. 各レイヤー3インターフェイスに接続する必要があるセキュリティプロファイルを構成します
B. 各レイヤー3インターフェースのトラフィックをルーティングするようにサービスルートを構成します
C. 各レイヤ3インターフェイスに接続する必要があるインターフェイス管理プロファイルを設定します
D. 各レイヤー3インターフェースのトラフィックをルーティングするように仮想ルーターを構成します
正解: **A (**コメントを発表する**)**

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu **875**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
組織は最近、インフラストラクチャと構成をNGFWに移行しました。NGFWでは、Panoramaがデバイスを管理します。組織はL2-L4ファイアウォールベンダーから来ていますが、不要になったポリシーを特定しながらApp-IDを使用したいと考えています。どのPanoramaツールが役立つかこの組織？
A. アプリケーショングループ
B. テストポリシーの一致
C. ポリシーオプティマイザー
D. 構成監査

正解: (正解を表示します)

質問: **33**
ネットワークセキュリティエンジニアは、Wildfireの活動を分析するよう求められています。ただし、[Wildfire Submissions]アイテムは[Monitor]タブからは表示されません。
何がこの状態を引き起こす可能性がありますか？
A. ポリシーがWildFire投稿トラフィックをブロックしています。
B. エンジニアのアカウントにWildFireの投稿を表示する権限がありません。
C. ファイアウォールにはアクティブなWildFireサブスクリプションがありません。
D. WildFireが動作していますが、現時点ではWildFire Submissionsのログエントリはありません。
正解: (正解を表示します)

質問: **34**
テンプレート -スタックが装置に割り当てられる、そして、スタックが重なり合うセッティングで3つのテンプレートを含むならば、テンプレート -スタックが押されるとき、どのセッティングが装置に発表されますか？
A. セッティングは、stack.の上にあるテンプレートに割り当てられます
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促されます。
C. すべてのセッティングは、全部でテンプレートを設定しました。
D. ファイアウォール場所に従い、Panoramaは、送るセッティングで決めます。
正解: **A** (コメントを発表する)
Reference:
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manag templates-and-template-stacks/configure-a-template-stack

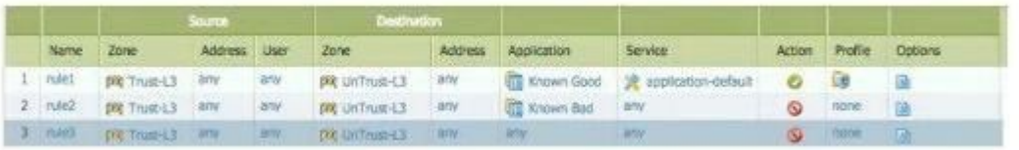
質問: **35**
Site-AとSite-Bの間にはサイト間VPNが設定されています。OSPFは、サイト間のルートを動的に作成するように構成されています。サイトAのOSPF設定は正しく設定されていますが、チューナーのルートが確立されていません。グラフィックのサイトBインターフェイスはブロードキャストリンクタイプを使用しています。管理者は、Site-BのOSPF設定が、そのインターフェイスの1つに不適切なリンクタイプを使用していると判断しました。

どのリンクタイプの設定でエラーを修正しますか？
A. Set Ethernet 1/1 to p2mp
B. Set tunnel. 1 to p2p
C. Set Ethernet 1/1 to p2p
D. Set tunnel. 1 to p2mp
正解: **B** (コメントを発表する)

質問: **36**
ネットワーク設計を変更するには、既存のファイアウォールが管理インターフェイスの代わりにデータプレーンインターフェイスアドレスからPalo Alto Updatesにアクセスする必要があります。
どの設定を変更する必要がありますか？
A. デフォルトルート
B. 管理プロファイル
C. 認証プロファイル
D. サービスルート
正解: **D** (コメントを発表する)

質問: **37**
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 // www companycom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にアクセスするときに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 :// www companycomにアクセスする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. 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
B. 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
C. 仮想ルーターのデフォルトルート上のネクストホップゲートウェイのパス監視を構成します
D. ファイアウォールの外部インターフェースのリンク監視プロファイルを有効にして構成します
正解: **C** (コメントを発表する)

質問: **38**
企業は、すべてのアプリケーションを拒否するポリシーを持っています。このポリシーは悪いと分類され、優良と分類されるアプリケーションのみが許可されます。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。



		Source			Destination						
	Name	Zone	Address	User	Zone	Address	Application	Service	Action	Profile	Options
1	rule1	Trust-L3	any	any	UnTrust-L3	any	Known Good	application-default			
2	rule2	Trust-L3	any	any	UnTrust-L3	any	Known Bad	any		none	
3	rule3	Trust-L3	any	any	UnTrust-L3	any	any	any		none	

特定のVLAN IDを受け入れるインターフェイス設定は何ですか？
ルール2とルール3の両方を持つことで得られるメリットはどれですか？ 2つ選ぶ）
A. ルール2および3は、異なるポート上のトラフィックに適用されます。
B. 個別のログ転送プロファイルは、ルール2と3に適用できます。
C. 異なるセキュリティプロファイルをトラフィックマッチングルール2および3に適用することができます。
D. 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。
正解: **(**正解を表示します**)**

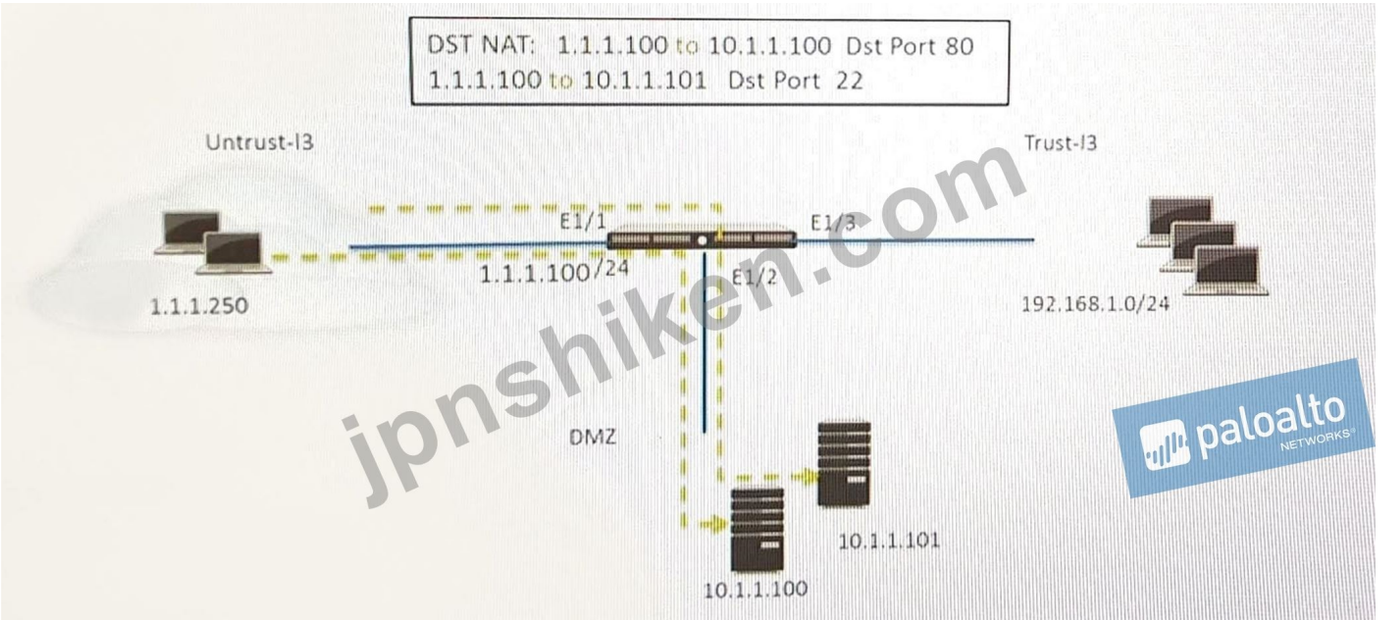
質問: **39**
パノラマを設定して動的更新を接続されたデバイスにプッシュするときに使用できる2つのサブスクリプションはどれですか？ 2つを選択してください）
A. Content-ID
B. User-ID
C. Applications and Threats
D. Antivirus
正解: **(**正解を表示します**)**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/device/device-dynamic-updates

質問: **40**
企業は既存のPalo Alto Networksファイアウォールをバージョン7.0.1から7.0.4にアップグレードしています。
ファイアウォール管理者は、PAN-OS 8.0.4を企業全体にインストールするためにどの3つの方法を使用できますか？ (Choose three)
A. 1つのファイアウォールを更新した後、PAN-OS 8.0.4アップデートを1つのファイアウォールから残りのすべてのファイアウォールにプッシュします。
B. PAN-OS 8.0.4ファイルをサポートサイトからダウンロードし、手動でアップロードした後に各ファイアウォールにインストールします。
C. 各ファイアウォールにPAN-OS 8.0.4を直接ダウンロードしてインストールしてください。
D. PAN-OS 8.0.4をUSBドライブにダウンロードすると、USBドライブがファイアウォールに挿入された後、ファイアウォールが自動的に更新されます。
E. 各ファイアウォールにインストールするには、サポートサイトからPAN-OS 8.0.4アップデートをプッシュします。
F. Panoramaから各ファイアウォールにPAN-OS 8.0.4をダウンロードしてプッシュします。

正解: **(**正解を表示します**)**

質問: **41**
必要なサービスへのアクセスを提供するためにインバンドデータポートが設定されている場合、サービスルートに割り当てられているインターフェイスには何が必要ですか。
A. DoSおよびゾーン保護を有効にする必要があります
B. インターフェースをレイヤー2レイヤー3または仮想ワイヤーに設定する必要があります
C. 必要なサービスへのトラフィックにはインターフェースを使用する必要があります
D. 静的IPアドレスを使用する必要があります
正解: **C (**コメントを発表する**)**

質問: **42**
展示を参照してください。



管理者はDNATを使用して、2つのサーバーを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）への信頼できない（任意）ssh、Webブラウジング許可
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
正解: **B,E (**コメントを発表する**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

jpnshiken.com

質問: **43**

ファイアウォールがMineMeldからIPアドレスをダウンロードしていません。そのイメージに基づいて、最も可能性が高いのは何でしょうか。

A. 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。

B. 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。

C. 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。

D. 外部動的リストはSSL接続をサポートしません。

正解: **(**正解を表示します**)**

質問: **44**

次の画像に基づいて、

jpnshiken.com
paloalto NETWORKS

ルート、中間、およびエンドユーザーの証明書の正しいパスは何ですか？

A. VeriSign > Symantec > Palo Alto Networks

B. Symantec > VeriSign > Palo Alto Networks

C. Palo Alto Networks > Symantec > VeriSign
D. VeriSign > Palo Alto Networks > Symantec
正解: (正解を表示します)

質問: **45**
管理者はユーザーID展開のトラブルシューティングを行う必要があります管理者はLDAP認証に関連する問題があると考えています管理者は管理プレーンでパケットキャプチャを作成したいと考えています管理者が構成を検証するためのパケットキャプチャを取得するために使用するCLIコマンド^
A. > scp export pcap from pcap to (usernameQhost:path)
B. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>
C. > scp export mgmt-pcap from mgmt.pcap to {usernameQhost:path>
D. > scp export pcap-mgmt from pcap.mgiat to (username@host:path)
正解: (正解を表示します)

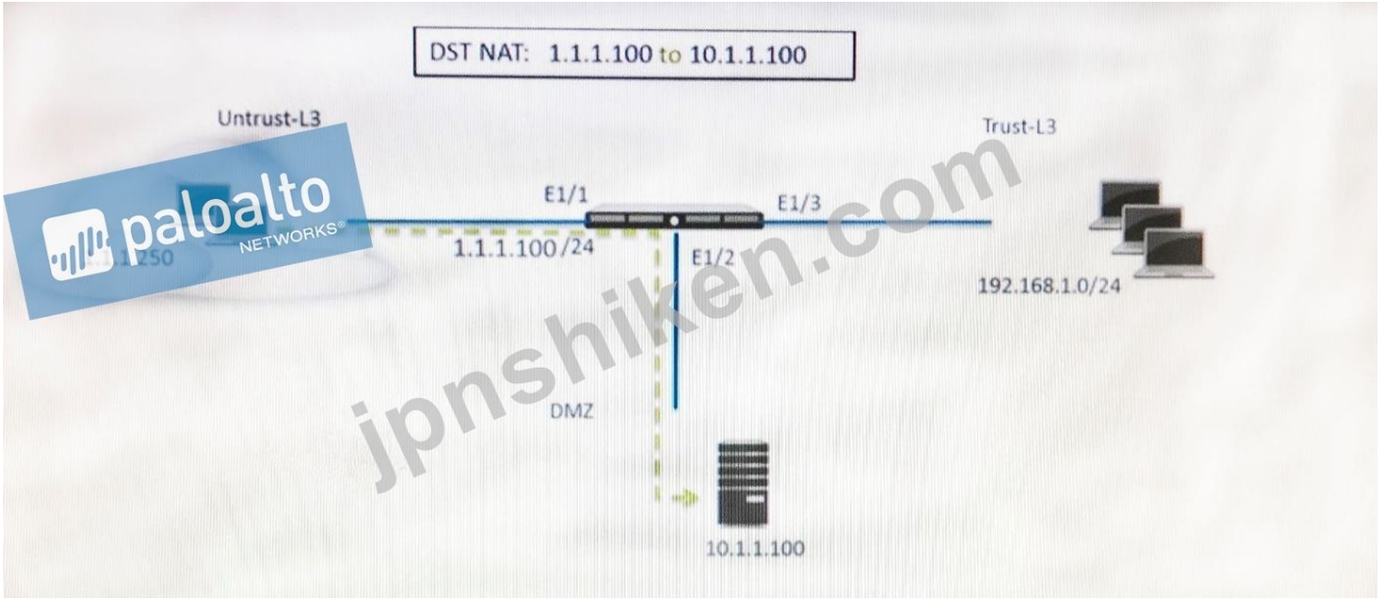
質問: **46**
管理者は、パロアルトネットワークNGFWの管理インターフェース上のトラフィックをどのように監視/キャプチャしますか？
A. デバッグデータプレーンのpacket-diag set capture stageファイアウォールファイルコマンドを使用します。
B. トラフィックキャプチャの4つの段階すべてを有効にします（TX、RX、DROP、ファイアウォール）。
C. debug dataplane packet-diag setキャプチャステージ管理ファイルコマンドを使用します。
D. topdumpコマンドを使用します。
正解: (正解を表示します)
Reference: https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/ta-p/62390
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-captu

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu
875問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**

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. 構成同期を無効にする
D. HAを無効にする
正解: **(**正解を表示します**)**

質問: **48**
展示を参照してください。



DMZ内のWebサーバーが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サーバーに流れるようにするセキュリティポリシールールはどれですか？
A. Untrust (any) to Untrust (10. 1.1. 100), web browsing - Allow
B. Untrust (any) to Untrust (1. 1. 1. 100), web browsing - Allow
C. Untrust (any) to DMZ (1. 1. 1. 100), web browsing - Allow
D. Untrust (any) to DMZ (10. 1. 1. 100), web browsing - Allow
正解: **C (**コメントを発表する**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

質問: **49**
管理者は、Palo Alto NetworksNGFW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？

jpnshiken.com

A. セキュリティポリシールール
B. サービスルート
C. CRL
D. スケジューラー
正解: **A (**コメントを発表する**)**

質問: **50**
管理者は、新しい構成をPanoramaからアクティブ/パッシブHAペアとして構成された一対のファイアウォールにプッシュします。
どのNGFWがPanoramaから設定を受信しますか？
A. パッシブファイアウォールはアクティブファイアウォールと同期します
B. アクティブなファイアウォールは、パッシブファイアウォールと同期します
C. 活発で受動的なファイアウォール それから、それは互いに同期します）
D. アクティブファイアウォールとパッシブファイアウォールの両方が独立しており、後で同期はありません
正解: **(**正解を表示します**)**
Explanation
Palo Alto NetworksPanorama 7.0 Administrator's Guide *77Manage FirewallsManage Device GroupsManage Device GroupsAdd a Device GroupCreate a Device Group HierarchyCreate Objects for Use in Shared or Device Group PolicyRevert to Inherited Object ValuesManage Unused Shared ObjectsManage Precedence of Inherited ObjectsMove or Clone a Policy Rule or Object to a Different Device GroupSelect a URL Filtering Vendor on PanoramaPush a Policy Rule to a Subset of FirewallsManage the Rule HierarchyAdd a Device GroupAfter adding firewalls (see Add a Firewall as a Managed Device), you can group them into Device Groups (up to 256), as follows. Be sure to assign both firewalls in an active-passive high availability (HA) configuration to the same device group so that Panorama will push the same policy rules and objects to those firewalls. ###############PAN-OS doesn't synchronize pushed rules across HA peers.########## To manage rules and objects at different administrative levels in your organization, Create a Device Group Hierarchy.
https://docs.paloaltonetworks.com/panorama/8-0/panorama-admin/manage-firewalls/transition-a-firewall-to-pano
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS

質問: **51**
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。
また、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を作成します。
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Unknownとしてドロップされたトラフィックを示します。

次の2つのエントリは、アプリケーションSSLとして許可された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. ファイアウォールの[排他キャッシュ]オプションを無効にします。
B. サポートされていないcypher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、そのプロファイルを復号化ルールに添付します。
C. 暗号化されたBitTorrentトラフィックとアクション 「No-Decrypt」の一致する復号ルールを作成し、ルールを復号ポリシーの最上位に配置します。
D. アプリケーションの "暗号化されたBitTorrent"と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置きます。
正解: **(**正解を表示します**)**

質問: **52**
ファイアウォールにリンク監視の設定がある場合、フェールオーバーはどのようなものになりますか？

A. ethernet1/3 and ethernet1/6 going down
B. ethernet1/3 going down
C. ethernet1/6 going down
D. ethernet1/3 or Ethernet1/6 going down
正解: **(**正解を表示します**)**

質問: **53**
どのCLIコマンドが現在の管理計画のメモリ使用率を表示していますか？
A. > システム情報を表示する
B. > システムリソースを表示する
C. > デバッグ管理サーバショー
D. > 実行中のリソースモニタを表示する
正解: **B (**コメントを発表する**)**
Explanation

https://live.paloaltonetworks.com/t5/Management-Articles/Show-System-Resource-Command-Displays-CPU-Ut

質問: **54**
ネットワーク管理者は、パノラマを使用して、ブランチオフィスの管理対象ファイアウォールにセキュリティポリシーを適用します。支店の管理者がこれらの製品を無効にする場合は、どのポリシータイプをPanoramaに設定する必要がありますか？
A. Pre Rules
B. Implicit Rules
C. Post Rules
D. Explicit Rules
正解: **(**正解を表示します**)**

質問: **55**
管理プレーンの負荷を軽減するのに最適な構成タスクはどれですか？
A. 開始時にセッションロギングを有効にする
B. デフォルトの拒否ルールでログを無効にする
C. 事前定義されたレポートを無効にする
D. アラートを送信するようにURLフィルタリングアクションを設定します
正解: **(**正解を表示します**)**

質問: **56**
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. ゾーン保護サブスクリプションをアクティブ化します。
C. 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
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
正解: **(**正解を表示します**)**

質問: **57**
管理者は、トラフィックログでunknown-tcpと識別された複数の受信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、会社の専有会計アプリケーションにアクセスする外部ユーザーのフォーム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、このトラフィックで脅威をスキャンする必要があります。
この結果を達成するオプションはどれですか？
A. カスタムApp-IDを作成し、 順序付けられた条件」チェックボックスを使用します。
B. カスタムApp-IDを作成し、詳細タブでスキャンを有効にします。

C. 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の署名を作成します。
D. 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。
正解: **C** (コメントを発表する)

質問: **58**
パロアルトネットワークファイアウォールがNTP増幅攻撃によりターゲットとされて、それには単一の宛先IPアドレスに1秒あたり数十 数千個のUDP接続が氾濫してポストている。
legitirnateトラフィックを他のホスト中ネットワークに低下させずに訂正入り口で可能な時のどのオプションが、この攻撃を和らげるか？
A. UDP洪水保護を持つゾーン保護方針
B. 最大限度以下のトラフィックを抑制するQoSポリシー
C. 攻撃を受けているIPアドレスとポートへのトラフィックを拒否するセキュリティポリシールール
D. 保護アクションのみで宛先IPを使用してDoS保護ポリシーを分類された
正解: **D** (コメントを発表する)

質問: **59**
管理者は、一対のPalo Alto Networks NGFWに対してアクティブ/アクティブHAを設定するように依頼されました。ファイアウォールは、レイヤ3インターフェイスを使用して、ペアの単一のゲートウェイIPにトラフィックを送信します。
どのHA構成が有効になりますか。
A. 2つのファイアウォールは単一のフローティングIPを共有し、フローティングIPを共有するためにgratuitous ARPを使用します。
B. 各ファイアウォールは個別のフローティングIPを持ち、優先順位によってどのファイアウォールがプライマリIPを持つかが決まります。
C. ファイアウォールは同じインターフェイスIPアドレスを共有し、デバイス0に障害が発生した場合、デバイス1はフローティングIPを使用します。
D. ファイアウォールは、アクティブ/アクティブHAでフローティングIPを使用しません。
正解: (正解を表示します)

質問: **60**
管理者は、ローカルの社内のラボ環境（「クラウド」ではなく）で100個の仮想ファイアウォールを作成するよう求められています。ブートストラップは、このタスクを実行する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について、どのオプションが説明されていますか？
A. USBスティックでconfig-driveを使用してください。
B. ISOを備えた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で仮想CD-ROMを使用します。
正解: **(**正解を表示します**)**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapp firewalls-for-rapid-deployment.html

質問: **61**
URLフィルタリングでは、どのコンポーネントがURLパターンに一致しますか？
A. 管理プレーンでのライブURLフィード
B. データプレーンでのセキュリティ処理
C. データプレーンでのシングルパスパターンマッチング
D. データプレーンでの署名マッチング
正解: **(**正解を表示します**)**

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu
375問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **62**
Site-AとSite-BはIKEv2を使用してVPN接続を確立する必要があります。サイトAは、公的なIPアドレスを使ってインターネットと直接接続する。Site-BはISPルータ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の間に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. パッシブモードでサイトBだけで有効にする
B. サイトBのみで有効にする
C. サイトAおよびサイトBで有効にする
D. サイトAのみで有効にする
正解: **(**正解を表示します**)**

質問: **63**
管理者は、世界中のGlobalProtectゲートウェイとして機能する15のファイアウォールを展開することを計画しています。Panoramaはファイアウォールを管理します。ファイアウォールはモバイルユーザーへのアクセスを提供し、オンプレミスインフラストラクチャへのエッジロケーションとして機能します。同じテンプレート構成を使用するファイアウォールの管理者がこの構成を拡張するために使用できる2つのソリューションはどれですか。 2つ選択してください。）

A. テンプレートスタック
B. 仮想システム
C. コレクターグループ
D. 変数
正解**: (**正解を表示します**)**

質問**: 64**
SSHプロキシ復号化ポリシーを作成する前に、どのような前提条件を満たす必要がありますか？
A. SSH鍵とSSL証明書の両方を生成する必要があります。
B. 前提条件は必要ありません。
C. SSHキーは手動で生成する必要があります。
D. SSL証明書を生成する必要があります。
正解**: B (**コメントを発表する**)**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssh-proxy
"In an SSH Proxy configuration, the firewall resides between a client and a server. SSH Proxy enables the firewall to decrypt inbound and outbound SSH connections and ensures that attackers don't use SSH to tunnel unwanted applications and content. SSH decryption does not require certificates and the firewall automatically generates the key used for SSH decryption when the firewall boots up."

質問**: 65**
証明書の失効ステータスを検証するために設定できる2つの方法はどれですか。 2つ選んでください。）
A. CRL
B. Cert-Validation-Profile
C. SSL/TLS Service Profile
D. OCSP
E. CRT
正解**: (**正解を表示します**)**

質問**: 66**
DMZゾーンでホストされているWebサーバーへのインターネットゾーン上のユーザーのために、どのゾーンペアとルールタイプを使用して接続できますか？ Webサーバーは、Palo Alto Networksの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. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ
Rule Type:

"intrazone"
B. Zone Pair:
Source Zone: Internet
Destination Zone: DMZ
Rule Type:
"intrazone" or "universal"
C. Zone Pair:
Source Zone: Internet
Destination Zone: Internet
Rule Type:
"intrazone" or "universal"
D. Zone Pair:
Source Zone: Internet
Destination Zone: Internet
Rule Type:
"intrazone"
正解**: B (**コメントを発表する**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/zo
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

質問**: 67**
HAフェイルオーバーのシナリオでは、セッションがSSL転送プロキシ復号化ポリシーに一致するとどうなりますか？
A. HA Syncは発生しません。既存のセッションは、アクティブなファイアウォールに転送されます。
B. HA同期が発生し、セッションがテストパスに送信されます
C. HA Syncが発生し、ファイアウォールがセッションを許可します。Putはセッションを復号化しません。
D. HA同期が発生しないファイアウォールがセッションをドロップします。
正解**: (**正解を表示します**)**

質問**: 68**
PAN-OSソフトウェアがMFAをサポートする3つの認証要素はどれですか（3つ選択してください）。
A. Push
B. Pull
C. Okta Adaptive

D. Voice
E. SMS
正解: **A,D,E (**コメントを発表する**)**
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authe

質問: **69**
クライアントはデータセンターに機密アプリケーションサーバーを持ち、特に分散型サービス拒否攻撃のためにリソースの枯渇を懸念しています。
パロアルトネットワークNGFWは、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保護するために、どのように構成できますか？
A. 正当なアプリケーショントラフィックだけがサーバに到達するように、カスタムApp-IDを定義します。
B. 攻撃をブロックする脆弱性保護プロファイルを追加します。
C. 着信要求を抑制するQoSプロファイルを追加します。
D. セッション数が定義されたDoSプロテクションプロファイルを追加します。
正解: **D (**コメントを発表する**)**
Reference: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

質問: **70**
トラフィックをスキャンし脅威から保護する能力を犠牲にすることなく、リモートクライアントをパロアルトネットワークインフラストラクチャに接続するために使用できるクライアントソフトウェアはどれですか？
A. X-Auth IPsec VPN
B. GlobalProtect Apple IOS
C. GlobalProtect SSL
D. GlobalProtect Linux
正解: **(**正解を表示します**)**
Explanation
(http://blog.webernetz.net/2014/03/31/palo-alto-globalprotect-for-linux-with-vpnc/)

質問: **71**
管理者が認証エンフォースメントを構成していて、特定のグループを認証から免除するための免除ルールを作成したいと考えています。どの認証実施オブジェクトを選択する必要がありますか？
A. デフォルト認証バイパス
B. default-browser-challenge
C. default-web-format

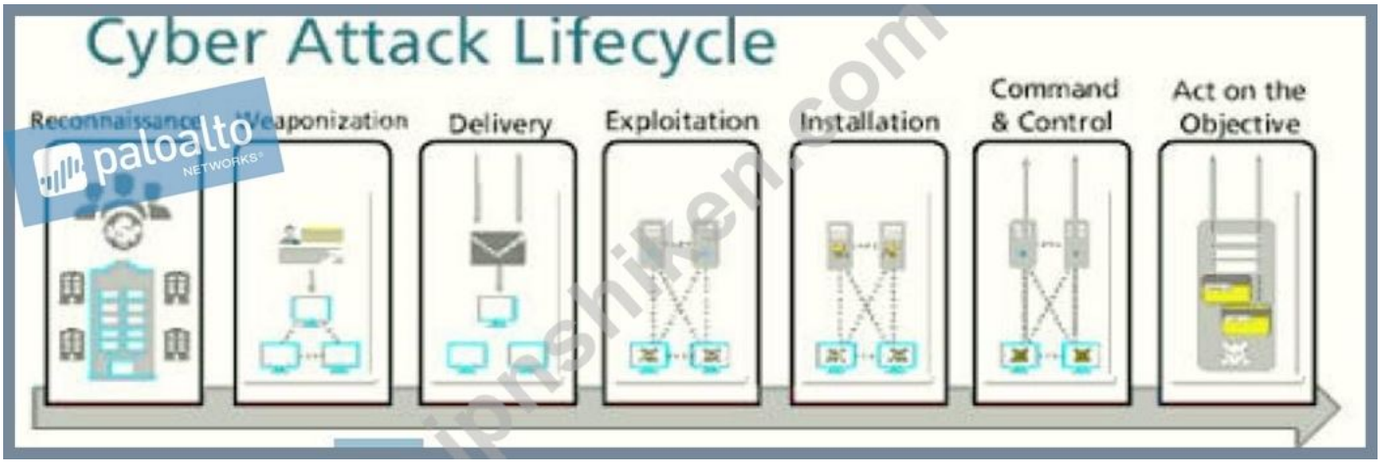
D. default-no-captive-portal
正解: **(**正解を表示します**)**

質問: **72**
パノラマで生成されたログを外部のセキュリティ情報およびイベント管理（SIEM）システムに転送できるパノラマ機能はどれですか？
A. パノラマログの設定
B. パノラマログテンプレート
C. パノラマデバイスグループのログ転送
D. コレクタグループのコレクタログ転送
正解: **(**正解を表示します**)**
Explanation
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/e

質問: **73**
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. GlobalProtectバージョン4.1とPAN-OS 8.0
B. GlobalProtectバージョン4.1（PAN-OS 8.1を使用）
C. PAN-OS 8.1を使用したGlobalProtectバージョン4.0
D. GlobalProtectバージョン4.0とPAN-OS 8.0
正解: **(**正解を表示します**)**

質問: **74**
ネットワークセキュリティエンジニアは、外部サーバが内部Webサーバにアクセスできるようにする必要があります内部のウェブサーバーは外部のサーバーとの関係も開始しなければならないNATポリシーを単純化するために何ができるのですか？
A. 一致するNATトラフィックを処理するようにECMPを設定する
B. 動的IPとポートを持つNATポリシールールを設定する
C. 既存のトラフィックと一致する新しいソースNATポリシールールを作成し、双方向オプションを有効にする
D. 既存のトラフィックと一致する新しい宛先NATポリシールールを作成し、双方向オプションを有効にする
正解: **(**正解を表示します**)**
Explanation
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples

質問: **75**



サイバー攻撃のライフサイクルのどの段階で、攻撃者は感染したPDFファイルを電子メールに添付しますか？

A. 配達

B. IPコマンドアンドコントロール

C. 偵察

D. 搾取

正解: **(**正解を表示します**)**

質問: **76**

ロギングインフラストラクチャでは、毎秒10,000以上のログを処理する必要があります。

専用ログ収集機能をサポートする2つのオプションはどれですか？ （2つ選択）

A. ESX上のパノラマ仮想アプライアンス のみ

B. M-500

C. パノラマがインストールされたM-100

D. M-100

正解: **(**正解を表示します**)**

Explanation

(https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181)

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu 375問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **77**

セキュリティプロファイルを設定する場合、どの3つの項目を使用できますか？ 3つ選択してください）
A. Wildfire analysis
B. anti-ransom ware
C. ウイルス対策
D. URLフィルタリング
E. 復号化プロファイル
正解: **A,C,D (**コメントを発表する**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles

質問: **78**
en A Pファイアウォールクラスターが IPsecトンネルセキュリティアソシエーション $A）を同期するとどうなりますか？
A. フェーズ1SAはHA1リンクを介して同期されます
B. フェーズ2SAはHA2フィンクを介して同期されます
C. フェーズ1およびフェーズ2のSAはHA3リンクを介して同期されます
D. フェーズ1およびフェーズ2のSAはHA2リンクを介して同期されます
正解: **(**正解を表示します**)**

質問: **79**
付属書類を参照してください。

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NGFWがあります。ネットワークチームは、企業のWAN上で過剰なトラフィックを報告しています。
パロアルトネットワークNGFW管理者は、既存のすべての監視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したか？
A. ファイアウォールからのログをPanoramaにのみ転送し、Panorama転送ログを他の外部サービスに転送します。

B. 外部ソースからのログを相関のためにPanoramaに転送し、Panoramaからそれらを 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と最適化機能を設定します。
D. M-500上の任意の構成は、不十分な帯域幅の問題に対処します。
正解: **(**正解を表示します**)**
Explanation
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and-
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClKFCA0
"When this has to be done over a WAN link with bandwidth limitation, it is necessary to consider reducing the number of log streams that are sent over the link" "With this configuration, firewalls will forward logs to Panorama, assuming that log forwarding was configured correctly on the firewall. The logs are forwarded to the syslog server, thus reducing the number of log streams significantly."

質問: **80**
パノラマはどの2つのSD_WAN機能を提供しますか？ 2つ選択してください。）
A. 物理ネットワークリンク
B. データプレーン
C. ネットワーク監視
D. コントロールプレーン
正解: **C,D (**コメントを発表する**)**

質問: **81**
エンジンはDecryptionBroker機能を構成する必要がありますエンジニアは、DecryptionBrokerセキュリティチェーンで使用される復号化転送インターフェイスをどのルーターに割り当てる必要がありますか？
A. データプレーントラフィックを渡すための追加のインターフェイスがなく、セキュリティチェーンで使用されているもの以外の構成済みルートがない仮想ルーター
B. DecryptionBrokerセキュリティチェーンが検査するトラフィックをルーティングする仮想ルーター
C. 少なくとも1つの動的ルーティングプロトコルで構成され、RIBに少なくとも1つのエントリがある仮想ルーター
D. デフォルトの仮想ルーター デフォルトの仮想ルーターがない場合、エンジニアはセットアップ中に作成する必要があります）
正解: **(**正解を表示します**)**

質問: **82**
顧客は、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する必要があります。

どの2つのフォーマットが集合インタフェースの命名に適していますか？ 2つを選択してください）
A. aggregate.8
B. ae.8
C. aggregate.1
D. ae.1
正解: (正解を表示します)

質問: **83**
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場合、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のNGFWは、レイヤ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は、トラフィックログに書き込まれます。
D. App-ID処理時間が増加します。
正解: (正解を表示します)
Reference:
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#

質問: **84**
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
正解: (正解を表示します)
Explanation
We know that SSL decryption is supposed to give us visibility of traffic that would otherwise be encrypted.
Therefore, we'd expect decrypted traffic to be identified as the underlying applications, such as web-browsing, facebook-base or other, but not as SSL.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS

質問: **85**

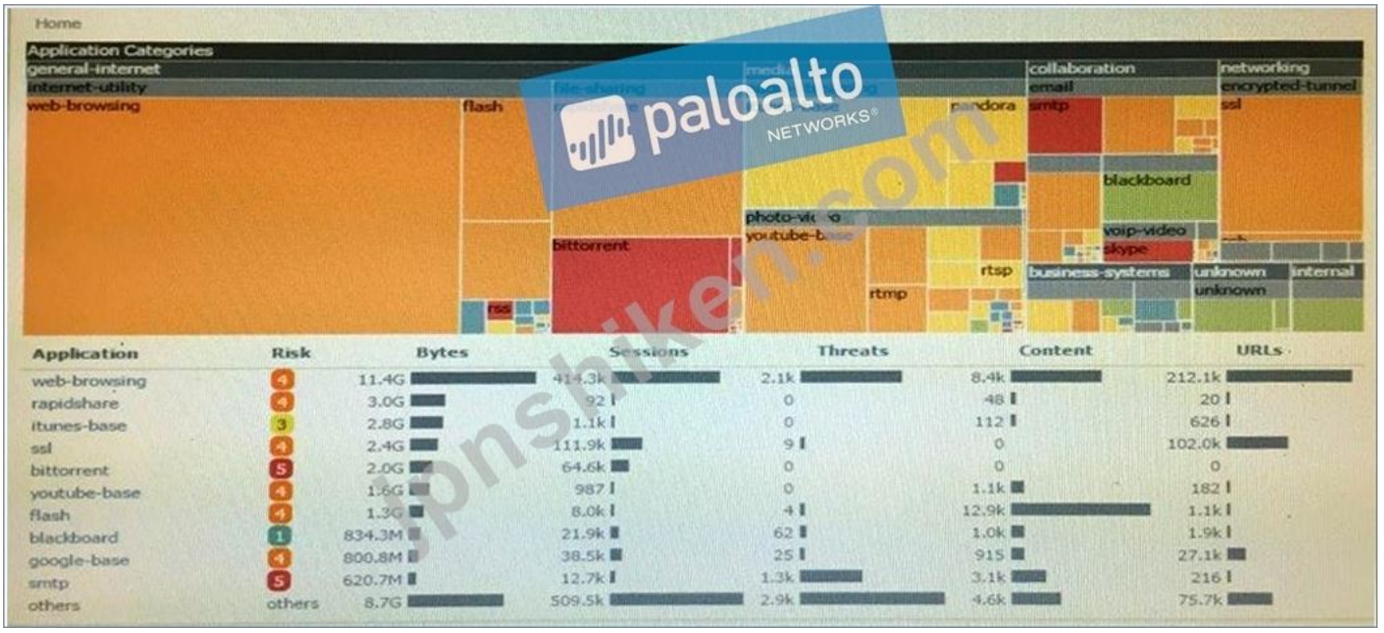
クライアントはデータセンターに機密性の高いアプリケーションサーバーを持っており、特にDoS（サービス拒否）攻撃のためセッションのフラッディングが懸念されます。
パロアルトネットワークNGFWは、単一のIPアドレスから発信されたセッションフラッドに対してこのサーバーを特別に保護するように、どのように構成できますか？
A. 攻撃者のIPアドレスをブロックするアンチスパイウェアプロファイルを追加する
B. 着信要求を抑制するQoSプロファイルを追加する
C. 正当なアプリケーショントラフィックだけがサーバに到達するようにカスタムApp-IDを定義する
D. 調整されたDoSプロテクションプロファイルを追加する
正解: **(**正解を表示します**)**

質問: **86**
基本的なWildFireサービスの一部としてサポートされているファイルタイプのアップロードは何ですか？
A. BAT
B. VBS
C. PE
D. ELF
正解: **(**正解を表示します**)**

質問: **87**
SAML SLOは、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つ選んでください。）
A. GlobalProtect Portal
B. CLI
C. CaptivePortal
D. WebUI
正解: **(**正解を表示します**)**

質問: **88**
特定のデバイスグループへの管理アクセスを制限するPanoramaオブジェクトはどれですか？
A. アクセスドメイン
B. 管理者の役割
C. テンプレート
D. 認証プロファイル
正解: **(**正解を表示します**)**

質問: **89**
展示品ボタンをクリックしなさい



管理者は、ビットトレント活動が大幅に増加していることに気づいています。管理者は、トラフィックが企業でどこで行われている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すか？
A. ビットトレントトラフィック用のグローバルフィルタを作成し、トラフィックログを表示します。
B. ビットトレントトラフィックのローカルフィルタを作成し、トラフィックログを表示します。
C. ビットトレントアプリケーションリンクをクリックして、ネットワークアクティビティを表示します。
D. ビットトレントリンクを右クリックし、コンテキストメニューから 値」を選択します。
正解: (正解を表示します)

質問: **90**
管理者は、新しいPalo Alto Networks NGFWがアプリケーションの自動更新を毎日取得することを望んでいるため、アプリケーションデータベースのスケジューラーを使用するように構成されています。残念ながら、インターネットに到達できないように管理ネットワークを分離する必要がありました。ファイアウォールがアプリケーションの更新を自動的にダウンロードしてインストールできるようにする構成はどれですか？
A. 更新サーバーのIPアドレスのポリシーベースの転送ポリシールールを構成して、更新サーバー宛ての管理インターフェイスから送信されたトラフィックが、インターネット接続として機能するインターフェイスから出て行くようにします。
B. 更新サーバーとの間のすべてのトラフィック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. MGTポートがインターネットに到達できない場合、アプリケーションの更新のダウンロードとインストールを自動的に実行することはできません。
D. トラフィックをインターネットにルーティングできるデータプレーンインターフェイスを使用するパロアルトネットワークサービスのサービスルートを構成し、必要に応じてそのインター

フェイスから更新サーバーへのトラフィックを許可するセキュリティポリシールールを作成します。

正解: (正解を表示します)

Explanation

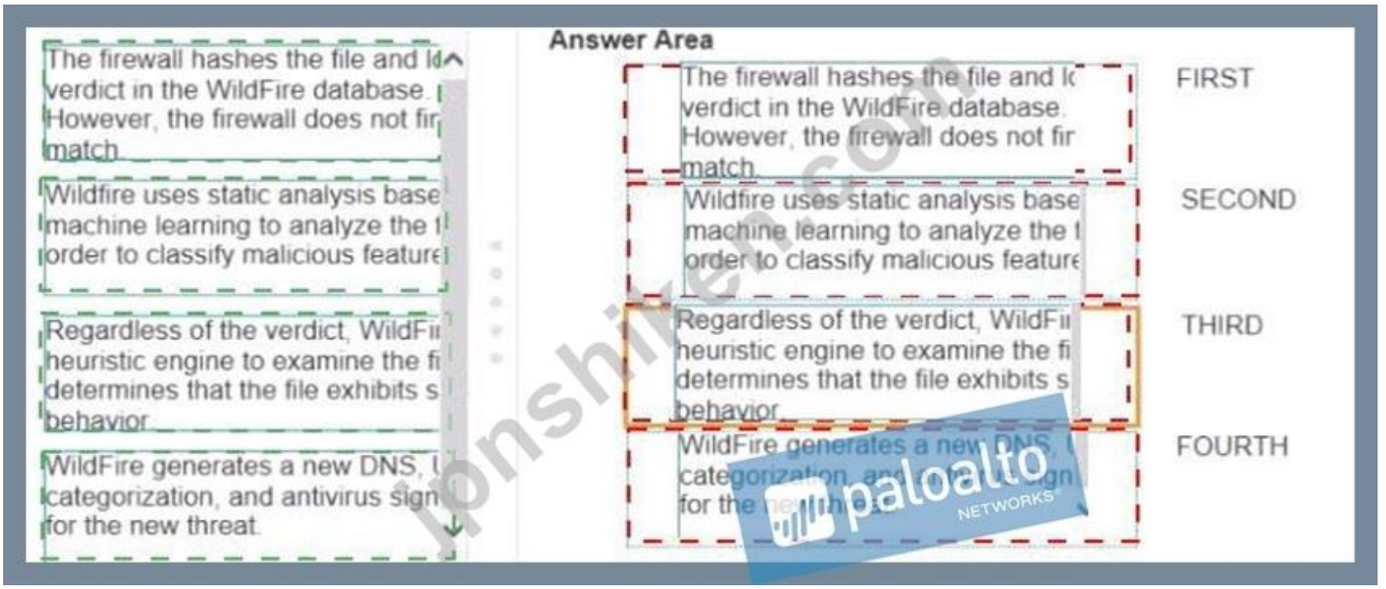
"By default, the firewall uses management interface to communicate to various servers including DNS, Email, Palo Alto Updates, User-ID agent, Syslog, Panorama etc. Service routes are used so that the communication between the firewall and servers go through the dataplane."https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGJCA0

"The firewall uses the service route to connect to the Update Server and checks for new content release versions and, if there are updates available, displays them at the top of the list."https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/device/device-dynamic-updates#

質問: **91**

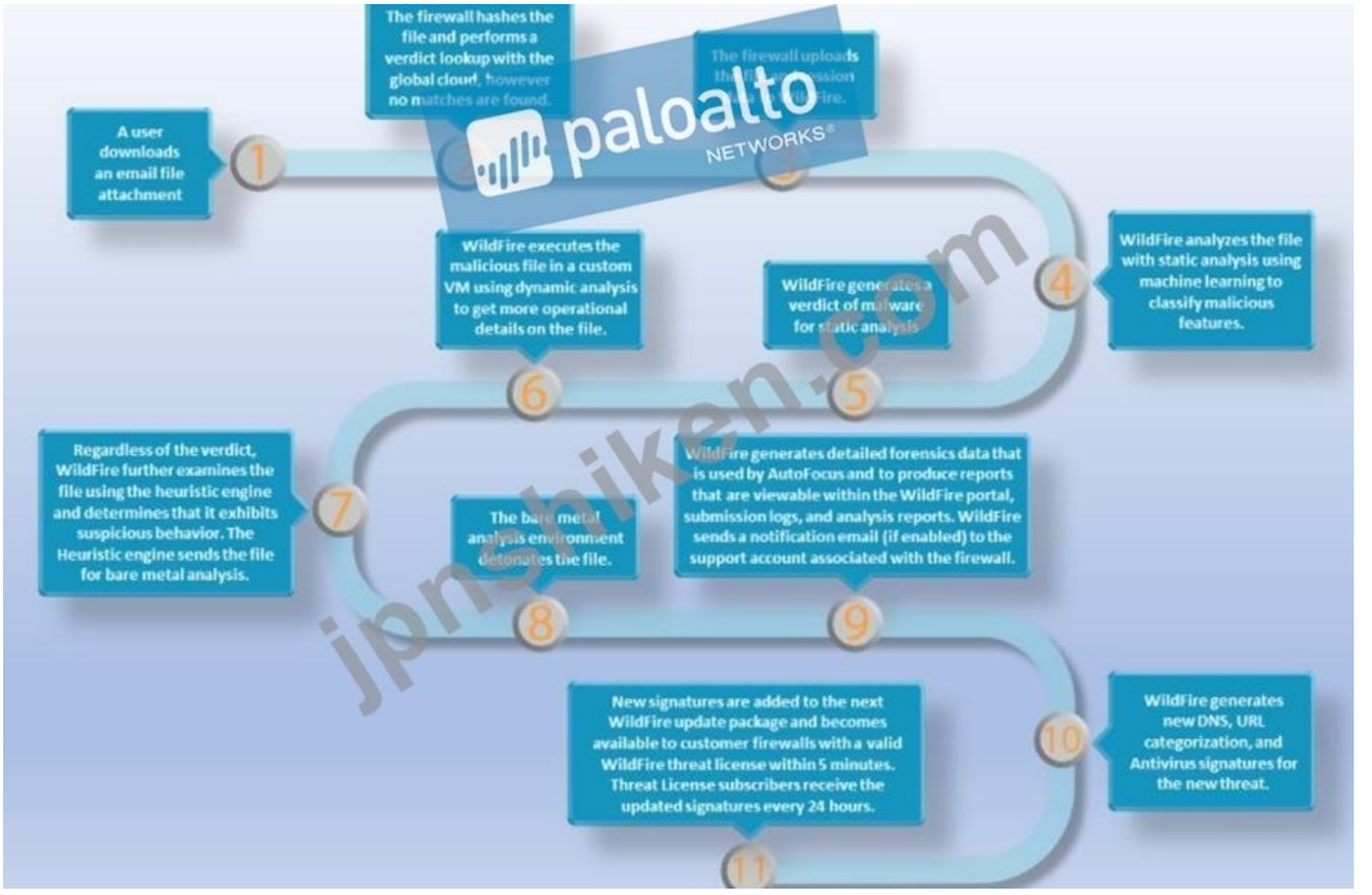
WildFireプロセスワークフローのステップを正しい順序で配置します。

正解:



Explanation

Timeline Description automatically generated



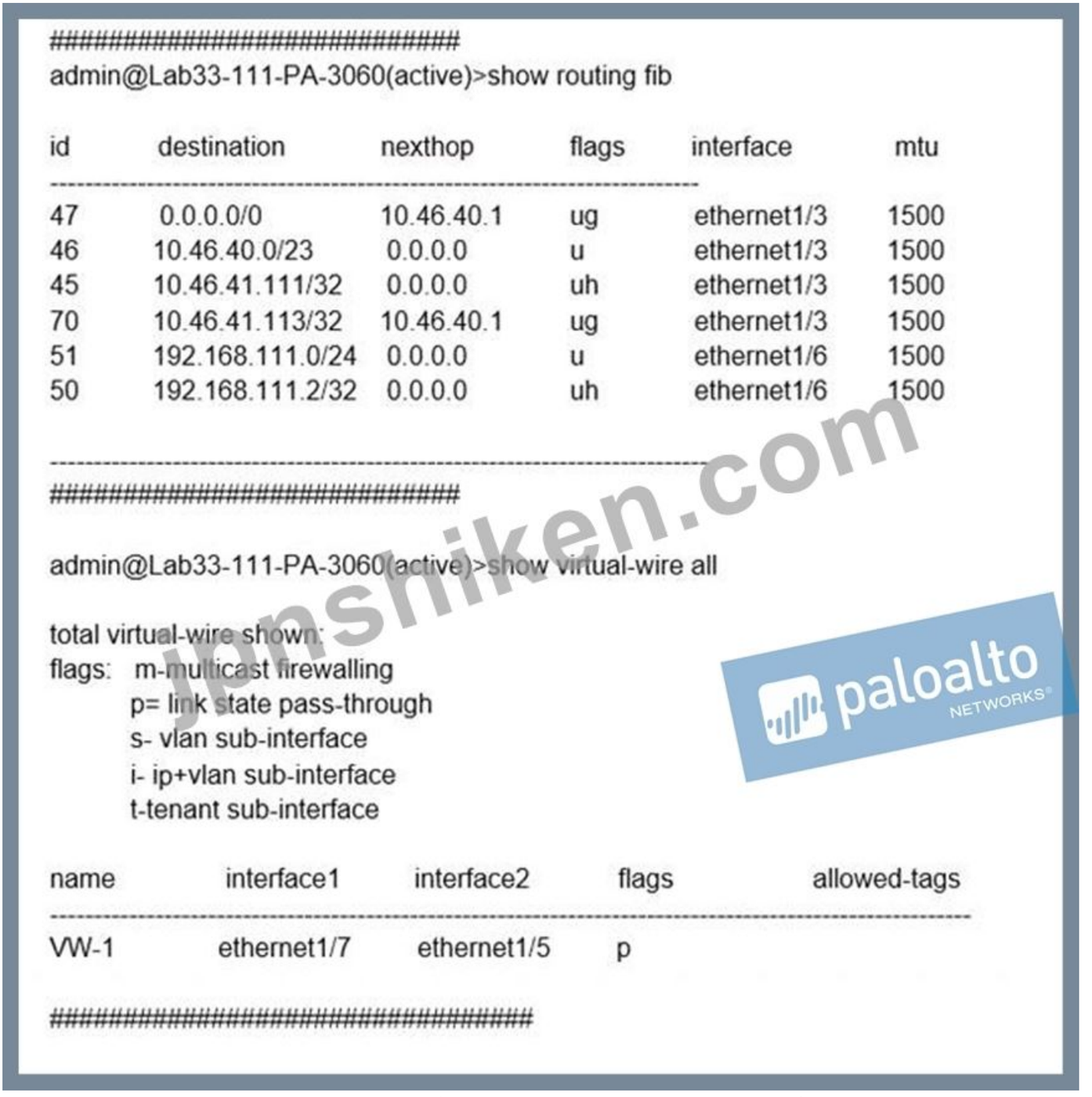
https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/about-wildfire.html

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu **875**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **92**
エンタープライズ情報セキュリティチームは、ADグループに基づいてポリシーを展開し、重要なインフラストラクチャシステムへのユーザーアクセスを制限しています。ただし、組織に対する最近の認証キャンペーンにより、情報セキュリティは、アクセスする必要のあるユーザーのために、重要な資産へのアクセスを保護できるより多くの制御を探すようになりました。これらのシステム情報セキュリティは、PAN-OS多要素認証（MFA）統合を使用してMFAを実施したいと考えています。
PAN-OS MFA1を使用するには、企業は何をすべきですか？
A. 認証シーケンスを使用するキャプティブポータル認証ポリシーを構成します
B. 認証プロファイルを作成し、キャプティブポータル認証ポリシーで使用される別の認証要素を割り当てます

C. RADIUSプロファイルを参照する認証プロファイルを使用するCaptivePorta1認証ポリシーを構成します
D. クレデンシャルフィッシングエージェントを使用して、クレデンシャルフィッシングキャンペーンの防止と軽減を検出します
正解: **(**正解を表示します**)**

質問: **93**
Exhibit:



jpnshiken.com

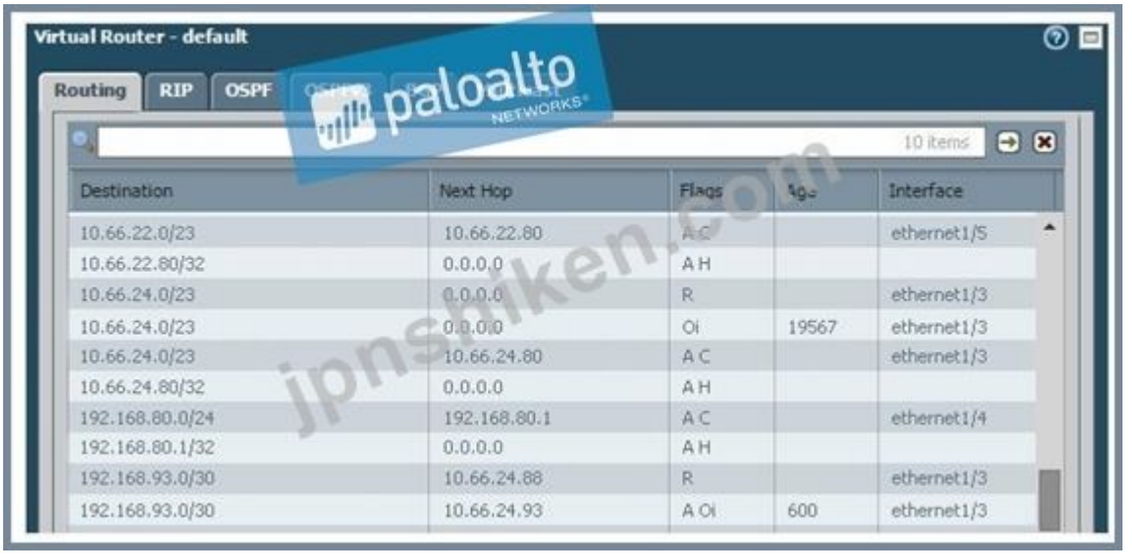
トラフィックの入力インターフェイスがethernet1 / 6からのものであれば、出力インターフェイスは何になりますか
また、192.168.111.3と、目的地の10.46.41.113に表示されていますか？

A. ethernet1/3
B. ethernet1/7
C. ethernet1/5
D. ethernet1/6
正解: **A (**コメントを発表する**)**

質問: **94**
管理者は、レイヤ7シグネチャを含むカスタムアプリケーションを作成します。最新のアプリケーションと脅威の動的更新が同じNGFWにダウンロードされます。この更新プログラムには、カスタムアプリケーションと同じトラフィックシグネチャに一致するアプリケーションが含まれています。
NGFWを通過するトラフィックを識別するためにどのアプリケーションを使用すべきですか？
A. カスタムアプリケーション
B. システムログにはアプリケーションエラーが表示され、いずれのシグネチャも使用されません。
C. カスタムおよびダウンロードされたアプリケーションシグネチャファイルがマージされ、両方が使用されます
D. ダウンロードしたアプリケーション
正解: **(**正解を表示します**)**

質問: **95**
どのPanorama管理者タイプで少なくとも1つのアクセスドメインの設定が必要か
（2つ選択）
A. Role Based
B. Device Group
C. Dynamic
D. Template Admin
E. Custom Panorama Admin
正解: **(**正解を表示します**)**

質問: **96**
以下のテーブルが与えられる。



ファイアウォールのどの設定変更により、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が使用されるのでしょうか？

A. RIPのメトリックをOSPF Extよりも低く設定する。

B. RIPの管理距離をOSPF Intの管理距離よりも小さく設定する。

C. RIPの管理距離をOSPF Extの管理距離よりも大きく設定する。

D. RIPのメトリックをOSPF Intのメトリックよりも高く設定する

正解: **(**正解を表示します**)**

質問: **97**

パノラマのTemplatesオブジェクト内で定義される3つの設定はどれですか？ （3つ選択してください）

A. Application Override

B. Setup

C. Interfaces

D. Virtual Routers

E. Security

正解: **(**正解を表示します**)**

質問: **98**

過去30日間に検出された脅威のような、一定期間にわたるトラフィックの傾向を管理者が確認できるのはどのツールですか？

A. Session Browser

B. Application Command Center

C. TCP Dump

D. Packet Capture

正解: **B (**コメントを発表する**)**

Reference:

https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Comm ACC/ta-p/67342

質問: **99**
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
正解: **(正解を表示します)**
Reference:
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/deploy-user-id-in-a-large-scale-netw

質問: **100**
管理者がファイアウォールのHAペアをPAN-OS10.1にアップグレードしたいと考えています。
ファイアウォールは現在PAN-OS8.1.17を実行しています。
HAセッションの同期を維持する そしてネットワークの停止を防ぐ）アップグレードパスはどれですか？
A. HAペアをベースイメージにアップグレードします
B. 一度に1つのメジャーバージョンをアップグレードします
C. 一度に2つのメジャーバージョンをアップグレードします
D. ターゲットのメジャーバージョンに直接アップグレードします
正解: **(正解を表示します)**

質問: **101**
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上の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、TCPポート8080のIPアドレスとレポートの両方を10.1.1.100に変換するように設定されています。

どのNATとセキュリティルールをファイアウォールで設定する必要がありますか？ (2つ選択)

A. Webブラウジングアプリケーションを使用して、dmz-l3ゾーン内のunstruct-l3 Zoneから10.1.1.100の宛先まで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、ソースがuntrust-l3ゾーンからdmz-zoneの宛先10.1.1.100までのNATルール。

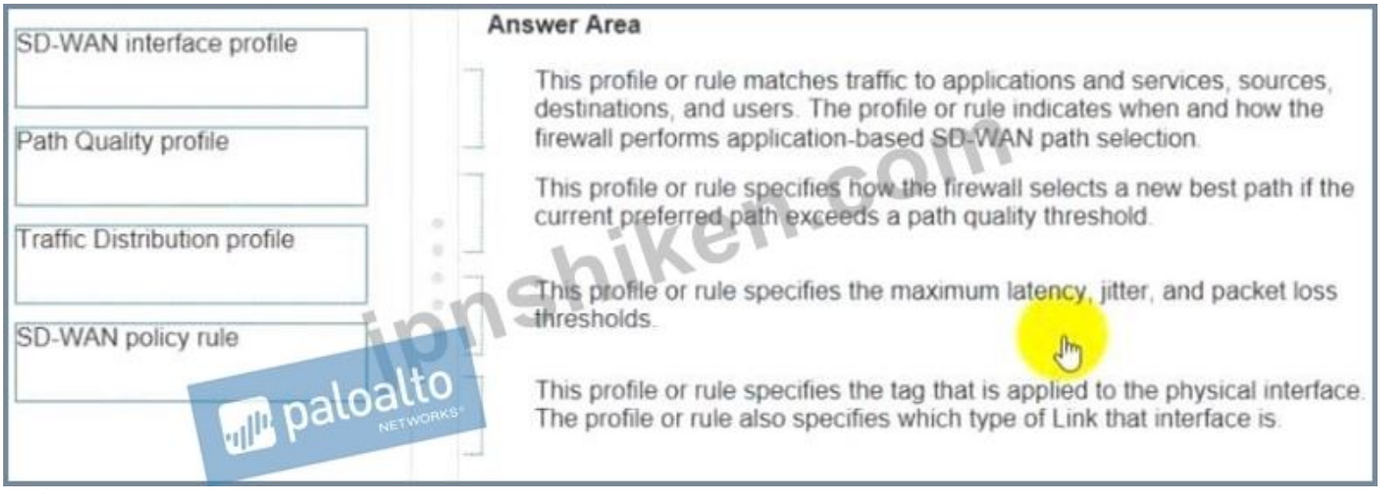
C. Webブラウジングアプリケーションを使用して、dmz-l3ゾーンの信頼できないl3ゾーンから1.1.100の宛先までのソースを持つセキュリティポリシー。

D. untrust-l3ゾーンからservice-httpサービスを使用して1.1.1.100の宛先までのいずれかのソースを持つNATルール。

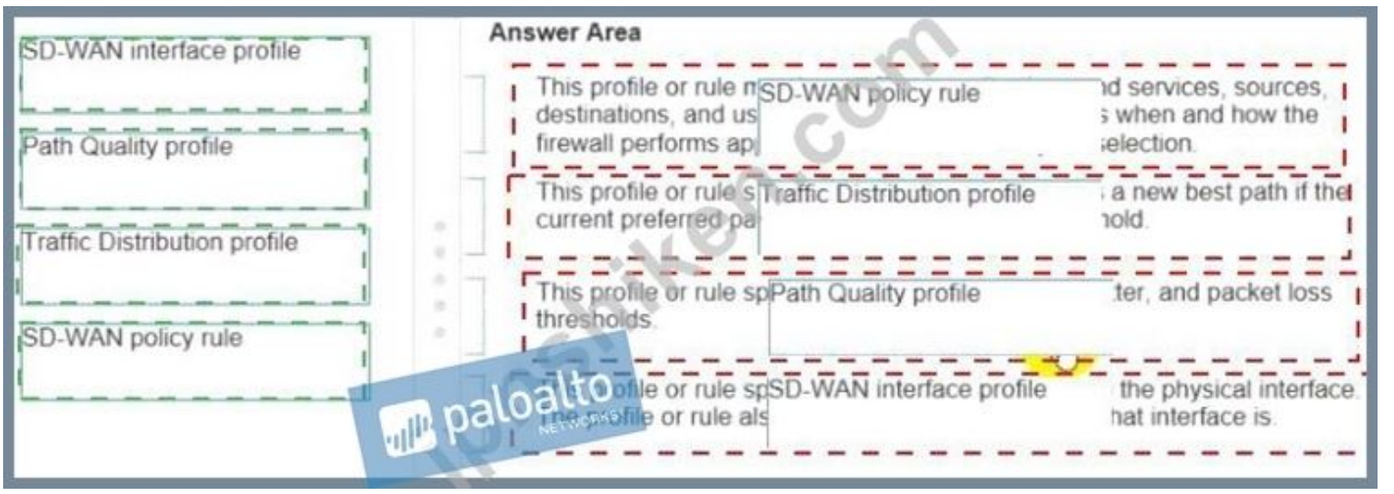
正解: **(**正解を表示します**)**

質問: **102**

各SD-WAN構成要素をその要素の説明と一致させます。



正解:



Explanation

* An

SD-WAN Interface Profile

specifies the Tag that you apply to the physical interface, and also specifies the type of Link that interface is (ADSL/DSL, cable modem, Ethernet, fiber, LTE/3G/4G/5G, MPLS, microwave/radio, satellite, WiFi, or other). The Interface Profile is also where you specify the maximum upload and download speeds (in Mbps) of the ISP's connection. You can also change whether the firewall monitors the path frequently or not; the firewall monitors link types appropriately by default.

* A Layer3 Ethernet

Interface

with an IPv4 address can support SD-WAN functionalities. You apply an SD-WAN Interface Profile to this interface (red arrow) to indicate the characteristics of the interface. The blue arrow indicates that physical Interfaces are referenced and grouped in a virtual SD-WAN Interface.

* A virtual

SD-WAN Interface

is a VPN tunnel or DIA group of one or more interfaces that constitute a numbered, virtual SD-WAN Interface to which you can route traffic. The paths belonging to an SD-WAN Interface all go to the same destination WAN and are all the same type (either DIA or VPN tunnel). (Tag A and Tag B indicate that physical interfaces for the virtual interface can have different tags.)

* A

Path Quality Profile

specifies maximum latency, jitter, and packet loss thresholds. Exceeding a threshold indicates that the path has deteriorated and the firewall needs to select a new path to the target. A sensitivity setting of high, medium, or low lets you indicate to the firewall which path monitoring parameter is more important for the applications to which the profile applies. The green arrow indicates that you reference a Path Quality Profile in one or more SD-WAN Policy Rules; thus, you can specify different thresholds for rules applied to packets having different applications, services, sources, destinations, zones, and users.

* A

Traffic Distribution Profile

specifies how the firewall determines a new best path if the current preferred path exceeds a path quality threshold. You specify which Tags the distribution method uses to narrow its selection of a new path; hence, the yellow arrow points from Tags to the Traffic Distribution profile. A Traffic Distribution profile specifies the distribution method for the rule.
* The preceding elements come together in
SD-WAN Policy Rules
The purple arrow indicates that you reference a Path Qualify Profile and a Traffic Distribution profile in a rule, along with packet applications/services, sources, destinations, and users to specifically indicate when and how the firewall performs application-based SD-WAN path selection for a packet not belonging to a session.
https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/sd-wan-configuration-elements.h

質問: **103**
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. トラフィックログエントリの詳細
B. 復号化ログ
C. データフィルタリングログ
D. 脅威ログエントリの詳細
正解: **(**正解を表示します**)**
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-Decryption/ta-p/5

質問: **104**
ethernet1 / 3に接続されたホストはインターネットにアクセスできません。デフォルトのゲートウェイはethernet1 / 4に接続されています。トラブルシューティング後。トラフィックがethernet1 / 3からethernet 1/4に通過できないと判断されます。問題の原因は何か？
A. インタフェースethernet1 / 3とethernet1 / 4は仮想ワイヤモードになっています。
B. インターフェイスethernet1 / 3はレイヤ2モードで、インターフェイスethernet1 / 4はレイヤ3モードです。
C. DHCPが自動に設定されています。
D. DNSがファイアウォールで正しく構成されていない
正解: **(**正解を表示します**)**

質問: **105**

ネットワークセキュリティエンジニアは、帯域幅使用量に関するレポートを提出するよう求められます。ACCのどのタブにレポートの作成に必要な情報がありますか？
A. ネットワーク活動
B. 脅威活動
C. 帯域幅アクティビティ
D. ブロックされた活動
正解: **A** (コメントを発表する)

質問: **106**
管理プレーンのパフォーマンスに影響を与える操作はどれですか？
A. DoS保護
B. SSLセッションの復号化
C. WildFireの提出
D. SaaSアプリケーションレポートの生成
正解: (正解を表示します)

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu 875問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

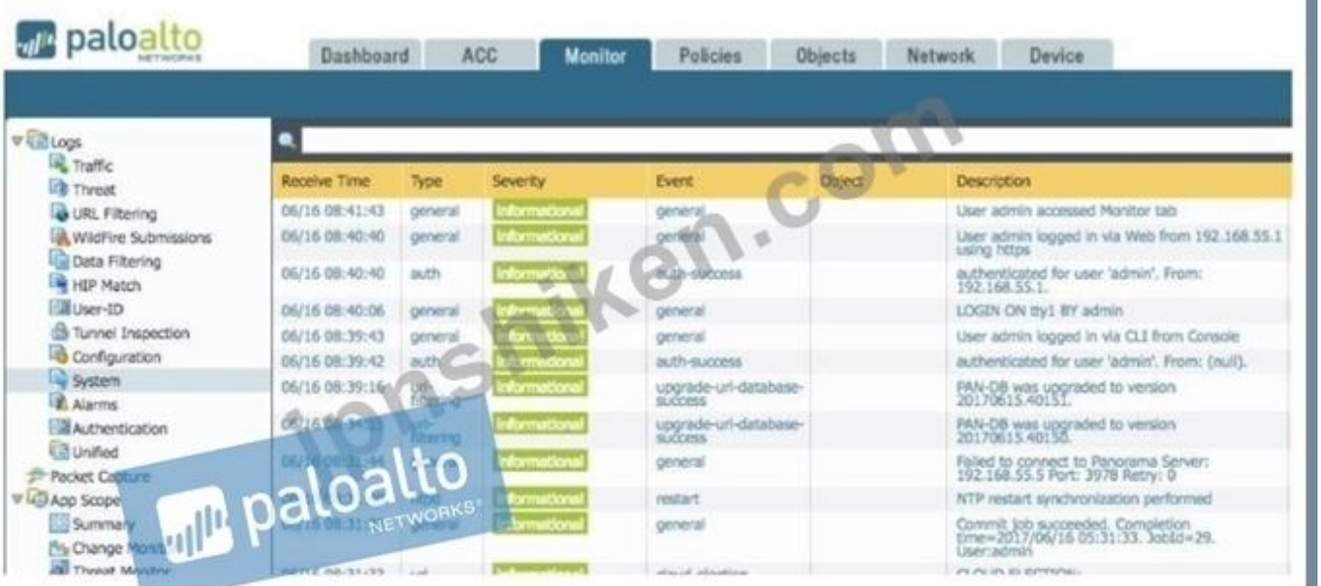
質問: **107**
ある会社が、VLANトランクリンク上の2つのコアスイッチの間にPA-3060ファイアウォールを設置したいと考えています。各VLANを独自のゾーンに割り当て、タグなし（ネイティブ）トラフィックを独自のゾーンに割り当てる必要があります。複数のVLANを個別のゾーンに区別するオプションはどれですか。
A. 2つのV-Wireインターフェイスを使用してV-Wireオブジェクトを作成し、V-Wireオブジェクトの[TagAllowed]フィールドに「0-4096」の範囲を定義します。
B. 2つのV-Wireサブインターフェイスを使用してV-Wireオブジェクトを作成し、V-Wireオブジェクトの「TagAllowed」フィールドに1つのVLAN ID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。。各インターフェイス/サブインターフェイ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。
物理層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tAを割り当てます。
ユニークゾーン。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. VLANごとにVLANオブジェクトを作成し、各VLANIDに一致するVLANインターフェースを割り当てます。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。
正解: **(**正解を表示します**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa Virtual wire interfaces by default allow all untagged traffic. You can, however, use a virtual wire to connect two interfaces and configure either interface to block or allow traffic based on the virtual LAN (VLAN) tags.
VLAN tag 0 indicates untagged traffic.You can also create multiple subinterfaces, add them into different zones, and then classify traffic according to a VLAN tag or a combination of a VLAN tag with IP classifiers (address, range, or subnet) to apply granular policy control for specific VLAN tags or for VLAN tags from a specific source IP address, range, or subnet.

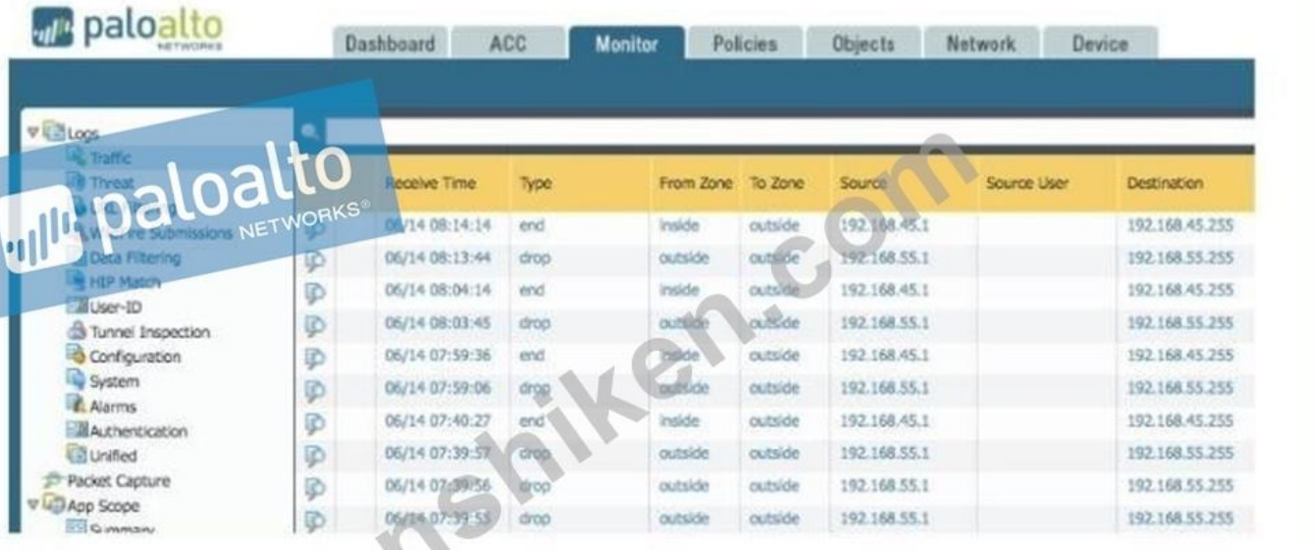
質問: **108**
管理者は、パロアルトネットワークNGFW上の仮想ルータ上でBGPを有効にしましたが、新しいルートは仮想ルータに投入されていないようです。管理者がこの問題のトラブルシューティングに役立つ2つのオプションはどれですか？ （2つを選択してください）
A. システムログを表示し、BGPに関するエラーメッセージを探します。
B. NGFW上のトラフィックpcapを実行して、BGPの問題を確認します。
C. 実行時の統計情報を表示し、BGP設定の問題を探します。
D. [ACC]タブを表示してルーティングの問題を特定します。
正解: **(**正解を表示します**)**
Explanation
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEWCA0

質問: **109**
コミットが終了する前に、管理者が誤ってコミットウィンドウ/画面を閉じました。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管理者が使用できる2つのオプションはどれですか。 （2つ選んでください。）

A



B



C

jpnshiken.com

D

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D
正解: **(**正解を表示します**)**

質問: **110**
既存のNGFWのお客様には、直接インターンが必要です。各サイトでローカルにオフロードにアクセスし、パブリックインターネットを介してすべてのブランチにiPSec接続します。1つの要件は、新しいSD-WANハードウェアを環境に導入しないことです。
お客様にとって最善の解決策は何ですか？
A. ポリシーベースの転送を構成します
B. PrismaAccessを使用してPrismaSD-WANを展開する
C. PAN-OSSD-WANサブスクリプションにアップグレードします
D. PAN-OSでリモートネットワークを構成します
正解: **C (**コメントを発表する**)**

質問: **111**
トラフィックログには、アプリケーションが 該当なし」と表示される場合があります。その理由は2つあります。 2つ選択してください）
A. ファイアウォールがTCPSYNパケットをドロップしました
B. 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でした
C. ファイアウォールがセッションをインストールしませんでした
D. アプリケーションデータを識別せずにTCP接続が終了しました
正解: **(**正解を表示します**)**

質問: **112**

管理者はCitrix XenApp 7 xを介してネットワークリソースにアクセスするユーザーを持っています。Citrixを使用してネットワークに接続してリソースにアクセスする複数のユーザーをマッピングするユーザーIDマッピングソリューションはどれですか？
A. グローバルプロテクト
B. Syslog監視
C. ターミナルサービスエージェント
D. クライアント探索
正解: **(**正解を表示します**)**

質問: **113**
現在SSL復号化処理を行っているセッションの総数を確認するために使用するコマンドは次のうちどれですか？
A. show session all filter ssl-decryption yes total-count yes
B. show session all filter ssl-decrypt yes count yes
C. show session filter ssl-decryption yes total-count yes
D. show session all ssl-decrypt yes count yes
正解: **(**正解を表示します**)**

質問: **114**
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
正解: **(**正解を表示します**)**
Explanation
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up

質問: **115**
ファイアウォール管理者がNGFWを通じて現在アクティブなトラフィックの詳細を表示できる項目はどれですか?
A. Session Browser
B. System Logs
C. App Scope
D. ACC
正解: **(**正解を表示します**)**

質問: **116**
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敏感であると識別されてい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ります述べています。company.comがパロアルトネットワークデバイス上のこのトラフィックに直ちに対処するために使用する方法はどれですか？
A. 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する
B. 社内アプリケーショントラフィックの唯一の識別子に一致するシグネチャでカスタムアプリケーションを作成する
C. Palo Alto Networks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。
D. シグネチャなしでカスタムアプリケーションを作成し、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。
正解: **B (**コメントを発表する**)**

質問: **117**
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
正解: **(**正解を表示します**)**
Explanation
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.htm

質問: **118**
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. 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。
B. 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。
C. 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

D. / 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。
E. 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
正解: **A,B** (コメントを発表する)

質問: **119**
キャプティブポータルポリシーを検証するために使用できるコマンドはどれですか？
A. request cp-policy-eval <criteria>
B. debug cp-policy <criteria>
C. test cp-policy-match <criteria>
D. eval captive-portal policy <criteria>
正解: **C** (コメントを発表する)

質問: **120**
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で始まるIPアドレス範囲に設定します。
B. 内部クライアントをIPアドレス192.168.10.1の内部ゲートウェイに強制的に接続します。
C. クライアントは、内部クライアントであることを検出するために192.168.10.1に対して逆DNSルックアップを実行できます。
D. ファイアウォールは動的DNS更新を実行し、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。
正解: (正解を表示します)
Reference:
https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-por the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations
"Select this option to allow the GlobalProtect agent to determine if it is inside the enterprise network. This option applies only to endpoints that are configured to communicate with internal gateways.When the user attempts to log in, the agent does a reverse DNS lookup of an internal host using the specified Hostname to the specified IP Address. The host serves as a reference point that is reachable if the endpoint is inside the enterprise network. If the agent finds the host, the endpoint is inside the network and the agent connects to an internal gateway; if the agent fails

to find the internal host, the endpoint is outside the network and the agent establishes a tunnel to one of the external gateways"

質問: **121**
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. 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
B. 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
C. ファイアウォールをアップグレードします。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
正解: **B** (コメントを発表する)

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu
875問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **122**
顧客は、カスタムPostgreSQLデータベース接続の1つで不明トップとして識別されているアプリケーションを持っています。カスタムデータベースアプリケーションを正しく分類するために使用できる2つの構成オプションはどれですか？ 2つ選択してください。）
A. アプリケーションオーバーライドポリシー。
B. 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。
C. カスタムアプリケーション。
D. カスタムサービスオブジェクト。
正解: **A,C** (コメントを発表する)
Explanation
Unlike the App-ID engine, which inspects application packet contents for unique signature elements, the Application Override policy's matching conditions are limited to header-based data only. Traffic matched by an Application Override policy is identified by the App-ID entered in the Application entry box.Choices are limited to applications currently in the App-ID database.Because this traffic bypasses all Layer 7 inspection, the resulting security is that of a Layer-4 firewall. Thus, this traffic should be trusted without the need for Content-ID inspection. The resulting application assignment can be used in other firewall functions such as Security policy and QoS.Use CasesThree primary uses cases for Application Override Policy are:

To identify "Unknown" App-IDs with a different or custom application signature To re-identify an existing application signature To bypass the Signature Match Engine (within the SP3 architecture) to improve processing timesA discussion of typical uses of application override and specific implementation examples is here:https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application- Ov

質問: **123**
ファイアウォールは、一般的な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の2つのオプションはどれですか？ （2つを選択してください）
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を識別するカスタムアプリケーションサーバー用のカスタムオブジェクトを作成します。
C. Apple-IDリクエストをPalo Alto Networksに提出してください。
D. セキュリティポリシーを作成して、カスタムアプリケーションを識別します。
正解: **(**正解を表示します**)**
Explanation
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/manage-custom-or-unknown-applica

質問: **124**
管理者は、Palo Alto NetworksのNGFWの管理インターフェイスを、NGFW自体を経由しないで専用のパスを介してインターネットに接続するように設定しました。
ファイアウォールが自動的にアプリケーションシグネチャの更新を取得するための設定またはステップはどれですか？
A. アプリケーションシグネチャ用にスケジューラを構成する必要があります。
B. ファイアウォールから更新サーバーへの更新要求を許可するセキュリティポリシールールを構成する必要があります。
C. 脅威防止ライセンスをインストールする必要があります。
D. サービスルートを設定する必要があります。
正解: **A (**コメントを発表する**)**
Reference:
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

質問: **125**
自動コミットリカバリ機能の操作を説明するオプションはどれですか？
A. ルールのシャドウイングが検出された場合、ファイアウォールを以前の構成に戻すことができます
B. アプリケーションの依存関係エラーが見つかった場合、ファイアウォールを以前の構成に戻すことができます

C. コミットによってPanorama接続障害が発生した場合、ファイアウォールを以前の構成に戻すことができます。
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
正解: **(**正解を表示します**)**

質問: **126**
内部システムが機能していないファイアウォール管理者は、誤った出力インターフェイスが使用されていると判断しました構成を確認した後、管理者はファイアウォールが静的ルートを使用していないと考えていますファイアウォールが静的ルートを使用しない理由は2つあります (2つ選択してください。)
A. 静的ルートが重複しています
B. ルートにインストールされていません
C. 静的ルートの無効化
D. 静的ルートでのパス監視
正解: **(**正解を表示します**)**

質問: **127**
管理者はFacebookのチャットをブロックするが、一般的にFacebookを許可するセキュリティポリシーのルールはどれですか？
A. アプリケーションのFacebookを許可する前にfacebook-chatアプリケーションを拒否する
B. 上にアプリケーションのfacebookを拒否する
C. 上にアプリケーションのfacebookを許可する
D. アプリケーションのfacebook-chatを拒否する前にアプリケーションのfacebookを許可する
正解: **A (**コメントを発表する**)**
Reference:
https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/11

有効的な**PCNSE-JPN**問題集はJPNTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTest.com PCNSE-JPN試験問題集はもう更新されました。ここで**PCNSE-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/PCNSE-JPN-mondaishu **875**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」