

# PaloAltoNetworks.PCNSE-JPN.v2022-09-26.q156

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 : 156  
バージョン : v2022-09-26  
ページの閲覧量 :600  
問題集の閲覧量 :16804  
<https://www.jpnsiken.com/shiken/PaloAltoNetworks.PCNSE-JPN.v2022-09-26.q156.html>

## 質問: 1

パケットキャプチャのためにファイアウォールを設定するとき、有効なステージタイプは何ですか？

- A. Receive, management , transmit , and drop
- B. Receive , firewall, send , and non-syn
- C. Receive management , transmit, and non-syn
- D. Receive , firewall, transmit, and drop

正解: ([正解を表示します](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CITJCA0docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-capture-overview.html>

## 質問: 2

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 \$)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](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIEyCAK>

"...behavior when selecting the Application as web-browsing and the Service to application-default. Web-browsing will be allowed over both its standard and secure port. The security policy will allow web-browsing over both port 80 and 443."

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CmdLCAS>

**質問: 3**

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. delivery
- B. IP command and control
- C. exploitation
- D. reconnaissance

正解: ([正解を表示します](#))

**質問: 4**

MFA認証をサポートするには、どのキャプティブポータルモードを設定する必要がありますか？

- A. Transparent
- B. NTLM
- C. Redirect
- D. Single Sign-On

正解: ([正解を表示します](#))

**質問: 5**

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している。legitimate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. 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
- 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. 最大限度以下のトラフィックを抑制するQoSポリシー

正解: **B** ([コメントを發表する](#))

**質問: 6**

会社は、Active Directoryグループを使用して、Panoramaからのセキュリティポリシーの作成を簡素化したいと考えています。

パノラマからグループを取得するには、どの構成が必要ですか？

- A. LDAPサーバープロファイルを構成し、管理インターフェースでユーザーIDサービスを有効にします。
- B. ターゲットテンプレート内のグループを取得するようにグループマッピングプロファイルを構成します。
- C. ユーザーIDエージェントからIPユーザーマッピングを受信するようにデータ再配布エージェントを構成します。
- D. デバイスグループ内でマスターデバイスを構成します。

正解: ([正解を表示します](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1FQCA0>

質問: 7

エンタープライズPKIを使用する管理者は、Panoramaと管理対象のファイアウォールおよびログコレクタ間の相互認証を保証するために、独自の信頼関係を確立する必要があります。

管理者はどのようにして信頼の連鎖を確立しますか？

- A. カスタム証明書を使用する
- B. 強力なパスワード認証の設定
- C. LDAPまたはRADIUSの統合を有効にする
- D. マルチファクタ認証を設定する

正解: ([正解を表示します](#))

質問: 8

次の画像に基づいて、

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. VeriSign > Palo Alto Networks > Symantec
- C. Palo Alto Networks > Symantec > VeriSign
- D. Symantec > VeriSign > Palo Alto Networks

正解: **A** ([コメントを發表する](#))

質問: 9

SSL Forward Proxy復号化が構成されていますが、ファイアウォールはUntrusted-CAを使用してWebサイトに署名しますhttps

// wwwimportant-website comcertificateエンドユーザーが私を受け取っています "セキュリティ証明書は信頼されていません警告ですSSL復号化がないと、WebブラウザはWebサイト証明書が信頼され、有名な証明書チェーンによって署名されていることを示しますよく知られているルートCA。

顧客を代表するネットワークセキュリティ管理者は、SSL転送プロキシが有効になっている場合、次の2つの動作を必要とします。

1エンドユーザーは、https //www.very-important-website.comWebサイトの警告を受け取らないようにする必要があります。

2エンドユーザーは、他の信頼できないWebサイトに対して警告を受け取る必要があります  
2つの顧客要件を満たすアプローチはどれですか？

- A. [デバイス]> [証明書管理]-[証明書]に移動します。sデフォルトの信頼できる認証局importWell-Known-intermediate-CAおよびWell-Known-Root-CA [Trusted Root CA]チェックボックスをオンにして、構成をコミットします。
- B. [デバイス]> [証明書管理]> [証明書]> [デバイス証明書]に移動し、Well-Known-intermediate-CAおよびWell-Known-Root-CAをインポートします。[信頼されたルートCA]チェックボックスを選択し、構成をコミットします。
- C. ユーザーおよびローカルコンピュータストアのすべてのエンドユーザーシステムに、Well-Known-intermediate-CAおよびWell-Known-Root-CA証明書をインストールします。
- D. Untrusted-CA証明書のForward Untrust Certificateチェックボックスをオフにして、構成をコミットします

正解: ([正解を表示します](#))

#### 質問: 10

どのCLIコマンドを使用して、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、どのセキュリティポリシールール、NAT変換、スタティックルート、またはPBFルールがトラフィックによってトリガーされるかを判断します。

- A. check
- B. find
- C. test
- D. sim

正解: ([正解を表示します](#))

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIQSCA0>

#### 質問: 11

復号化ポリシールール的一致に有効な3つの修飾子は何ですか？ 3つ選択してください)

- A. ユーザーID
- B. カスタムURLカテゴリ
- C. アプリID
- D. 宛先ゾーン
- E. ソースインターフェイス

正解: ([正解を表示します](#))

#### 質問: 12

Cortex XDRは、エンドポイントのグレーウェアについて管理者に通知します。

対応するファイアウォールのログには、グレーウェアに関するエントリはありません。

グレーウェアの判定をログに記録するために、管理者はファイアウォールでどの設定を構成できますか？

- A. Threat GeneralSettings^で[ReportGraywareFiles]を選択します
- B. WildFireの一般設定で、[Graywareファイルのレポート]を選択します
- C. セキュリティポリシールールに添付されたログ転送プロファイル内
- D. [デバイス]タブの[ログ設定]オプション内

正解: ([正解を表示します](#))

#### 質問: 13

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. 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
- 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. ファイアウォール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
- 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

正解: **D** ([コメントを发表する](#))

Locally defined dynamic updates setting on a managed Palo Alto Networks firewall take preference over the Panorama pushed setting.

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKQCA0>

#### 質問: 14

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](#))

([https://www.paloaltonetworks.com/documentation/60/panorama/panorama\\_adminguide/set-up-panorama/set-up-the-m-100-appliance](https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance))

#### 質問: 15

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 i)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](#))

(<https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/tap/72181>)

質問: 16

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. Okta Adaptive

B. プッシュ

C. プル

D. 声

E. SMS

正解: ([正解を表示します](#))

有効的なPCNSE-JPN問題集はJPNTTest.com提供され、PCNSE-JPN試験に合格することに役に立ちます！JPNTTest.comは今最新PCNSE-JPN試験問題集を提供します。JPNTTest.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: 17

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. クライアント探索

B. ターミナルサービスエージェント

C. グローバルプロテクト

D. Syslog監視

正解: ([正解を表示します](#))

質問: 18

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** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication> For end-user authentication via Authentication Policy, the firewall directly integrates with several MFA platforms (Duo v2, Okta Adaptive, PingID, and RSA SecurID), as well as integrating through RADIUS or SAML for all other MFA platforms.

質問: **19**

テンプレートとテンプレートスタックをより簡単に再利用するために、構成で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. #Panorama
- C. &Panorama
- D. \$Panorama

正解: ([正解を表示します](#))

Create a template and template stack using a variable name for an object. Variable names must start with the dollar sign ( "\$" ) symbol. For example, you could use \$Panorama as a variable for the Panorama IP address that you want to configure on multiple managed firewalls and appliances <https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama-features/configuration-reusability-for-templates-and-template-stacks.html>

質問: **20**

方針がナットを適用するアドレスを含んでいるセキュリティ方針規則において何が使われなければならないか？

- A. Pre-NAT address and Pre-NAT zones
- B. Post-Nat addresses and Pre-NAT zones
- C. Post-NAT address and Post-Nat zones
- D. Pre-NAT address and Post-Nat zones

正解: **D** ([コメントを發表する](#))

質問: **21**

組織の管理者は、組織のセキュリティ体制を強化するためにファイアウォールを追加購入するために利用できる資金を持っています。

パートナーSEは、ファイアウォールを保護するリソースのできるだけ近くに配置することを推奨しています。SEのアドバイスは正しいですか、その理由または理由は何ですか。

- A. はいファイアウォールはセッションベースであるため、数百万のCPSに拡張できません
- B. 境界DDoSデバイスの前にファイアウォールを配置しないことで、ネットワーク内の機密性の高いデバイスに対する保護が強化されます
- C. はいゾーン保護プロファイルは、特定のデバイスタイプとオペレーティングシステムの構成を介して保護するリソースに合わせて調整できます

D. 配置に関係なく、サイバー攻撃のライフサイクルのすべての段階で攻撃者を防ぐための新しい防御と回復力を提供するファイアウォールはありません

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection>

#### 質問: 22

内部システムのユーザーは、プライベートIPが10.250.241.131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？

- A)
- 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

正解: D ([コメントを發表する](#))

#### 質問: 23

企業には、アクティブ/パッシブハイアベイラビリティ (HA)のペアとして構成された1組のPalo Alto Networksファイアウォールがあります。

何のため、ファイアウォール管理者は、フェールオーバーイベントが最後に発生した日を特定できますか？

- A. CLI問題から、ショー・システム・ログを使います
- B. フィルタサブタイプeq haをシステムログに適用する
- C. GUIのDashboardでHigh Availabilityウィジェットのステータスを確認する
- D. フィルタサブタイプeq haを設定ログに適用する

正解: ([正解を表示します](#))

#### 質問: 24

パロアルトネットワークNGFWを通過するユーザーのトラフィックが時々到達することがあります

<http://www.company.com>。それ以外の時はセッションがタイムアウトします。NGFWは、ユーザーのトラフィックが<http://www.company.com>に行くときに一致するPBFルールで設定されています。

ファイアウォールを自動的に設定する方法は、次のホップがダウンした場合にPBFルールを無効にしますか？

- A. 問題のPBFルールでWait Recover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。
- B. 問題のPBFルールでFailoverのアクションを持つMonitorプロファイルを作成して追加します。
- C. ファイアウォールの外部インターフェイスのリンクモニタリングプロファイルをイネーブルにして設定します。
- D. 仮想ルータ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モニタリングを設定します。

正解: [B \(コメントを發表する\)](#)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIFIcAK>

#### 質問: 25

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。

正解:

#### 質問: 26

GlobalProtect Portalを設定する際、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には
- D. ポータルへのクライアントマシン認証を有効にするには

正解: [\(正解を表示します\)](#)

The additional options of Browser and Satellite enable you to specify the authentication profile to use for specific scenarios. Select Browser to specify the authentication profile to use to authenticate a user accessing the portal from a web browser with the intent of downloading the GlobalProtect agent (Windows and Mac). Select Satellite to specify the authentication profile to use to authenticate the satellite.

Reference <https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/globalprotect/network-globalprotect-portals>

#### 質問: 27

ファイアウォールが「ドメインクレデンシャルフィルタ」方式を使用したクレデンシャルフィッシング防止用に設定されている場合、どのログインはクレデンシャル盗難として検出されますか？

- A. ログインしているユーザのIPアドレスへのマッピング。
- 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する。
- D. 有効な企業ユーザー名を行進させる。

正解: [A \(コメントを發表する\)](#)

<https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential-phishing-prevention>

質問: 28

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プルします。
- B. ログデータベースをエクスポートします
- C. scplogdbexportコマンドを使用します
- D. ACCを使用してログを統合します

正解: ([正解を表示します](#))

commands:

request logdb

migrate-to-panorama start end-timestart-timetype

<https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/migrate-panorama-logs-to-new-log-format>

質問: 29

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. 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。
- B. 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。
- C. 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。
- D. 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

正解: ([正解を表示します](#))

質問: 30

どのセキュリティポリシールール設定オプションを使用すると、ウイルス対策とスパイウェア対策のスキャンをサーバー-クライアントフローのみで無効にできますか？

- A. サーバーレスポンス検査を無効にする
- B. アプリケーションオーバーライドを適用する
- C. サーバーIPセキュリティポリシーの例外を追加する
- D. HIPプロファイルを無効にする

正解: [A \(コメントを發表する\)](#)

質問: 31

下の展示ボタンをクリックしてください。

ファイアウォールには、3つのPBF規則と、デフォルトVRに設定されている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には、192.168.10.10というIPアドレスを持つPCがあります。彼はHTTPS接続をします  
172.16.10.20。

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. 172.20.30.1
- C. 172.20.40.1
- D. 172.20.20.1

正解: [D \(コメントを發表する\)](#)

有効的なPCNSE-JPN問題集はJPNTTest.com提供され、PCNSE-JPN試験に合格することに役に立ちます！JPNTTest.comは今最新PCNSE-JPN試験問題集を提供します。JPNTTest.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: 32

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. 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時、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。
- 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. 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。
- 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: [B \(コメントを發表する\)](#)

質問: 33

SSL復号化では、ファイアウォールを信頼できるサードパーティとして確立し、SSL/TLS接続を保護するためにクライアントとサーバー間の信頼を確立するために何が必要ですか？

- A. リンク状態
- B. ステートフルファイアウォール接続
- C. 証明書
- D. プロファイル

正解: [\(正解を表示します\)](#)

[https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL%20decryption%20\(both%20forward%20proxy,secure%20an%20SSL%20FTLS%20connection.](https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-overview.html#:~:text=SSL%20decryption%20(both%20forward%20proxy,secure%20an%20SSL%20FTLS%20connection.)

**質問: 34**

管理者は、パロアルトネットワークNGFWのペアに対してアクティブ/パッシブHAを設定するように求められています。管理者は、アクティブファイアウォールに優先度100を割り当てます。パッシブファイアウォールにはどの優先順位が適していますか？

- A. 0
- B. 99
- C. 1
- D. 255

正解: **D** ([コメントを發表する](#))

Reference:

[https://docs.paloaltonetworks.com/content/dam/techdocs/en\\_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf](https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-0/pan-os-admin/pan-os-admin.pdf) page 315

**質問: 35**

機密性の高いビジネスデータを含む内部アプリケーションへのアクセスをユーザーに許可する前に、ユーザーに追加の資格情報の提供を強制するには、どのPAN-OSポリシーを構成する必要がありますか？

- A. セキュリティポリシー
- B. 復号化ポリシー
- C. 認証ポリシー
- D. アプリケーションオーバーライドポリシー

正解: ([正解を表示します](#))

Authentication policy enables you to authenticate end users before they can access services and applications. Whenever a user requests a service or application (such as by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods (factors), such as login and password, Voice, SMS, Push, or One-time Password (OTP) authentication

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/authentication/authentication-policy>

**質問: 36**

自動コミットリカバリの操作をトリガーする2つのイベントはどれですか？ (2つ選択してください。)

- A. 集約イーサネットインターフェイスコンポーネントに障害が発生した場合
- B. パノラマが構成をプッシュするとき
- C. ファイアウォールHAペアがフェイルオーバーしたとき
- D. ファイアウォールがローカルコミットを実行するとき

正解: **B,D** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html> Automatic commit recovery allows you to configure the firewall to attempt a specified number of connectivity tests after:

- 1- you push a configuration from Panorama or
- 2- commit a configuration change locally on the firewall.

Additionally, the firewall checks connectivity to Panorama every hour to ensure consistent communication in the event unrelated network configuration changes have disrupted connectivity between the firewall and Panorama or if implications to a pushed committed configuration may have affected connectivity.

質問: **37**

パノラマの方針を定義する時に、どの3種類の規則タイプが入手可能であるか？ (3を選びなさい。)

- A. Pre Rules
- B. Post Rules
- C. Default Rules
- D. Stealth Rules
- E. Clean Up Rules

正解: ([正解を表示します](#))

<https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/defining-policies-on-panorama>

質問: **38**

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. フォワードトラスト
- B. デフォルトの信頼できる認証局からの証明書
- C. ドメインルート証明書
- D. ドメインサブCA

正解: **D** ([コメントを發表する](#))

質問: **39**

管理者は、パロアルトネットワークNGFWを構成して、内部システム上のオペレーティングシステムの欠陥を悪用しようとしている外部ホストに対して保護を提供するように求められました。この攻撃を防ぐセキュリティプロファイルの種類はどれですか？

- A. Anti-Spyware
- B. URL Filtering
- C. Vulnerability Protection
- D. Antivirus

正解: ([正解を表示します](#))

質問: 40

ネットワークに移動するとき > GlobalProtect>ポータル>メソッドセクション、利用可能な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. ログオン前、次にオンデマンド
- B. ユーザーログオン (常時オン)
- C. ログオン後 (常時オン)
- D. 証明書ログオン
- E. オンデマンド (ユーザーが手動で開始する接続)

正解: A,B ([コメントを發表する](#))

質問: 41

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. HSCI-C
- B. HA2 backup
- C. Console Backup
- D. HA3

正解: ([正解を表示します](#))

質問: 42

エンジニアは、単一セッションのDoS攻撃から保護するために、入力ゾーンでパケットバッファ保護を構成しています。パケットバッファ保護はどのセッションに適用されますか？

- A. 新しいセッションに適用され、グローバルです
- B. 既存のセッションに適用され、グローバルではありません
- C. 既存のセッションに適用され、グローバルです
- D. 新しいセッションに適用され、グローバルではありません

正解: ([正解を表示します](#))

質問: 43

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. Interfaces
- B. Setup
- C. Application Override
- D. Security
- E. Virtual Routers

正解: ([正解を表示します](#))

質問: 44

管理者は、管理プレーンとデータプレーンの両方でCPU使用率に関する情報を収集する必要があります。管理者は目的のデータをどこで表示しますか？

- A. アプリケーションコマンドアンドコントロールセンター
- B. サポート>リソース
- C. 監視>使用率
- D. ダッシュボードのリソースウィジェット

正解: [C \(コメントを发表する\)](#)

質問: 45

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

正解: [\(正解を表示します\)](#)

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/networking-features/wildcard-address>

質問: 46

どのパロアルトネットワークスVM-SeriesファイアウォールがVMware NSXでサポートされていますか？

- A. VM-300
- B. VM-200
- C. VM-100
- D. VM-1000-HV

正解: [\(正解を表示します\)](#)

有効的な**PCNSE-JPN**問題集はJPNTTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTTest.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: 47

ネットワークセキュリティエンジニアは、IPv6アドレスを使用して仮想ルータを設定する必要があります。

どの2つのルーティングオプションがこれらのアドレスをサポートしていますか？ (2つ選択)

- A. 確かでないBGP
- B. OSPFv3
- C. RIP
- D. 静的ルート

正解: **B,D** ([コメントを发表する](#))

<https://live.paloaltonetworks.com/t5/Management-Articles/Does-PAN-OS-Support-Dynamic-Routing-Protocols-OSPF-or-BGP-with/ta-p/62773>

質問: 48

どの3つのフィールドをpcapフィルタに含めることができますか？ (3つ選択)

- A. Egress interface
- B. Source IP
- C. Rule number
- D. Destination IP
- E. Ingress interface

正解: ([正解を表示します](#))

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

質問: 49

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
- B. 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
- C. 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
- D. 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
- E. 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

正解: ([正解を表示します](#))

質問: 50

ユーザーが選択したオフィススイートアプリケーションにアクセスできるようにする必要があります。オフィススイートのアプリケーションへのアクセスを許可するようにファイアウォールをどのように構成する必要がありますか？

- A. アプリケーショングループを作成し、それにビジネスシステムを追加します。
- B. アプリケーションフィルターを作成し、Officeプログラムという名前を付けてから、ビジネスシステムカテゴリでフィルター処理します。
- C. アプリケーションフィルターを作成し、Officeプログラムという名前を付けてから、Officeプログラムサブカテゴリでフィルターします。

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

正解: ([正解を表示します](#))

質問: 51

ファイアウォール管理者は、どのログを使用してセッションが復号化されたかどうかを判断できます。

- A. 関連イベント
- B. トラフィック
- C. 復号化
- D. セキュリティポリシー

正解: ([正解を表示します](#))

<https://live.paloaltonetworks.com/t5/certification-articles/pcnse-and-pcnsa-exam-changes-with-10-0/ta-p/344832>

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/troubleshoot-and-monitor-decryption/decryption-logs.html> The Decryption Log (Monitor Logs Decryption ) provides comprehensive information about sessions that match a Decryption policy to help you gain context about that traffic so you can accurately and easily diagnose and resolve decryption issues. The firewall does not log traffic if the traffic does not match a Decryption policy.

質問: 52

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. 構成監査
- B. ポリシーオプティマイザー
- C. アプリケーショングループ
- D. テストポリシーの一致

正解: B ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer> his new feature identifies port-based rules so you can convert them to application-based rules that allow the traffic or add applications to existing rules without compromising application availability. <https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/app-id-features/policy-optimizer.html>

質問: 53

どの2つの設定は、ファイアウォール上でローカルにのみ設定でき、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されませんか？ (2つ選択)

- A. HA1 IPアドレス

- B. ネットワークインターフェイスタイプ
- C. マスターキー
- D. ゾーン保護プロファイル

正解: [A,C \(コメントを发表する\)](#)

<https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-exceptions.html># You can use Templates and Template Stacks to define a wide array of settings but you can perform the following tasks only locally on each managed firewall:

Configure a device block list.

Clear logs.

Enable operational modes such as normal mode, multi-vsyst mode, or FIPS-CC mode.

Configure the IP addresses of firewalls in an HA pair.

Configure a master key and diagnostics.

Compare configuration files (Config Audit).

Renaming a vsyst on a multi-vsyst firewall.

#### 質問: 54

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
- 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. 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
- D. 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。

正解: [\(正解を表示します\)](#)

#### 質問: 55

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. 変数
- B. テンプレートスタック
- C. コレクターグループ
- D. 仮想システム

正解: [\(正解を表示します\)](#)

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/templates-and-template-stacks>

<https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables.html>

**質問: 56**

WildFireのベストプラクティスを実装するための重要なステップは何ですか？

- A. セキュリティ優先のネットワークでは、WildFireのサイズ制限を最小値に設定します
- B. コンテンツの更新を毎分取得するようにファイアウォールを構成します
- C. 脅威防止サブスクリプションがアクティブであることを確認します
- D. ミッションクリティカルなネットワークで、WildFireのサイズ制限を最大値に増やします

正解: ([正解を表示します](#))

**質問: 57**

グラフィックに基づいて、サーバー監視パネルに表示される出力を正確に説明しているステートメントはどれですか？

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

正解: ([正解を表示します](#))

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

**質問: 58**

どのCLIコマンドが現在の管理プレーンのメモリ使用率を表示していますか？

- A. > デバッグ管理サーバショー
- B. > 実行中のリソースモニタを表示する
- C. > システム情報を表示する
- D. > システムリソースを表示する

正解: **D** ([コメントを發表する](#))

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/tap/59364>

"The command show system resources gives a snapshot of Management Plane (MP) resource utilization including memory and CPU. This is similar to the 'top' command in Linux."

<https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Interpret-show-system-resources/tap/59364>

**質問: 59**

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。
- 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。
- D. 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。

正解: ([正解を表示します](#))

質問: 60

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](#))

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/networking/nat-configuration-examples>

質問: 61

ファイアウォールとネットワークを、パケットバッファを圧倒し、正当なトラフィックをドロップさせる可能性のある単一ソースのサービス拒否 (DoS) 攻撃から保護するために、を構成できます。

- A. PBP (パケットバッファ保護)
- B. BGP (ボーダーゲートウェイプロトコル)
- C. PBP (プロトコルベースの保護)
- D. PGP (パケットゲートウェイプロトコル)

正解: ([正解を表示します](#))

有効的なPCNSE-JPN問題集はJPNTTest.com提供され、PCNSE-JPN試験に合格することに役に立ちます！JPNTTest.comは今最新PCNSE-JPN試験問題集を提供します。JPNTTest.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: 62

管理者は、Panoramaとその管理対象デバイスがSSL / TLSサービスに使用する証明書とプロトコルを定義するためにどのオプションを選択しますか？

- A. 復号化プロファイルを設定し、SSL / TLSサービスを選択します。
- B. ポリシー/サービス/ URLカテゴリ/サービスでSSL / TLSを設定します。
- C. SSL / TLSプロファイルを設定します。
- D. SSL通信を許可するセキュリティポリシールールを設定します。

正解: ([正解を表示します](#))

質問: 63

Connectメソッドが事前ログオンに設定されている場合、GlobalProtectのユーザーを認証するために使用される公開キーインフラストラクチャコンポーネントはどれですか？

- A. マシン証明書
- B. 信頼された根証明書
- C. オンライン証明書ステータスプロトコル
- D. 証明書撤回リスト

正解: A ([コメントを發表する](#))

質問: 64

DoSおよびゾーン保護を計画するためのPANWのベストプラクティスに基づいて、各タイプのDoS攻撃をそのタイプの攻撃の例と一致させます。

正解:

質問: 65

管理者は、ユーザーIDの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. > ftp export mgmt-pcap from mgmt.pcap to <FTP host>
- B. > scp export mgmt-pcap from mgmt.pcap to {username@host:path}
- C. > scp export pcap-mgmt from pcap.mgmt to (username@host:path)
- D. > scp export pcap from pcap to (username@host:path)

正解: ([正解を表示します](#))

Additionally, you can manually export the PCAP via SCP or TFTP, i.e.: > scp export mgmt-pcap from mgmt.pcap to <value> Destination (username@host:path) Ref:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000C1eECAS>

質問: 66

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:

**質問: 67**

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. 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。
- C. 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
- 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](#))

PAN-OS 10.0

<https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/administer-panorama/enable-automated-commit-recovery.html>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery>

**質問: 68**

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ーの[ルールの使用法]ページ

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/use-application-objects-in-policy/resolve-application-dependencies.html>

**質問: 69**

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. 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。
- 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. 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。

正解: ([正解を表示します](#))

**質問: 70**

ネットワーク管理者は、特定のスパイウェアシグニチャのデフォルトのアクションを表示する必要があります。管理者は、[オブジェクト]> [セキュリティプロファイル]> [スパイウェア対策]のタブとメニューに従い、デフォルトのプロファイルを選択します。

次に何をすべきですか？

- A. simple-criticalルールをクリックしてから、[Action]ドロップダウンリストをクリックします。
- B. [ルール]タブをクリックし、[アクション]列で「デフォルト」のルールを探します。
- C. [例外]タブをクリックしてから、[すべての署名を表示]をクリックします。
- D. [アクション]列に表示されるデフォルトのアクションを表示します。

正解: [\(正解を表示します\)](#)

**質問: 71**

AP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 (SA)を同期するとどうなりますか？

- A. フェーズ2SAはHA2リンクを介して同期されます
- B. 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
- C. フェーズ1SAはHA1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HA3リンクを介して同期されます

正解: [A \(コメントを发表する\)](#)

From the Palo Alto documentation below, "when a VPN is terminated on a Palo Alto firewall HA pair, not all IPSEC related information is synchronized between the firewalls... This is an expected behavior. IKE phase 1 SA information is NOT synchronized between the HA firewalls." And from the second link, "Data link (HA2) is used to sync sessions, forwarding tables, IPsec security associations, and ARP tables between firewalls in the HA pair. Data flow on the HA2 link is always unidirectional (except for the HA2 keep-alive). It flows from the active firewall to the passive firewall."

<https://know>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW>

[ledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&)

[&lang=en\\_US%E2%80%A9](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&)

[lang=en\\_US%E2%80%A9&](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&)

[&refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&)

[refURL=http%3A%2F%2Fknowledgebase.paloaltonetworks.com%2FKCSArticleDetail](https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&)

**質問: 72**

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. 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。
- B. 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。
- C. 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。
- D. 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。

正解: [D \(コメントを发表する\)](#)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIRtCAK> Block sessions that use cipher suites you don't support. You configure which cipher suites (encryption algorithms) to allow on the SSL Protocol Settings tab. Don't allow users to connect to sites with weak cipher suites.

質問: 73

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://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/ha-firewall-states.html>

質問: 74

次の構成では、宛先10.10.0.4にどのルートが使用されますか？

- A. ルート1
- B. ルート4
- C. ルート3
- D. ルート3

正解: [\(正解を表示します\)](#)

質問: 75

ファイアウォールでローカルにテンプレート構成をオーバーライドする場合、何を考慮する必要がありますか？

- A. パノラマのみがオーバーライドを元に戻すことができます
- B. パノラマはオーバーライドされた構成の可視性を失います
- C. パノラマはオーバーライドされた値でテンプレートを更新します
- D. ファイアウォールテンプレートは、Panorama内で同期していないことを示します

正解: **B** ([コメントを發表する](#))

Based on my knowledge out-of-sync message appear on Panorama only was perform a commit to Panorama but not pushed to the NGFW. <https://live.paloaltonetworks.com/t5/general-topics/reason-for-out-of-sync-message-in-panorama/td-p/328292>

質問: 76

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:

有効的な**PCNSE-JPN**問題集はJPNTTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTTest.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

PA-5050のデータプレーンにはどの3つの機能がありますか？ (3つ選択)

- A. 署名の一致
- B. ネットワーク処理
- C. 動的ルーティング
- D. プロトコルデコーダ
- E. 管理

正解: ([正解を表示します](#))

質問: 78

管理者は、ファイアウォールデバイスグループにコミットおよびプッシュされた最近のポリシー変更を評価する必要があります。

管理者は構成の変更をどのように特定する必要がありますか？

- A. [監視]タブで構成ログを確認します
- B. [プッシュスコープ]の下の[変更のプレビュー]をクリックします
- C. Test Policy Matchを使用して、Panoramaのポリシーを確認します
- D. コンテキスト影響を受けるファイアウォールに切り替えて、構成監査ツールを使用します

正解: **A** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/panorama-web-interface/panorama-commit-operations.html>

質問: **79**

ファイアウォール管理者は、ファイアウォールGUIを認証できません。

ファイアウォールのどの2つのログに、この問題のトラブルシューティングに役立つ認証関連情報が含まれていますか？ (2つを選択してください)

- A. dp-monitor .log
- B. System log
- C. authd log
- D. ms log
- E. Traffic log

正解: ([正解を表示します](#))

質問: **80**

デフォルトでは、GlobalProtectアプリがGlobalProtectゲートウェイへのIPSecトンネルの確立に失敗するとどうなりますか？

- A. GlobalProtectゲートウェイへのIPSecトンネルを確立しようとし続けます
- B. GlobalProtectゲートウェイへのトンネル確立処理を直ちに停止します
- C. SSL / TLSを使用してGlobalProtectゲートウェイへのトンネルを確立しようとします
- D. SSL / TLSを使用してGlobalProtectポータルへのトンネルを確立しようとします

正解: **C** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-agent-configuration-tab/globalprotect-portals-agent-app-tab.html>

質問: **81**

同僚の作業を監査しており、それらがスパイウェア対策プロファイルのパロアルトネットワークスのベストプラクティスと一致していることを確認する必要があります。

ベストプラクティスの基準を満たすために、シングルパケットキャプチャを有効にする必要がある3つの重大度レベルはどれですか。 (3つ選択してください)

- A. 高
- B. 中
- C. クリティカル
- D. 情報
- E. 低

正解: **A,B,C** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/security-profiles>

**質問: 82**

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

正解: [B,D,E \(コメントを發表する\)](#)

<https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-with-pre-logon.html>

**質問: 83**

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: [\(正解を表示します\)](#)

**質問: 84**

リモート管理者は、信頼されていないインターフェイスでファイアウォールにアクセスする必要があります。WebUIへの証明書ベースの管理者認証を構成するためにファイアウォールで必要な2つのコンポーネントはどれですか。 2つ選択してください)

- A. クライアント証明書
- B. 証明書プロファイル
- C. 認証局 (CA) 証明書
- D. サーバー証明書

正解: [\(正解を表示します\)](#)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/configure-administrative-accounts-and-authentication/configure-certificate-based-administrator-authentication-to-the-web-interface.html>

**質問: 85**

エンジニアは、さまざまなディレクトリサービス環境にUser-IDを展開する計画段階にあります。ユーザーIDによるサーバー監視に使用できるサーバーOSプラットフォームはどれですか？

- A. Novell eDirectory、Microsoftターミナルサーバー、およびMicrosoft Active Directory

- B. Microsoftターミナルサーバー、Red Hat Linux、およびMicrosoft Active Directory
- C. Microsoft Active Directory、Red Hat Linux、およびMicrosoft Exchange
- D. Microsoft Exchange、Microsoft Active Directory、およびNovelleDirectory

正解: ([正解を表示します](#))

質問: 86

SSL復号化中に、リソース消費に影響を与える3つの要因はどれですか1? (3つ選択してください)

- A. TLSプロトコルバージョン
- B. トランザクションサイズ
- C. 鍵交換アルゴリズム
- D. 非標準ポートを使用するアプリケーション
- E. 証明書発行者

正解: **A,B,C** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/best-practices/8-1/decryption-best-practices/decryption-best-practices/plan-ssl-decryption-best-practice-deployment.html>

質問: 87

企業のログイン情報をウェブサイトフォームに提出できない機能は何ですか?

- A. データフィルタリング
- B. ユーザーID
- C. ファイルブロック
- D. クレデンシャルフィッシング防止

正解: ([正解を表示します](#))

Reference:

"Credential phishing prevention works by scanning username and password submissions to websites and comparing those submissions against valid corporate credentials. You can choose what websites you want to either allow, alert on, or block corporate credential submissions to based on the URL category of the website. Alternatively, you can present a page that warns users against submitting credentials to sites classified in certain URL categories. This gives you the opportunity to educate users against reusing corporate credentials, even on legitimate, non-phishing sites. In the event that corporate credentials are compromised, this feature allows you to identify the user who submitted credentials so that you can remediate."

質問: 88

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. 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
- B. ファイアウォールがTCPSYNパケットをドロップしました
- C. 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
- D. 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

正解: ([正解を表示します](#))

質問: 89

管理者は、パノラマレポートでパロアルトネットワークスNGFW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にあるようです。正しく構成されていない場合、トラフィックログのみがNGFWからPanoramaに送信されなくなる可能性が高いのはどの設定ですか。

- A)
- B)
- C)
- 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

正解: ([正解を表示します](#))

質問: 90

イメージに基づいて、何がコミット警告を引き起こしましたか。

- A. FWDtrustのCA証明書はファイアウォールにインポートされていません。
- B. FWDtrust証明書は、信頼されたルートCAとしてマークされていません。
- C. FWDtrust証明書に証明書チェーンがありません。
- D. SSL転送プロキシでは、パブリック証明書をファイアウォールにインポートする必要があります。

正解: ([正解を表示します](#))

質問: 91

どのCLIコマンドを使用すると、管理者はデータプレーンのCPU使用率を確認できますか？

- A. 実行中のリソースモニタを表示する
- 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. 実行リソースのデバッグ

正解: **A** ([コメントを公表する](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIXwCAK>

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

有効的な**PCNSE-JPN**問題集はJPNTTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTTest.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: 92

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追加するか？

- A. アラート
- B. デフォルト
- C. 許可
- D. ログ

正解: ([正解を表示します](#))

質問: 93

企業は、最小限の事前構成でリモートサイトに送信されるようにファイアウォールを事前構成する必要があります。展開後、各ファイアウォールは、複数の地域データセンターに戻る安全なトンネルを確立して、将来の地域データセンターを含める必要があります。将来のサイト？

- A. IKEv2を使用したIPsecトンネル
- B. PPTPトンネル
- C. GlobalProtect衛星
- D. GlobalProtectクライアント

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite-configuration-tab.html>

質問: 94

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. SSLセッションの復号化
- B. WildFireの提出
- C. DoS保護
- 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](#))

質問: 95

ファイアウォールは、パケットが新しいセッションの最初のパケットであるかどうか、またはパケットが既存のセッションの一部であるかどうかを、どの種類の一致を使用して判断しますか？

A. 6タプルマッチ：

送信元IPアドレス、宛先IPアドレス、送信元ポート、宛先ポート、プロトコル、および送信元セキュリティゾーン

B. 5タプルマッチ：

送信元IPアドレス、宛先IPアドレス、送信元ポート、宛先ポート、プロトコル

**C. 7タプルマッチ :**

送信元IPアドレス、宛先IPアドレス、送信元ポート、宛先ポート、送信元ユーザー、URLカテゴリ、および送信元セキュリティゾーン

**D. 9タプルマッチ :**

送信元IPアドレス、宛先IPアドレス、送信元ポート、宛先ポート、送信元ユーザー、送信元セキュリティゾーン、

正解: ([正解を表示します](#))

Destination Security Zone, Application, and URL Category

Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVECA0> On a Palo Alto Networks firewall, a session is defined by two uni-directional flows each uniquely identified by a 6-tuple key: source-address, destination-address, source-port, destination-port, protocol, and security-zone.

**質問: 96**

HA Liteではどの3つのオプションがサポートされていますか？ 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. 構成同期
- E. セッション同期

正解: ([正解を表示します](#))

"The PA-200 firewall supports HA Lite only. HA Lite is an active/passive deployment that provides configuration synchronization and some runtime data synchronization such as IPSec security associations. It does not support any session synchronization (HA2), and therefore does not offer stateful failover."

**質問: 97**

管理者は、インターレース構成がファイアウォールでローカルにオーバーライドされていることに気づきました。構成をPanoramaから管理する必要があり、オーバーライドは許可されていません。管理者がこの要件を満たすことができる1つの方法は何ですか？

- A. 実行コンフィギュレーションをリロードし、ファイアウォールのローカルコミットを実行します。
- B. [デバイスとネットワークテンプレートを含める]オプションを使用して、Panoramaからデバイスグループのコミットプッシュを実行します。
- C. ファイアウォールのCLIからコミットを実行します。
- D. [テンプレート値を強制する]オプションを使用して、Panoramaからテンプレートコミットプッシュを実行します

正解: ([正解を表示します](#))

**質問: 98**

ブートストラップUSBフラッシュドライブは、以前ラボで使用されていたパロアルトネットワーク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

正解: ([正解を表示します](#))

<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>

**質問: 99**

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. 新しいカテゴリアクションをアラートに変更して、設定をもう一度プッシュします
- 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

正解: [C \(コメントを發表する\)](#)

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000PNqw>

**質問: 100**

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. 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。

正解: ([正解を表示します](#))

"If the list source is secured with SSL (i.e. lists with an HTTPS URL), enable server authentication. Select a Certificate Profile or create a New Certificate Profile for authenticating the server that hosts the list. The certificate profile you select must have root certificate authority (CA) and intermediate CA certificates that match the certificates installed on the server you are authenticating."

#### 質問: 101

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ーフェイスの命名に適していますか？ (2つを選択してください)

- A. ae.8
- B. aggregate.1
- C. ae.1
- D. aggregate.8

正解: **A,C** ([コメントを发表する](#))

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/network/network-interfaces/aggregate-ethernet-ae-interface-group.html>

#### 質問: 102

顧客は、カスタムPostgreSQLデータベース接続の1つで不明トー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: ([正解を表示します](#))

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 Cases Three 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 times A discussion of typical uses of application override and specific implementation examples is here: <https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-and-Tricks-How-to-Create-an-Application-Override/ta-p/65513>

**質問: 103**

管理者が稼働時間、PAN-OSバージョン、シリアル番号などのファイアウォールに関する詳細を表示できるようにするCLIコマンドはどれですか。

- A. デバッグシステムの詳細
- B. セッション情報を表示
- C. システム情報を表示
- D. システムの詳細を表示

正解: ([正解を表示します](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIZuCAK>

**質問: 104**

エンジニアは、動的ユーザーグループ (DUG)に基づいてセキュリティポリシーを作成しています。これにはどのような利点がありますか？

- A. ポリシーやグループの変更を手動で作成してコミットすることなく、ユーザーをメンバーとして自動的に含める
- B. DUGは、管理者がパロアルトネットワークファイアウォールの管理インターフェイスにアクセスできるようにするためにのみ使用されます
- C. トラフィックを復号化し、ユーザーIDベースのポリシーの悪意のある動作をスキャンする機能を有効にします
- D. 指定されたタグに一致する新しいユーザーでDUGを更新するために、定期的にコミットをスケジュールします

正解: ([正解を表示します](#))

Dynamic user groups help you to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. Previously, quarantining users in response to suspicious activity meant time- and resource-consuming updates for all members of the group or updating the IP address-to-username mapping to a label to enforce policy at the cost of user visibility, as well as having to wait until the firewall checked the traffic. Now, you can configure a dynamic user group to automatically include users as members without having to manually create and commit policy or group changes and still maintain user-to-data correlation at the device level before the firewall even scans the traffic.

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html>

**質問: 105**

復号化転送インターフェイスのペアでサポートされているDecryptionBrokerセキュリティチェーンの数を正しく識別する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. ファイアウォールごとに単一の透過的なブリッジセキュリティチェーンがサポートされます
- B. インターフェイスのペアごとに単一の透過的なブリッジセキュリティチェーンがサポートされます
- C. L3セキュリティチェーンは最大64のセキュリティチェーンをサポートします
- D. L3セキュリティチェーンは最大32のセキュリティチェーンをサポートします

正解: ([正解を表示します](#))

質問: 106

動的ユーザーグループに含まれるようにユーザー名にタグを付けるために使用できる2つの機能はどれですか？ (2つ選択してください)

- A. ログ転送の自動タグ付け
- B. GlobalProtectエージェント
- C. ユーザーIDWindowsベースのエージェント
- D. XML API

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically.html> You can enable the dynamic registration process using any of the following options:

User-ID agent for Windows\*

VM Information Sources

Panorama Plugin

VMware Service Manager

XML API\*

Auto-Tag\*

[https://www.paloaltonetworks.com/content/dam/pan/en\\_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf](https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.pdf) Usernames can also be tagged and untagged using the auto-tagging feature in a Log Forwarding Profile. You also can program another utility to invoke PAN-OS XML API commands to tag or untag usernames.

有効的な**PCNSE-JPN**問題集はJPNTTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTTest.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: 107

スタック内の複数のテンプレートを使用して多くのファイアウォールを管理すると、2つの利点がありますか？ (2つ選択してください。)

- A. テンプレートからアドレスオブジェクトを継承する
- B. ファイアウォールの一般的な標準テンプレート構成を定義します
- C. すべてのスタックでサーバープロファイルと認証構成を標準化する
- D. すべてのスタックにわたるセキュリティポリシーのログ転送プロファイルを標準化する

正解: ([正解を表示します](#))

Template stacks simplify management because they allow you to define a common base configuration for all devices attached to the template stack and they give you the ability to layer templates to create a combined configuration.

#### 質問: 108

動的ユーザーグループメンバーシップの更新は自動的に行われるため、静的グループオブジェクトの代わりに動的ユーザーグループを使用すると、次のことが可能になります。

- A. 手動のポリシー変更を使用して、ユーザーの行動の変化や潜在的な脅威に対応する
- B. ポリシーを自動的に変更せずに、ユーザーの行動の変化や潜在的な脅威に対応する
- C. 手動のポリシー変更でユーザーの行動の変化と確認された脅威に対応する
- D. 手動でポリシーを変更することなく、ユーザーの行動の変化や潜在的な脅威に対応する

正解: [D \(コメントを发表する\)](#)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups#:~:text=Because%20updates%20to%20dynamic%20user,threats%20without%20manual%20policy%20changes.>

#### 質問: 109

ファイアウォールは、復号化されたトラフィックを検査のためにセキュリティチェーンに転送するために、どのタイプのインターフェイスを使用しますか？

- A. レイヤー2
- B. タップ
- C. レイヤー3
- D. 復号化ミラー

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/network-packet-broker/configure-routed-layer-3-security-chains> Configure security chain devices with Layer 3 interfaces to connect to the security chain network. These Layer 3 interfaces must have an assigned IP address and subnet mask. <https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/decryption-broker/security-chain-layer-3-guidelines.html>

#### 質問: 110

どの管理認証方式が外部サービスによる許可をサポートしますか？

- A. Certificates

- B. LDAP
- C. RADIUS
- D. SSH keys

正解: [C \(コメントを发表する\)](#)

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication>

質問: 111

管理者は、世界中で90のファイアウォールのWildFireサブスクリプションを購入しました。管理者はWildFireインフラストラクチャに関して何を考慮する必要がありますか？

- A. データプライバシー規制に準拠するために、WildFireの署名と評決はグローバルに共有されません。
- B. Palo Alto Networksは、1つのグローバルクラウドと4つのWildFireリージョナルクラウドを所有および維持しています。
- C. WildFireグローバルクラウドはベアメタル分析のみを提供します。
- D. 各WildFireクラウドはサンプルを分析し、他のWildFireクラウドとは独立してマルウェアのシグネチャと判定を生成します。

正解: [\(正解を表示します\)](#)

質問: 112

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: [\(正解を表示します\)](#)

質問: 113

ファイアウォール管理に証明書認証を使用する場合、承認にはどの方法が使用されますか？

- A. ローカル
- B. Kerberos
- C. 半径
- D. LDAP

正解: [B \(コメントを发表する\)](#)

質問: 114

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ポータルとGlobalProtectゲートウェイ
- C. GlobalProtectアプリとGlobalProtect衛星
- D. GlobalProtectアプリとGlobalProtectポータル

正解: **A** ([コメントを發表する](#))

UDP 4501 Used for IPSec tunnel connections between GlobalProtect apps and gateways.

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/firewall-administration/reference-port-number-usage/ports-used-for-globalprotect.html>

質問: **115**

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記録するか？

- A. ログ
- B. アラート
- C. 許可
- D. デフォルト

正解: **B** ([コメントを發表する](#))

<https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/url-filtering/url-filtering-profile-actions>

質問: **116**

各SD-WAN構成要素をその要素の説明と一致させます。

正解:

質問: **117**

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

正解: **C,D** ([コメントを發表する](#))

[https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-](https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html)

[notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html](https://docs.paloaltonetworks.com/plugins/vm-series-and-panorama-plugins-release-notes/panorama-plugin-for-sd-wan/sd-wan-plugin-200/features-introduced-in-sd-wan-2-0.html)

<https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?>

[pagePath=/content/pan/en\\_US/resources/guides/pan-os-secure-sd-wan-deployment-guide](https://www.paloaltonetworks.nl/apps/pan/public/downloadResource?)

質問: **118**

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://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html>

#### 質問: 119

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. サイトBのみで有効にする
- B. サイトAのみで有効にする
- C. パッシブモードでサイトBだけで有効にする
- D. サイトAおよびサイトBで有効にする

正解: ([正解を表示します](#))

#### 質問: 120

セキュリティポリシーの一致にサービスを使用する場合とアプリケーションを使用する場合の違いは何ですか？

- A. 「サービス」の使用は、十分なパケットがApp-IDの識別を可能にした後に、ファイアウォールが行動を起こすことを可能にする
- B. 「サービス」を使用すると、ポート番号に基づいて最初に観測されたパケットでファイアウォールが即座に処理されます。「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-
- C. 「サービス」と「アプリケーション」の間には違いはありません。「アプリケーション」を使用すると、ポート番号の代わりにフレンドリーなアプリケーション名を使用できるようになるため、構成が簡単になります。
- D. 「サービス」の使用により、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で即座に処置を取ることができます。「アプリケーション」を使用すると、ファイアウォールは即座にアクションを取ることができます。使用されているポートは、アプリケーションstandardport listのメンバーです

正解: ([正解を表示します](#))

<https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508#> A service on the Palo Alto Networks firewall is a TCP or UDP port which port is open or closed and does not look beyond Layer 4. An application it goes into Layer 7 inspection to ascertain which application is active in a data flow and will enforce "normal" behavior onto it, DNS Query <https://live.paloaltonetworks.com/t5/blogs/what-are-applications-and-services/ba-p/342508#>  
Concept 1 A service on the Palo Alto Networks firewall is a TCP or UDP port, as it would be defined on a traditional firewall or access list. It simply defines which port is open or closed and does not look beyond Layer 4.

#### Concept 2

An application is what makes the Palo Alto Networks next-generation firewall so powerful; it goes into Layer 7 inspection to ascertain which application is active in a data flow and will enforce "normal" behavior onto it (e.g., a session identified as DNS that suddenly sends an SQL query is abnormal and will be blocked).

#### 質問: 121

新しいデバイスグループを作成してファイアウォールを管理するたびに、パノラマでデフォルトで割り当てられるデバイスグループオプションは何ですか？

- A. Universal
- B. Global
- C. Master
- D. Shared

正解: ([正解を表示します](#))

有効的なPCNSE-JPN問題集はJPNTTest.com提供され、PCNSE-JPN試験に合格することに役に立ちます！JPNTTest.comは今最新PCNSE-JPN試験問題集を提供します。JPNTTest.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: 122

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。

お客様は、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. 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。
- 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. 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
- 正解: ([正解を表示します](#))

質問: 123

用語を対応する定義と一致させてください。

正解:

質問: 124

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. Dynamic
- B. Custom Panorama Admin
- C. Role Based
- D. Device Group
- E. Template Admin

正解: D,E ([コメントを发表する](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIETCA0>

質問: 125

ファイアウォール管理者は、重要なビジネスアプリケーションの稼働時間要件のために、A / PHAペアをより迅速にフェイルオーバーする必要があります。

正しい設定は何ですか？

- A. HAタイマープロファイルを「ユーザー定義」に変更し、手動でタイマーを設定します。
- B. HAタイマープロファイルを「高速」に変更します。
- C. HAタイマープロファイルを「アグレッシブ」に変更するか、詳細プロファイルの設定をカスタマイズします。
- D. HAタイマープロファイルを「クイック」に変更し、高度なプロファイルでカスタマイズします。

正解: ([正解を表示します](#))

Use the Recommended profile for typical failover timer settings and the Aggressive profile for faster failover timer settings. The Advanced profile allows you to customize the timer values to suit your network requirements. <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/high-availability/ha-concepts/ha-timers.html>

**質問: 126**

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。

正解: **B** ([コメントを发表する](#))

Both templates and template stacks support variables. Variables allow you to create placeholder objects with their value specified in the template or template stack based on your configuration needs. Create a template or template stack variable to replace IP addresses, Group IDs, and interfaces in your configurations. <https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/override-a-template-setting.html>

**質問: 127**

管理者は、インターネットから開始された接続をDMZ内の複数のWebサーバーに受信させたいと考えています。

206.15.22.9ポート80 / TCP宛てのトラフィックは、10.1.1.22のサーバに転送する必要があります。

画像に表示されている情報に基づいて、どのNATルールがWeb閲覧トラフィックを正しく転送するのでしょうか。

- A)
  - B)
  - C)
  - D)
- A. Option A
  - B. Option B
  - C. Option C
  - D. Option D

正解: ([正解を表示します](#))

NAT zones are just whatever interface traffic is going to. The source (the big cloud internet) is obviously internet, and the destination zone is the internet facing interface of the firewall, so the destination is also internet. It then is translated into an IP that the internal network can read.

**質問: 128**

Palo Alto Networks NGFWにユーザ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

正解: [A,E,F \(コメントを发表する\)](#)

The administrative accounts are DEFINED on an external SAML, TACACS+, or RADIUS server. The server performs both authentication and authorization. For authorization, you define Vendor-Specific Attributes (VSAs) on the TACACS+ or RADIUS server, or SAML attributes on the SAML server. PAN-OS maps the attributes to administrator roles, access domains, user groups, and virtual systems that you define on the firewall. Kerberos, LDAP, and PAP required the admin account to be locally defined on the firewall. <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/firewall-administration/manage-firewall-administrators/administrative-authentication.html>

質問: 129

ファイアウォールが通過するトラフィックをキャプチャできないようにする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. トラフィックはオフロードされません。
- B. ファイアウォールのDP CPUが50%を超えています。
- C. トラフィックがパケットキャプチャフィルタと一致しません。
- D. ファイアウォールはマルチvsysモードです。

正解: [\(正解を表示します\)](#)

質問: 130

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: [\(正解を表示します\)](#)

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>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cle8CAC>

**質問: 131**

Palo Alto Networks NGFWをアップグレードする前に、何をする必要がありますか？

- A. ファイアウォールがサポートされているバージョンのアプリと脅威の更新を実行していることを確認します
- B. ファイアウォールのデバイス状態をエクスポートします
- C. PAN-OSサポート契約が少なくとももう1年間有効であることを確認してください
- D. ファイアウォールが、ライセンスされたサブスクリプションをサポートするバージョンのウイルス対策ソフトウェアとバージョンのWildFireを実行していることを確認します。

正解: ([正解を表示します](#))

**質問: 132**

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: [A \(コメントを發表する\)](#)

Reference:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClboCAC> The Question is simply asking how to verify if traffic was being decrypted. There are (2) ways to see this in the traffic logs:

1. To confirm that the traffic is decrypted inside the WebGUI > Monitor > Logs > Traffic. Click the magnifying glass icon in the traffic log entries to confirm that the connections were decrypted.
2. Another way to validate the decrypted session is by enabling the column "Decrypted" as below Traffic logs . This can be done by clicking on the arrow down next to any column title and selecting the Columns > Decrypted. This shows decrypted status in regular traffic log view.

**質問: 133**

ローカルオブジェクトとポリシーを備えたスタンドアロンファイアウォールをPanoramaに移行する必要があります。パノラマがファイアウォールを完全に管理するために、どの手順を使用する必要がありますか？

- A. 「パノラマ構成スナップショットのインポート」操作を使用してから、デバイスとネットワークテンプレートを含める」を使用してデバイスグループのコミットプッシュを実行します
- B. デバイス構成をPanoramaにインポート」操作を使用してから、デバイス構成バンドルをエクスポートまたはプッシュ」して構成をプッシュします
- C. 「パノラマ構成スナップショットのインポート」操作を使用してから、デバイス構成バンドルのエクスポートまたはプッシュ」を使用して構成をプッシュします

D. 「デバイス構成をパノラマにインポート」操作を使用してから、「デバイスとネットワークテンプレートを含める」を使用してデバイスグループのコミットプッシュを実行します

正解: **B** ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/panorama/9-1/panorama-admin/manage-firewalls/transition-a-firewall-to-panorama-management/migrate-a-firewall-to-panorama-management.html>

質問: **134**

WF-500アプライアンスはどの3つのオプションでローカル分析をサポートしていますか？ (3つ選択)

A. jar files

B. PNG files

C. Portable Executable (PE) files

D. APK files

E. E-mail links

正解: **A,C,E** ([コメントを發表する](#))

質問: **135**

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](#))

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/user-id/user-id-concepts/user-mapping/xml-api.html>

<https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/user-id-concepts/user-mapping/server-monitoring.html>

質問: **136**

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. ファイアウォールに対するユーザーIDエージェント

B. ファイアウォール

C. ドメインコントローラからユーザー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

正解: **B** ([コメントを發表する](#))

<https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-firewalls-to-redispatch-user-mapping-information>

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/user-id/deploy-user-id-in-a-large-scale-network/redistribute-user-mappings-and-authentication-timestamps/firewall-deployment-for-user-id-redistribution.html#ide3661b46-4722-4936-bb9b-181679306809>

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: 137

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: B ([コメントを發表する](#))

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: 138

高可用性では、どの情報がHAデータリンク経由で転送されますか？

- A. HA状態情報
- B. 鼓動
- C. セッション情報
- D. ユーザーID情報

正解: C ([コメントを發表する](#))

質問: 139

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](#))

Palo Alto Networks Panorama 7.0 Administrator's Guide \*77 Manage Firewalls Manage Device Groups Manage Device GroupspAdd a Device Group Create a Device Group Hierarchy Create Objects for Use in Shared or Device Group Policy Revert to Inherited Object Values Manage Unused Shared ObjectspManage Precedence of Inherited ObjectspMove or Clone a Policy Rule or Object to a Different Device Group Select a URL Filtering Vendor on Panorama Push a Policy Rule to a Subset of FirewallspManage the Rule Hierarchy Add a Device Group After 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-panorama-management/migrate-a-firewall-ha-pair-to-panorama-management>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleOCAS>

質問: 140

HAプロモーションの保留時間を最もよく表すものは何ですか？

- A. 隣接デバイスの時折のフラッピングによるHAフェイルオーバーを回避するために推奨される時間
- B. 両方のファイアウォールで同じリンク/パスモニターの障害が同時に発生した場合にフェイルオーバーを回避するために推奨される時間
- C. HAピアとの通信が失われた後、パッシブファイアウォールがアクティブファイアウォールとして引き継ぐまで待機する時間
- D. デバイスの優先度が低いパッシブファイアウォールが、ファイアウォールが再び機能している場合にアクティブファイアウォールとして引き継ぐ前に待機する時間

正解: C ([コメントを發表する](#))

質問: 141

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. Antivirus
- B. Content-ID
- C. User-ID

## D. Applications and Threats

正解: ([正解を表示します](#))

### 質問: 142

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](#))

<https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and-reporting>

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIKFCA0>

"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: 143

管理者は、信頼できるインターフェイスでファイアウォールにアクセスする必要があります。Web UIへの証明書ベースの安全な認証を構成するために必要な2つのコンポーネントはどれですか？ 2つ選択してください)

- A. SSL/TLSサービスプロファイル
- B. サーバー証明書
- C. SSHサービスプロファイル
- D. 証明書プロファイル

正解: ([正解を表示します](#))

### 質問: 144

PAN-OS 8.0でどの認証方式が追加されたかをサポートしていますか？

- A. RADIUS
- B. LDAP

- C. Diameter
- D. TACACS+

正解: ([正解を表示します](#))

<https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1>

**質問: 145**

管理者が着信の復号化に問題が発生しました。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. SSLをターゲットサーバに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"を有効にして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

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/decryption/configure-ssl-inbound-inspection.html>

**質問: 146**

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. 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。
- B. 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。
- 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. 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。
- F. 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。

正解: **A,B,E** ([コメントを發表する](#))

**質問: 147**

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. 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。
- C. 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。
- D. ルールの使用法ヒットカウンタがリセットされます。

正解: ([正解を表示します](#))

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIVICA0>

"Notice how the rules looks after selecting "Highlight Unused Rules." You can now see exactly what rules have and have not been used since the last reboot."

質問: 148

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. / 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。
- B. 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
- 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. 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。
- E. 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-Seriesファイアウォールを自動展開できます。

正解: C,E ([コメントを發表する](#))

<https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/bootstrap-the-vm-series-firewall-in-aws.html>

質問: 149

SYNフラッド保護のしきい値を構成できる2つのファイアウォールコンポーネントはどれですか？ (2つ選択してください)

- A. DoS保護ポリシー
- B. QoSプロファイル
- C. ゾーン保護プロファイル
- D. DoS保護プロファイル

正解: ([正解を表示します](#))

Flood Attack Protection

Zone Protection Profiles protect against of five types of floods:

- \* SYN (TCP)
- \* UDP
- \* ICMP
- \* ICMPv6
- \* Other IP

質問: 150

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てから、検査ツールのセキュリティチェーンにクリアテキストとして送信します。
- B. 未知の暗号スイートを強制的に復号化する
- C. IPsecトンネル内の検査トラフィック
- D. 検査ツールのセキュリティチェーンに送信する前に、SSLトラフィックをより弱い暗号に減らす

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/decryption-features/decryption-broker>

質問: 151

ポリシールールUUIDはどのような利点を提供しますか？

- A. ポリシーアクションをスケジュールするための機能
- B. ポリシーでのユーザーIPマッピングとグループの使用
- C. デバイスグループ間のポリシーの複製
- D. ポリシーの存続期間にわたる監査証跡

正解: ([正解を表示します](#))

<https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-new-features/management-features/universally-unique-identifiers-for-policy-rules.html>

有効的なPCNSE-JPN問題集はJPNTTest.com提供され、PCNSE-JPN試験に合格することに役に立ちます！JPNTTest.comは今最新PCNSE-JPN試験問題集を提供します。JPNTTest.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: 152

管理者は、管理者の自宅でIPSec VPNをCisco ASAに設定し、接続を完了する問題を経験しています。コマンド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. パブリックIPアドレスは、Palo Alto NetworksファイアウォールとASAの両方で一致しません。
- B. Palo Alto NetworksファイアウォールのプロキシIDがASAの設定と一致しません。
- C. デッドピア検出の設定が、Palo Alto NetworksファイアウォールとASAの間で一致しません
- D. 共有秘密はPalo Alto NetworksファイアウォールとASAの間で一致しません。

正解: ([正解を表示します](#))

質問: 153

DoS保護とゾーン保護プロファイルについて正しい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. ゾーン保護プロファイルは入力ゾーンを保護します
- B. ゾーン保護プロファイルは出力ゾーンを保護します
- C. DoS保護プロファイルはパケットベースであり、署名ベースではありません
- D. DoS保護プロファイルはセキュリティポリシールールにリンクされています

正解: ([正解を表示します](#))

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

#### 質問: 154

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。
- B. 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。
- 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。

正解: ([正解を表示します](#))

#### 質問: 155

IPv6ルーティングプロトコルはどれですか？

- A. OSPv3
- B. BGP NG
- C. RIPv3
- D. OSPFv3

正解: D ([コメントを發表する](#))

#### 質問: 156

ethernet1 / 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 ethernet1 / 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

正解: D ([コメントを發表する](#))

Example output:

```
> show system state filter-pretty sys.s1.p1.phy
```

```
sys.s1.p1.phy: {  
link-partner: {}  
media: CAT5,  
type: Ethernet,  
}
```

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC>

有効的な**PCNSE-JPN**問題集はJPNTTest.com提供され、**PCNSE-JPN**試験に合格することに役に立ちます！JPNTTest.comは今最新**PCNSE-JPN**試験問題集を提供します。JPNTTest.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**」