PaloAltoNetworks.PCNSE.v2020-03-01.q86

試験コード：	PCNSE
試験名称：	Palo Alto Networks Certified Network Security Engineer Exam
認証ベンダー：	Palo Alto Networks
無料問題の数：	86
バージョン：	v2020-03-01
ページの閲覧量：	1308
問題集の閲覧量：	31042

https://www.jpnshiken.com/shiken/PaloAltoNetworks.PCNSE.v2020-03-01.q86.html

質問: **1**
サーバーからクライアントへのフローのみのウイルス対策およびスパイウェア対策スキャンを無効にするセキュリティポリシールールの構成オプションはどれですか？
A. HIPプロファイルを無効にします
B. アプリケーションオーバーライドの適用
C. サーバー応答検査を無効にする
D. サーバーIPセキュリティポリシーの例外を追加
正解: **(**正解を表示します**)**

質問: **2**
ネットワーク管理者は、パノラマを使用して、セキュリティポリシーをブランチオフィスの管理対象ファイアウォールにプッシュします。ブランチオフィスサイトの管理者がこれらの製品を上書きする場合、Panoramaでどのポリシータイプを設定する必要がありますか？
A. 暗黙のルール
B. 事前ルール
C. 投稿ルール
D. 明示的なルール
正解: **(**正解を表示します**)**

質問: **3**
管理者が管理者の自宅でCisco ASAにIPSec VPNを設定しており、接続の完了に関する問題が発生しています。コマンドからの出力は次のとおりです。
この問題の原因は何ですか？
A. デッドピア検出設定は、Palo Alto NetworksファイアウォールとASAの間で一致しません。
B. 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。
C. Palo Alto Networksファイアウォールのプロキシidは、ASAの設定と一致しません。
D. 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。
正解: **(**正解を表示します**)**

質問: **4**

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、パケットがどの種類の一致を使用して既存のセッションの一部であるかを判断しますか？
A. 6タプル一致：
ソースIPアドレス、宛先IPアドレス、ソースポート、宛先ポート、プロトコル、およびソースセキュリティゾーン
B. 5タプル一致：
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タプル一致：
ソースIPアドレス、宛先IPアドレス、ソースポート、宛先ポート、ソースユーザー、URLカテゴリ、およびソースセキュリティゾーン
D. 9タプル一致：
送信元IPアドレス、送信先IPアドレス、送信元ポート、送信先ポート、送信元ユーザー、送信元セキュリティゾーン、送信先セキュリティゾーン、アプリケーション、およびURLカテゴリ
正解: (正解を表示します)
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVECA0

質問: **5**
「復号化なし」アクションで復号化プロファイルを復号化ポリシールールに割り当てると、2つの利点がありますか？（2つ選択してください。）
A. 有効期限が切れた証明書を持つセッションをブロックする
B. クライアント認証でセッションをブロックする
C. サポートされていない暗号スイートでセッションをブロックします
D. 信頼できない発行者とのセッションをブロックする
E. 資格情報フィッシングをブロックする
正解: (正解を表示します)
説明
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-exce

質問: **6**
管理者が、WildFire分析のために新たに発見したスパイウェアを提出したところです。スパイウェアは、ユーザーの知らないうちに動作を受動的に監視します。
WildFireから予想される評決は何ですか？
A. グレーウェア
B. マルウェア
C. スパイウェア
D. フィッシング
正解: (正解を表示します)
説明

Wildfireの判定は次のようになります4-Phishing
https://www.paloaltonetworks.com/documentation/80/wildfire
/ wf_admin / wildfire-overview / wildfire-concepts / verdicts

質問: **7**
ネットワーク管理者は、大規模VPNソリューションを展開したいと考えています。ネットワーク管理者がGlobalProtect Satelliteソリューションを選択しました。この構成は複数のリモートオフィスに展開する必要があり、ネットワーク管理者はPanoramaを使用して構成を展開することにしました。
これはどのように達成すべきですか？
A. 適切なIKEゲートウェイ設定でテンプレートを作成します
B. 適切なIPSecトンネル設定でテンプレートを作成します
C. 適切なIPSecトンネル設定でデバイスグループを作成します
D. 適切なIKEゲートウェイ設定でデバイスグループを作成します
正解: **(**正解を表示します**)**

質問: **8**
「ドメイン資格情報フィルター」方式を使用した資格情報フィッシング防止用にファイアウォールが構成されている場合、どのログインが資格情報の盗難として検出されますか？
A. ログインしているユーザーのIPアドレスへのマッピング。
B. 有効な企業ユーザー名に一致するユーザー名の最初の4文字。
C. 同じユーザーの企業ユーザー名とパスワードを使用します。
D. 有効な企業ユーザー名をマーチングします。
正解: **(**正解を表示します**)**
説明
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-new-features/content-inspection-features/credential- entionリファレンス：
https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content-inspection-features/crede phishing-prevention

質問: **9**
ファイアウォールは、MineMeldからIPアドレスをダウンロードしていません。画像に基づいて、おそらく何が間違っていますか？
A. クライアント証明書を含む証明書プロファイルを選択する必要があります。
B. 外部動的リストはSSL接続をサポートしていません。
C. ソースアドレスは、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。
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**)**

質問: **10**
展示を参照してください。
管理者がDNATを使用して、2つのサーバーを単一のパブリックIPアドレスにマップしています。ホストA（10.1.1.100）がHTTPトラフィックを受信し、ホストB（10.1.1.101）がSSHトラフィックを受信するアプリケーションに基づいて、トラフィックは特定のサーバーにステアリングされます。この構成を実行するセキュリティポリシールールは2つですか？（2つ選択してください。）
A. Untrust（Any）to Untrust（10.1.1.1）、web-browsing -Allow
B. Untrust（Any）to Untrust（10.1.1.1）、ssh -Allow
C. DMZ（10.1.1.1）に対するUntrust（Any）、Webブラウズ許可
D. Untrust（Any）to DMZ（10.1.1.1）、ssh -Allow
E. DMZ（10.1.1.100.10.1.1.101）、ssh、web-browsingに対するUntrust（Any）-Allow
正解: **(**正解を表示します**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/networking/nat/nat-configuration-examples/destinat

質問: **11**
どのパノラマ管理者タイプで、少なくとも1つのアクセスドメインの構成が必要ですか？（2つ選択）
A. テンプレート管理者
B. ダイナミック
C. ロールベース
D. デバイスグループ
E. カスタムパノラマ管理
正解: **(**正解を表示します**)**

質問: **12**
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トグしますか？
A. ログ
B. デフォルト
C. 許可
D. アラート
正解: **D (**コメントを発表する**)**

質問: **13**
管理者がPalo Alto Networks NGFWにログインし、WebUIに[ポリシー]タブがないことを報告します。[ポリシー]タブが表示されない原因はどのプロファイルですか？
A. 承認
B. WebUI

C. 認証
D. 管理者ロール
正解: (正解を表示します)

質問: **14**
管理者が、YouTubeアプリケーションの最大許容帯域幅を制限するQoSポリシールールとQoSプロファイルを構成しました。ただし、YouTubeは、設定された最大帯域幅割り当てを超えて消費しています。
QoSを有効にするには、どの構成手順を構成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モニターを有効にする
C. QoSインターフェイスを有効にします
D. インターフェイス管理プロファイルでQoSを有効にします。
正解: (正解を表示します)
説明
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/network/network-qos/qos-interface-sett

質問: **15**
Panoramaは、最大ストレージ容量に達したときに受信ログをどのように処理しますか？
A. ストレージ容量がいっぱいになると、Panoramaは受信ログを破棄します。
B. 追加のストレージスペースのライセンスが適用されるまで、パノラマはログの受け入れを停止します
C. パノラマは、ストレージスペースをクリーンにするために再起動するまでログの受け入れを停止します。
D. Panoramaは古いログを自動的に削除して、新しいログ用のスペースを作成します。
正解: (正解を表示します)
説明
https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/determ

質問: **16**
管理者は、DMZとコアネットワークの間にNGFWを実装する必要があります。2つの環境間のEIGRPルーティングが必要です。どのビジネスタイプがこのビジネス要件をサポートしますか？
A. レイヤー3インターフェイス、ただし接続された仮想ルーターでEIGRPを構成
B. IPsecトンネルでEIGRPルーティングを終了するトンネルインターフェイス（SVPNおよびEIGRPプロトコルをサポートするGlobalProtectライセンスを使用）
C. EIGRPルーティングがコアとDMZの間に残ることを許可する仮想ワイヤインターフェイス
D. レイヤー3または集約イーサネットインターフェース、ただしサブインターフェースのみでEIGRPを構成

正解: (正解を表示します)

質問: **17**
同社のパノラマサーバー（IP 10.10.10.5）は、最近導入されたファイアウォールを管理できません。ファイアウォールの専用管理ポートは、管理ネットワークへの接続に使用されています。
新しいファイアウォールのCLIからこの問題をトラブルシューティングするために使用できる2つのコマンドはどれですか？（2つ選択）
A. パノラマステータスを表示
B. 10.10.10.5に一致するarpをすべて表示
C. topdump filter "ホスト10.10.10.5
D. パノラマ接続10.10.10.5のテスト
E. データプレーンパケットダイアグセットキャプチャのデバッグ
正解: (正解を表示します)

質問: **18**
展示を参照してください。
管理者は、Panorama上のPalo Alto Networks NGFWのトラフィックログを見ることができません。構成の問題はファイアウォール側にあるようです。構成が正しいかどうかを確認するために、Palo Alto Networks NGFWで最適な場所はどこですか？ A）
B）
C）
D）
A. オプションA
B. オプションB
C. オプションC
D. オプションD
正解: (正解を表示します)
説明
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forward

質問: **19**

分散ログコレクションの展開には、専用のログコレクターがあります。開発者は、ログをコレクターグループに送信する代わりに、パノラマにログを送信するデバイスを必要とします。
最初に何をすべきですか？
A. 以前の構成に戻す
B. 管理インターフェースからケーブルを取り外し、Log Collectorをリロードしてから、そのケーブルを再接続します
C. コレクターグループからデバイスを削除します
D. パロアルトネットワークスのサポートチームに連絡して、カーネルモードコマンドを入力して調整を許可します
正解: **(**正解を表示します**)**

質問: **20**
次の画像に基づいて、
ルート証明書、中間証明書、エンドユーザー証明書の正しいパスは何ですか？
A. シマンテック> VeriSign> Palo Alto Networks
B. VeriSign>シマンテック> Palo Alto Networks
C. パロアルトネットワークス>シマンテック> VeriSign
D. VeriSign> Palo Alto Networks>シマンテック
正解: **A (**コメントを発表する**)**

質問: **21**
ロギングインフラストラクチャは、毎秒10,000を超えるログを処理する必要がある場合があります。
専用のログコレクター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 のみのパノラマ仮想アプライアンス
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**)**
説明
（https://live.paloaltonetworks.com/t5/Management-Articles/Panorama-Sizing-and-Design-Guide/ta-p/72181）

質問: **22**
新しいセキュリティポリシールールを作成するとき、どのフィールドがオプションですか？
A. アクション
B. 宛先ゾーン
C. 名前
D. 説明
E. ソースゾーン

正解: (正解を表示します)

質問: **23**
GlobalProtectポータルインターフェイスとIPアドレスが設定されました。GlobalPortect Portalのネットワーク設定の構成を完了するには、他にどの値を定義する必要がありますか？
A. サーバー証明書
B. クライアント証明書
C. 認証プロファイル
D. 証明書プロファイル
正解: **A** (コメントを発表する)
説明
（https ://live.paloaltonetworks。
com / t5 / Configuration-Articles / How-to-Configure-GlobalProtect / ta-p / 58351）

質問: **24**
管理者は、ローカルのオンプレミスラボ環境に100個の仮想ファイアウォールを作成するように求められています（
"クラウド"）。ブートストラップは、このタスクを実行する最も適切な方法です。
オンプレミスの仮想環境でのブートストラップパッケージの展開を説明するオプションはどれですか？
A. USBスティックのconfig-driveを使用します。
B. ISOでS3バケットを使用します。
C. 仮想ハードディスク（VHD）を作成して接続します。
D. ISOで仮想CD-ROMを使用します。
正解: **D** (コメントを発表する)
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/management-features/bootstrapp firewalls-for-rapid-deployment.html

質問: **25**
いくつかのオフィスは、静的IPv4ルートを使用してVPNで接続されています。管理者は、静的ルーティングを置き換えるためにOSPFの実装を任されています。
この目標を達成するにはどのステップが必要ですか？
A. 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
B. 各サイトで新しいVPNゾーンを作成して、各VPN接続を終了します
C. 各トンネルインターフェイスでOSPFv3を有効にし、エリアID 0.0.0.0を使用します
D. 各サイトの各トンネルインターフェイスにIPアドレスを割り当てます
正解: (正解を表示します)

質問: **26**
Company.comには、Palo Alto Networksデバイスが正しく識別しない社内アプリケーションがあります。脅威管理チームのメンバーは、この社内アプリケーションは非常に機密性が高く、識別され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ると述べています。パロアルトネットワークスのデバイスでこのトラフィックにすぐに対処するには、company.comを使用する方法はどれですか？
A. 公式のアプリケーション署名がパロアルトネットワークスから提供されるまで待ちます。
B. 社内アプリケーショントラフィックの一意の識別子に一致する署名を持つカスタムアプリケーションを作成します
C. 社内アプリケーションのニーズを満たすために、最も近い参照先アプリケーションのセッションタイマー設定を変更します
D. 署名なしのカスタムアプリケーションを作成し、トラフィックのソース、宛先、宛先ポート/プロトコル、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: **27**
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およびサービスとして表示されますか？
A. Webブラウジングと443
B. SSLおよび80
C. SSLおよび443
D. Webブラウジングと80
正解: **A (**コメントを発表する**)**
説明
SSL復号化は、そうでなければ暗号化されるトラフィックの可視性を提供することになっていることを知っています。したがって、復号化されたトラフィックは、SSLとしてではなく、Web閲覧、facebook-baseなどの基礎となるアプリケーションとして識別されると予想されます。

質問: **28**
セキュリティポリシールールは、脆弱性保護プロファイルと 拒否」のアクションで構成されます。これにより、一致したトラフィックの構成はどのアクションになりますか？
A. 構成が無効です。アクションが次のように設定されている場合、プロファイル設定セクションはグレー表示されます。
 拒否」。
B. 脆弱性の署名が検出されない限り、構成は一致したセッションを許可します。の
 拒否」アクションは、関連する脆弱性保護プロファイルで定義された重大度ごとに定義されたアクションに優先します。

C. 構成が無効です。これにより、ファイアウォールはこのセキュリティポリシールールをスキップします。コミット中に警告が表示されます。
D. 設定は有効です。ファイアウォールは一致したセッションを拒否します。セキュリティポリシールールアクションが「拒否」に設定されている場合、設定済みのセキュリティプロファイルは効果がありません。
正解: **(**正解を表示します**)**
説明
「セキュリティプロファイルは、トラフィックフローの一致基準では使用されません。セキュリティプロファイルは、アプリケーションまたはカテゴリがセキュリティポリシーで許可された後にトラフィックをスキャンするために適用されます。」
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/policy/security-profiles.html#

質問: **29**
復号化証明書検証エラーを受け取る正当な理由ではないのはどれですか？
A. 不明な証明書ステータス
B. サポートされていないHSM
C. 信頼できない発行者
D. クライアント認証
正解: **B (**コメントを発表する**)**

質問: **30**
ネットワーク設計の変更には、管理インターフェイスではなくデータプレーンインターフェイスアドレスからPalo Alto Updatesへのアクセスを開始するために、既存のファイアウォールが必要です。
どの構成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. 認証プロファイル
C. 管理プロファイル
D. サービスルート
正解: **D (**コメントを発表する**)**

質問: **31**
ファイアウォール管理者は、Palo Alto Networksファイアウォールを通過するトラフィックの問題をトラブルシューティングしています。適切なパケットフィルターを構成した後、トラフィックに関連付けられたグローバルカウンターを表示する方法はどれですか？
A. CLIから、show counter global filter packet-filter yesコマンドを発行します。
B. GUIから、モニタータブの下にあるグローバルカウンターの表示を選択します。
C. CLIから、show counter global filter pcap yesコマンドを発行します。
D. CLIから、入力インターフェースに対してshow counter interfaceコマンドを発行します。
正解: **A (**コメントを発表する**)**

質問: **32**
Palo Alto NetworksファイアウォールをAutoFocusに接続するには、どの設定を有効にする必要がありますか？
A. デバイス>セットアップ>サービス>オートフォーカス
B. デバイス>セットアップ>管理>オートフォーカス
C. AutoFocusは、Palo Alto Networks NGFWでデフォルトで有効になっています
D. デバイス>セットアップ> WildFire>オートフォーカス
E. デバイス>セットアップ>管理>ログとレポートの設定
正解: **B** (コメントを発表する)
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-inte

質問: **33**
構成ファイルをバックアップして保存するとき、ファイアウォールのみを使用して何が達成され、Panoramaでは使用できませんか？
A. 設定バージョンのロード
B. 名前付き構成スナップショットをロード
C. 候補の構成を保存
D. デバイス状態のエクスポート
正解: **D** (コメントを発表する)

質問: **34**
ネットワークエンジニアが、ファイアウォールのvr1を介して98.139.183.24に達する問題の報告を復活させました。このファイアウォールのルーティングテーブルは広範で複雑です。
どのCLIコマンドが問題の特定に役立ちますか？
A. テストルーティングfib-lookup ip 98.139.183.24 virtual-router vr1
B. ルーティングルートタイプの静的宛先98.139.183.24を表示
C. ルーティングfib仮想ルーターvr1のテスト
D. ルーティングインターフェイスを表示
正解: **A** (コメントを発表する)

質問: **35**
WildFireが分析されたサンプルに提供できる3つの可能な判定は何ですか？ （3つ選択）
A. クリーン
B. ベンギン
C. アドウェア
D. 疑わしい
E. グレーウェア
F. マルウェア
正解: **(**正解を表示します**)**
説明
https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayw

質問: **36**
パケットキャプチャ用にファイアウォールを構成する場合、有効なステージタイプは何ですか？
A. 受信、管理、送信、およびドロップ
B. 管理、送信、および非同期の受信
C. receive、firewall、send、およびnon-syn
D. 受信、ファイアウォール、送信、およびドロップ
正解: **(**正解を表示します**)**

質問: **37**
ファイアウォール管理者がNGFWを介して現在アクティブなトラフィックに関する詳細を表示できるメニュー項目はどれですか？
A. システムログ
B. セッションブラウザ
C. アプリの範囲
D. ACC
正解: **(**正解を表示します**)**

質問: **38**
展示ボタンをクリックします
管理者は、ビットトレントアクティビティの大幅な増加に気付きました。管理者は、トラフィックが会社のどこに向かっている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. bittorrentリンクを右クリックして、コンテキストメニューから[値]を選択します
B. bittorrentトラフィック用のローカルフィルターを作成し、トラフィックログを表示します。
C. bittorrentトラフィック用のグローバルフィルターを作成し、トラフィックログを表示します。

D. bittorrentアプリケーションの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
正解: **(**正解を表示します**)**

質問: **39**
パケットフロープロセスでコンテンツ検査はいつ実行されますか？
A. アプリケーションが識別された後
B. セッション検索の前
C. パケット転送プロセスの前
D. SSLプロキシがパケットを再暗号化した後
正解: **C (**コメントを発表する**)**
参照：
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

質問: **40**
管理者のPalo Alto Networks NGFW向けのVPNトラフィックは、インターセプターによって悪意を持って傍受され、再送信されています。VPNトンネルを作成する場合、この悪意のある動作を防ぐためにどの保護プロファイルを有効にできますか？
A. ゾーン保護
B. DoS保護
C. Webアプリケーション
D. リプレイ
正解: **(**正解を表示します**)**
説明
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec

質問: **41**
どの3つのフィールドをpcapフィルターに含めることができますか？ （3つ選択）
A. 出力インターフェース
B. 送信元IP
C. ルール番号
D. 宛先IP
E. 入力インターフェース
正解: **B,C,D (**コメントを発表する**)**
説明
（https://live.paloaltonetworks.com/t5/Featured-Articles/Getting-Started-Packet-Capture/ta-p/72069）

質問: **42**
別紙を参照してください：
ファイアウォールには、3つのPDFルールと、デフォルトVRで設定された172.29.19.1のネクストホップを持つデフォルトルートがあります。XXという名前のユーザーは、192.168.101.10のIPアドレスを持つPCになります。
彼は172.16.10.29へのHTTPS接続を確立します。
Wills PCからのHTTPSトラフィックのネクストホップIPアドレスは何ですか。
A. 172.20.30.1
B. 172.20.20.1
C. 172.20.10.1
D. 172.20.40.1
正解: **(**正解を表示します**)**

質問: **43**
管理者は、NGFW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。以下が発生しています：
*ファイアウォールには、e1 / 1を介したインターネット接続があります。
*デフォルトのセキュリティルールと、任意のゾーンとの間で送受信されるすべてのSSLおよびWeb閲覧トラフィックを許可するセキュリティルール。
*サービスルートが設定され、e1 / 1から更新トラフィックが供給されます。
*更新が実行されると、システムログに通信エラーが表示されます。
*ダウンロードは完了しません。
ファイアウォールがPAN-OSソフトウェアの現在のバージョンをダウンロードできるようにするには、何を構成する必要がありますか？
A. PAN-OSソフトウェアの時限ダウンロードのスケジューラー
B. 静的ルートポインティングアプリケーションの更新サーバーへのPaloAlto-updates
C. 解決に使用するファイアウォールのDNS設定
D. PaloAlto-updatesをアプリケーションとして許可するセキュリティポリシールール
正解: **(**正解を表示します**)**

質問: **44**
いくつかのオフィスは、静的IPV4ルートを使用してVPNで接続されています。管理者は、静的ルーティングを置き換えるためにOSPFの実装を任されています。
この目標を達成するにはどのステップが必要ですか？
A. 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
B. 各サイトに新しいVPNゾーンを作成して、各VPN接続を終了します
C. 各サイトの各トンネルインターフェイスにIPアドレスを割り当てます
D. 各トンネルインターフェイスでOSPFv3を有効にし、エリアID 0.0.0.0を使用します
正解: **(**正解を表示します**)**

質問: **45**
PAN-OSでサポートされている4つのNGFW多要素認証要素はどれですか？ 4つ選択してください。）
A. ショートメッセージサービス
B. プッシュ
C. ユーザーログオン
D. 音声
E. SSHキー
F. ワンタイムパスワード
正解: **(**正解を表示します**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-auth

質問: **46**
ローカルファイアウォールで対応する管理者アカウントを定義せずに、管理者がPalo Alto Networks NGFWに対して管理者を認証するために使用できる認証サービスはどれですか？ 3つ選択してください。）
A. Kerberos
B. PAP
C. SAML
D. TACACS +
E. RADIUS
F. LDAP
正解: **(**正解を表示します**)**
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat管理アカウントは、外部SAML、TACACS +、またはRADIUSサーバーで定義されます。サーバーは、認証と承認の両方を実行します。許可のために、TACACS +またはRADIUSサーバーでベンダー固有の属性（VSA）を定義するか、SAMLサーバーでSAML属性を定義します。PAN-OSは、管理者ロール、アクセスドメイン、ユーザーグループ、およびファイアウォールで定義した仮想システムに属性をマップします。詳細については、以下を参照してください。
SAML認証の構成TACACS +認証の構成RADIUS認証の構成

セス、https://www.jpntest.com/shiken/PCNSE-mondaishu　375問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **47**
管理者は、Palo Alto Networks NGFWの仮想ルーターでBGPを有効にしましたが、新しいルートが仮想ルーターに入力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でトラフィックpcapを実行して、BGPの問題を確認します。
C. ランタイム統計を表示し、BGP構成の問題を探します。
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**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEWCA0

質問: **48**
Panoramaでポリシーを定義するときに使用できる3つのルールタイプはどれですか？　3つ選択してください。）
A. 事前ルール
B. 投稿ルール
C. デフォルトのルール
D. ステルスルール
E. ルールのクリーンアップ
正解: **A,B,C (**コメントを発表する**)**
説明
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/panorama-web-interface/definin

質問: **49**
WebサーバーはDMZでホストされ、サーバーはTCPポート8080でのみ着信接続をリッスンするように構成されています。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して、サーバ。
tcp / 8080のシンサーバーへのクリアテキストWebブラウズトラフィックのみを許可するように構成する必要があるアプリケーションとサービス。
A. アプリケーション：Webブラウジング。サービス：application-default
B. アプリケーション：Webブラウジング。サービス：service-https
C. アプリケーション：ssl;サービス：任意
D. アプリケーション：Webブラウジング。サービス：（宛先TCPポート8080のカスタム）
正解: **D (**コメントを発表する**)**

説明
FWをチェックインする場合、Webブラウジングのデフォルトポートはtcp 80なので、カスタムアプリが必要になります。
admin @ PA-LAB-01＃show defined web-browsing web-browsing {category general-internet;サブカテゴリのインターネットユーティリティ。ブラウザーベースのテクノロジー。分析 'Webブラウジングは進化し続けています。最初は単純にHTML形式の情報を表示するために使用されていたWebブラウザーがクライアントになり、ユーザーはそれを介して、単純な情報ブラウジングをはるかに超える機能を提供する新しいアプリケーションにアクセスできます。これらのアプリケーションには、Webメール、インスタントメッセージング、ストリーミングメディア、Web会議、ブログ、ファイル共有、その他のソーシャルネットワーキングアプリケーションが含まれます。プレーンなWebブラウジングアクティビティの多くは、他のすべてのアプリケーションによって効果的に隠されています。}デフォルト{port tcp / 80; } tunnel-applications http-proxy;リスク4; }
[編集]

質問: **50**
クライアントのデータセンターには機密性の高いアプリケーションサーバーがあり、サービス拒否攻撃によるセッションフラッディングが特に懸念されます。
単一のIPアドレスから発生するセッションフラッドからこのサーバーを保護するために、Palo Alto Networks NGFWをどのように構成できますか？
A. スパイウェア対策プロファイルを追加して、攻撃IPアドレスをブロックします
B. QoSプロファイルを追加して、着信要求を調整します
C. カスタムApp-IDを定義して、正当なアプリケーショントラフィックのみがサーバーに到達するようにします
D. 調整されたDoS保護プロファイルを追加する
正解: **D (**コメントを発表する**)**

質問: **51**
ファイアウォールを管理するために新しいデバイスグループが作成されるたびに、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どれですか？
A. グローバル
B. マスター
C. 共有
D. ユニバーサル
正解: **C (**コメントを発表する**)**

質問: **52**
顧客がトンネルインターフェイスを使用してサイト間VPNをセットアップしたいですか？
トンネルインターフェイスの名前付けに適した2つの形式はどれですか？ 2つ選択してください。）
A. vpn-tunne.1

B. トンネル。1
C. トンネル1025
D. Vpn-tunnel.1024
正解: **(**正解を表示します**)**

質問: **53**
ファイアウォールがリブートされたときの、未使用ルールの強調表示とルール使用ヒットカウンターの2つの動作の違いは何ですか？　2つ選択してください。）
A. ルール使用ヒットカウンターがリセットされます。
B. 未使用のルールを強調表示すると、ゼロのルールが強調表示されます。
C. 未使用のルールを強調表示すると、すべてのルールが強調表示されます。
D. ルール使用ヒットカウンターはリセットされません
正解: **(**正解を表示します**)**

質問: **54**
新しいPalo Alto Networks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化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構成する場合
B. GlobalProtectポータルを構成する場合
C. ユーザーアクティビティレポートを構成する場合
D. アンチウイルスの動的更新を構成する場合
正解: **(**正解を表示します**)**

質問: **55**
どのインターフェイス構成が特定のVLAN IDを受け入れますか？
A. トランクインターフェイス
B. アクセスインターフェイス
C. サブインターフェース
D. タブモード
正解: **(**正解を表示します**)**

質問: **56**
管理者には、復号化されたトラフィックをPalo Alto Networks NGFWからサードパーティのディープレベルのパケット検査アプライアンスにエクスポートする必要があります。
要件を満たすには、どのインターフェイスタイプとライセンス機能が必要ですか？
A. 脅威分析ライセンスを備えた復号化ミラーインターフェイス
B. 復号化ポートエクスポートライセンスを使用した仮想ワイヤインターフェイス
C. 復号化ポートミラーライセンスのインターフェイスをタップします
D. 復号化ミラーインターフェースと関連する復号化ポートミラーライセンス
正解: **(**正解を表示します**)**

参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/decryption-mirroring
「復号化ミラーリングを有効にする前に、復号化ポートミラーライセンスを取得してインストールする必要があります。ライセンスは無料で、次の手順で説明するようにサポートポータルからアクティブ化できます。復号化ポートミラーライセンスをインストールして再起動すると、ファイアウォールでは、復号化ポートミラーリングを有効にできます。」

質問: **57**
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。
その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の情報が含まれますか？ （2つ選択してください。）
A. dp-monitor .log
B. authdログ
C. システムログ
D. msログ
E. トラフィックログ
正解: **B,C (**コメントを発表する**)**

質問: **58**
Panoramaの外部のホストに候補または実行構成をコピーするにはどうすればよいですか？
A. 実行中の構成をコミットします。
B. 構成スナップショットを保存します。
C. 候補の構成を保存します。
D. 名前付き構成スナップショットをエクスポートします。
正解: **(**正解を表示します**)**
参照：
https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/administer-panorama/bapanorama-and-firewall-configurations

質問: **59**
ICMPパケットの送信元アドレスは何ですか？
A. 10.46.64.94
B. 10.30.0.93
C. 192.168.93.1
D. 10.46.72.93
正解: **(**正解を表示します**)**

質問: **60**
どのCLIコマンドを使用してtcpdumpキャプチャをエクスポートできますか？

A. mgmt.pcapから<username @ host :path>へのscp export tcpdump
B. scmtはmgmt.pcapからmgmt-pcapを<username @ host :path>に抽出します
C. mgmt.pcapから<username @ host :path>へのmgp-pcapのエクスポート
D. mgmt.-pcapをダウンロードします
正解: (正解を表示します)
参照：
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-I p / 55415

質問: **61**
次の表を考えます。
ファイアウォールのどの構成変更により、ファイアウォールの次のホップとして10.66.24.88が使用されます
192.168.93.0/30ネットワーク？
A. RIPのメトリックをそのOSPF Ext。よりも低く設定します。
B. RIPのメトリックをOSPF Intのメトリックよりも高く設定します。
C. RIPの管理距離をOSPF Intの管理距離よりも低く設定します。
D. RIPの管理距離をOSPF Extの管理距離よりも高く設定します。
正解: (正解を表示します)

質問: **62**
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ethernet1 / 4に通過できないと判断されます。問題の原因は何ですか？
A. DNSがファイアウォールで適切に構成されていません
B. DHCPは自動に設定されています。
C. インターフェースethernet1 / 3はレイヤー2モードで、インターフェースethernet1 / 4はレイヤー3モードです。
D. インターフェースethernet1 / 3およびethernet1 / 4は仮想ワイヤモードです。
正解: (正解を表示します)

質問: **63**

パケットフロープロセス中、アプリケーション識別で実行される2つのプロセスはどれですか？（2つ選択してください。）
A. パターンベースのアプリケーション識別
B. アプリケーションオーバーライドポリシーの一致
C. コンテンツ検査から変更されたアプリケーション
D. セッションアプリケーションが識別されました。
正解: **(**正解を表示します**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0
http://live.paloaltonetworks.com//t5/image/serverpage/image-id/12862i950F549C7D4E6309

質問: **64**
トラフィックログのセッションは、アプリケーションを「不完全」として報告しています。「不完全」とはどういう意味ですか？
A. 3ウェイTCPハンドシェイクが観察されましたが、アプリケーションを識別できませんでした。
B. スリーウェイTCPハンドシェイクは完了しませんでした。
C. トラフィックがUDPを通過しているため、アプリケーションを識別できませんでした。
D. データは受信されましたが、App-IDが適用される前に拒否ポリシーが適用されたため、すぐに破棄されました。
正解: **B (**コメントを発表する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

質問: **65**
ファイル共有アプリケーションが許可されており、このアプリケーションの用途が誰にもわかりません。
このアプリケーションをどのようにブロックする必要がありますか？
A. 既知のすべての内部カスタムアプリケーションをブロックします
B. セキュリティポリシーを使用して、許可されていないアプリケーションをすべてブロックします
C. レイヤー4およびレイヤー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します
D. レイヤー4およびレイヤー7攻撃をブロックするWildFire分析プロファイルを作成する
正解: **(**正解を表示します**)**

質問: **66**
管理者は、どのCLIコマンドを使用して、稼働時間、PAN-OSバージョン、シリアル番号など、ファイアウォールに関する詳細を表示できますか？
A. システムの詳細をデバッグします
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: **C (**コメントを発表する**)**
参照：
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/technical-documentation/pan-os-60/PAN- CLI-ref.pdf

質問: **67**
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. アクティブ
B. 機能的
C. 保留中
D. パッシブ
E. 一時停止
正解: **A,D,E (**コメントを発表する**)**
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-firewall-states

質問: **68**
クライアントのデータセンターには機密性の高いアプリケーションサーバーがあり、分散型サービス拒否攻撃によるリソースの枯渇を特に懸念しています。
このサーバーを複数のIPアドレスからのリソース枯渇（DDoS攻撃）から特に保護するために、Palo Alto Networks NGFWをどのように構成できますか？
A. カスタムApp-IDを定義して、正当なアプリケーショントラフィックのみがサーバーに到達するようにします。
B. 脆弱性保護プロファイルを追加して、攻撃をブロックします。
C. QoSプロファイルを追加して、着信要求を調整します。
D. セッションカウントを定義したDoS保護プロファイルを追加します。
正解: **(**正解を表示します**)**
参照 :https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

質問: **69**
管理者がNGFWの仮想ルーターでOSPFを有効にしました。OSPFは、仮想ルーターに新しいルートを追加していません。管理者がこの問題のトラブルシューティングを行うことができる2つのオプションはどれですか？ （2つ選択してください。）
A. 仮想ルーターのランタイム統計を表示します。
B. システムログを表示します。
C. BGP更新として転送する再配布プロファイルを追加します。
D. ルーティング段階でトラフィックpcapを実行します。

正解: **A,D** (コメントを発表する)
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CldcCAC

質問: **70**
管理プレーンのCPU使用率を削減する3つのステップはどれですか？ （3つ選択してください。）
A. 管理インターフェースでSNMPを無効にします。
B. SSLアプリケーションのアプリケーションオーバーライド。
C. セキュリティポリシーのセッション開始時のログ記録を無効にします。
D. 定義済みレポートを無効にします。
E. ファイアウォールによって復号化されるトラフィックを減らします。
正解: (正解を表示します)
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleLCAS

質問: **71**
ファイアウォールは、パケットフローシーケンスの一部としてパケットを破棄する2つの理由はどれですか？ （2つ選択してください）
A. アクション「allow」とのルール一致
B. 等コストマルチパス
C. アクション「拒否」とのルール一致
D. 入力処理エラー
正解: **C,D** (コメントを発表する)

質問: **72**
データプレーンインターフェイスでパケットキャプチャを実行するときにSSLパケットが欠落する可能性があるのは何ですか？
A. パケットは、データプレーン上のオフロードされたプロセッサーにハードウェアオフロードされます
B. 欠落パケットは管理プレーンCPUにオフロードされます
C. パケットは暗号化されているためキャプチャされません
D. 管理プレーンでのFPGAのオフロードにハードウェアの問題があります
正解: **A** (コメントを発表する)

質問: **73**
PAN-OS 8.0で追加された認証方法のサポートは？
A. RADIUS
B. LDAP
C. 直径
D. TACACS +

正解: **(**正解を表示します**)**
説明
https://www.paloaltonetworks.com/resources/datasheets/whats-new-in-pan-os-7-1

質問: **74**
展示を参照してください。
Forwarded Trust証明書として使用できる証明書はどれですか？
A. Forward_Trust
B. ドメインルート証明書
C. デフォルトの信頼認証局からの証明書
D. ドメインサブCA
正解: **D (**コメントを発表する**)**

質問: **75**
PAN-OSソフトウェアがMFAをサポートする認証要素はどれですか 3つ選択してください。）
A. プッシュ
B. プル
C. Okta Adaptive
D. 音声
E. SMS
正解: **A,D,E (**コメントを発表する**)**
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-multi-factor-authe

質問: **76**
Panoramaの次の画像で、一部の値が赤で表示されるのはなぜですか？
A. us3には、管理者が設定したしきい値から逸脱したロギングレートがあります。
B. sg2セッション数は、他の管理対象デバイスと比較して最低です。
C. uk3のロギングレートは、7日間の計算ベースラインから逸脱しています。
D. sg2のセッションしきい値が誤って設定されています。
正解: **C (**コメントを発表する**)**

質問: **77**
管理者がデータプレーンのCPU使用率を確認できるCLIコマンドはどれですか？
A. 実行中のリソースモニターを表示
B. データプレーンdp-cpuのデバッグ
C. システムリソースを表示
D. 実行中のリソースのデバッグ
正解: (正解を表示します)
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClXwCAK

質問: **78**
GlobalProtectのどのバージョンが、宛先ドメイン、クライアントプロセス、およびHTTP / HTTPSビデオストリーミングアプリケーションに基づくスプリットトンネリングをサポートしていますか？
A. PAN-OS 8.0を使用するGlobalProtectバージョン4.0
B. PAN-OS 8.1を使用するGlobalProtectバージョン4.1
C. PAN-OS 8.1を使用するGlobalProtectバージョン4.0
D. PAN-OS 8.0を使用するGlobalProtectバージョン4.1
正解: (正解を表示します)

質問: **79**
どのDoS保護メカニズムがセッション枯渇攻撃を検出して防止しますか？
A. パケットベースの攻撃保護
B. 洪水防御
C. リソース保護
D. TCPポートスキャン保護
正解: (正解を表示します)
参照 :https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

質問: **80**
次の画像に表示される証明書情報は、どのタイプの証明書のものですか？
示す：
A. 信頼証明書の転送
B. 自己署名ルートCA証明書
C. パブリックCA署名証明書
D. Webサーバー証明書

正解: **B** (コメントを発表する)

質問: **81**
HA2リンクを通じて何が交換されますか？
A. こんにちはハートビート
B. ユーザーID情報
C. セッション同期
D. HA状態情報
正解: **(**正解を表示します**)**
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

質問: **82**
管理者が過去30日間に検出された脅威など、一定期間のトラフィックの傾向を確認できるツールはどれですか？
A. セッションブラウザ
B. アプリケーションコマンドセンター
C. TCPダンプ
D. パケットキャプチャ
正解: **B** (コメントを発表する)
参照：
https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the-Application-Comm ACC / ta-p / 67342

質問: **83**
サイトAとサイトBには、サイト間VPNがセットアップされています。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設定は適切に設定されていますが、チューナーのルートは確立されていません。図のSite-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、サイトBのOSPF構成がそのインターフェイスの1つに間違った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が修正されますか？
A. トンネルを設定します。1からp2mp
B. トンネルを設定します。1からp2p
C. イーサネット1/1をp2mpに設定
D. イーサネット1/1をp2pに設定
正解: **B** (コメントを発表する)

質問: **84**

Palo Alto Networks VM-Seriesファイアウォールの展開を公式にサポートしている仮想化プラットフォームはどれですか？ （2つ選択してください。）
A. Red Hat Enterprise Virtualization（RHEV）
B. カーネル仮想化モジュール（KVM）
C. ブートストラップ仮想化モジュール（BSVM）
D. Microsoft Hyper-V
正解: **B,D** (コメントを発表する)
参照：
https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

質問: **85**
ネットワークセキュリティエンジニアは、Wildfireアクティビティの分析を求められています。ただし、Wildfire Submissionsアイテムは[モニター]タブからは表示されません。
この状態の原因は何ですか？
A. 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。
B. WildFireは機能していますが、現在、WildFire Submissionsログエントリはありません。
C. ポリシーがWildFire送信トラフィックをブロックしています。
D. エンジニアのアカウントには、WildFire提出物を表示する権限がありません。
正解: (正解を表示します)

質問: **86**
パロアルトネットワークスは、悪意のあるドメインの動的なデータベースを維持しています。
脅威を防止するためにこのデータベースを使用する2つのSecurity Platformコンポーネントはどれですか？ （2つ選択）
A. DNSベースのコマンドアンドコントロール署名
B. PAN-DB URLフィルタリング
C. ブルートフォース署名
D. BrightCloud URLフィルタリング
正解: (正解を表示します)