PaloAltoNetworks.PCNSE.v2023-07-26.q198

試験コード:	PCNSE
試験名称:	Palo Alto Networks Certified Network Security Engineer Exam
認定資格:	Palo Alto Networks
無料問題数:	198
バージョン:	v2023-07-26
アクセス数:	1868
ページビュー数:	1980
https://www.jpnpdf.com/PaloAltoNetworks.PCNSE.v2023-07-26.q198-mondaishu.html	

最新問題: **1**
[ネットワーク:] > [GlobalProtect] > [ポータル] > [メソッド] セクションに移動すると、どの 3 つのオプションが利用可能ですか? (3つお選びください)
A. ログオン前、その後オンデマンド
B. オンデマンド (ユーザーが手動で開始した接続)
C. 証明書ログオン
D. ログオン後 (常時オン)
E. ユーザーログオン (常時オン)
Answer: (解答を表示する**)**

最新問題: **2**
管理者は、トラフィック ログで、unknown-tcp として識別されるいくつかの受信セッションを確認します。管理者は、これらのセッションが、会社独自の会計アプリケーションにアクセスする外部ユーザーからのものであると判断します。管理者は、このトラフィックをアカウンティング アプリケーションとして確実に識別し、このトラフィックをスキャンして脅威を検出したいと考えています。
どのオプションを選択するとこの結果が得られますか?
A. アプリケーション オーバーライド ポリシーを作成します。
B. カスタム App-ID を作成し、詳細タブでスキャンを有効にします。
C. カスタム App-ID を作成し、 順序付けされた条件」チェック ボックスを使用します。
D. アプリケーション オーバーライド ポリシーとアプリケーションのカスタム脅威シグネチャを作成します。
Answer: B (メーッセージを残す**)**

最新問題: **3**

管理者は、DMZ 内の複数の Web サーバーがインターネットから開始された接続を受信できるようにし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 のサーバーに転送する必要があります。画像に示されている情報に基づいて、どの NAT ルールが Web ブラウジング トラフィックを正しく転送しますか?
A.
B.
C.
D.
Answer: (解答を表示する**)**

最新問題**: 4**
高可用性タイマー設定について正しいのはどれですか?
A. 一般的なフェイルオーバー タイマー設定には、中程度のタイマーを使用します。
B. テイスター フェイルオーバー タイマー設定にはクリティカル タイマーを使用します。
C. フェールオーバー タイマー設定を高速化するには、推奨タイマーを使用します。
D. テイスター フェイルオーバー タイマー設定にアグレッシブ タイマーを使用します。
Answer: (解答を表示する**)**
説明
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/ha-concepts/ha-timers

最新問題**: 5**
管理者は、アプリケーションのパフォーマンス低下に関する苦情を受け取りました。ACC確認後。管理者は、過剰な量の SSL トラフィックがあることを確認しました。この問題に対処するために管理者が設定する必要がある 3 つの要素はどれですか? （3つお選びください。）
A. アプリケーション ID ごとの QoS ポリシー
B. トラフィック クラスを定義する QoS プロファイル
C. トラフィック フローの出力インターフェイスの QoS
D. トラフィック フローの入力インターフェイスの QoS
E. SSL トラフィックのアプリケーション オーバーライド ポリシー
Answer: A,B,E (メーッセージを残す**)**

最新問題**: 6**
ある企業は、ネットワークの冗長性を高めようとしています。これを実現するにはどのインターフェイス タイプが役立ちますか?
A. レイヤー2
B. 仮想ワイヤー
C. タップ
D. アグリゲートイーサネット

Answer: D (メーッセージを残す**)**
説明
集約グループは、結合されたインターフェイス全体でトラフィックの負荷を分散することにより、ピア間の帯域幅を増やします。冗長性も提供しますhttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/config

最新問題**: 7**
企業の情報セキュリティ チームは、重要なインフラストラクチャ システムへのユーザー アクセスを制限するために、AD グループに基づくポリシーを導入しました。しかし、組織に対する最近のフィッシング キャンペーンにより、情報セキュリティは、重要な資産へのアクセスを保護できるさらなる制御を模索するようになりました。これらのシステムの情報セキュリティでは、PAN-OS 多要素認証 (MFA) 統合を使用して MFA を強制したいと考えています。
企業がPAN-OS MFA1を使用するには何をすべきでしょうか?
A. RADIUS プロファイルを参照する認証プロファイルを使用する Captive Porta1 認証ポリシーを構成します。
B. 認証シーケンスを使用するキャプティブ ポータル認証ポリシーを構成する
C. 認証プロファイルを作成し、キャプティブ ポータル認証ポリシーで使用される別の認証要素を割り当てます。
D. クレデンシャル フィッシング エージェントを使用して、クレデンシャル フィッシング キャンペーンを検出し、防止および軽減します。
Answer: B (メーッセージを残す**)**

最新問題**: 8**
ファイアウォールのペアでアクティブ/パッシブ モードで HA を構成した後、管理者は次の詳細を含む失敗したコミットを受け取ります。
この種の問題について 2 つの説明は何ですか? (2つお選びください)
A. ピア IP は管理インターフェイス設定の許可リストに含まれていません
B. コミットの発行時にバックアップ ピア HA1 IP アドレスが構成されていませんでした
C. 管理インターフェイスまたはデータ プレーン インターフェイスのいずれかが HA1 バックアップとして使用されます。
D. ファイアウォールの 1 つがサスペンド状態になりました
Answer: (解答を表示する**)**
原因 この問題は、HA1 バックアップが管理 (MGT) またはインバンド インターフェイスで構成されている場合に発生します。「バックアップ ピア HA1 IP アドレス」が構成されていません:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000008UmPCAU&lang=en_US%E2%80%A9

最新問題**: 9**

管理者が SMTP トラフィックを復号化する必要があり、サーバーの証明書を所有している場合、パロアルトネットワークス NGFW はどの SSL 復号化モードでサーバーへのトラフィックを検査できますか?
A. TLS 双方向検査
B. SSL インバウンド検査
C. SSH フォワード プロキシ
D. SMTP インバウンド復号化
Answer: B (メーッセージを残す**)**
参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-ssl-inbound-inspection

最新問題**: 10**
すでにパロアルト ファイアウォールを導入している企業が、最初の Panorama サーバーを購入しました。セキュリティ チームは、すでにすべてのファイアウォールに Panorama IP アドレスを設定し、すべてのファイアウォールのシリアル番号を Panorama a に追加しています。ファイアウォールから Panorama に設定を移行するには、次の手順は何ですか?
A. デバイス構成を Panorama にインポートし、続いて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ます
B. 各ファイアウォールで名前付き構成スナップショットをエクスポートし、続いて Panorama で名前付き構成スナップショットをインポートします。
C. API 呼び出しを使用して、管理対象デバイスから構成を直接取得します。
D. ファイアウォール移行プラグインを使用して、管理対象デバイスから設定を直接取得します。
Answer: A (メーッセージを残す**)**

最新問題**: 11**
エンジニアは、会社の既存のプロキシからユーザー ID マッピングを収集する必要があります。サードパーティのプロキシからこのデータを取得するために使用できる 2 つの方法はどれですか? (2つお選びください。)
A. XFF ヘッダー
B. サーバー監視
C. シスログ
D. クライアントのプローブ
Answer: A,C (メーッセージを残す**)**

最新問題**: 12**
顧客のアプリケーションは、カスタム PostgreSQL データベース接続の 1 つで不明の上位として識別されています。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つお選びください。)
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。
Answer: B,C (メーッセージを残す**)**

最新問題**: 13**
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つお選びください。)
A. ファイアウォールは multi-vsys モードです。
B. トラフィックがオフロードされます。
C. トラフィックがパケット キャプチャ フィルタに一致しません。
D. ファイアウォールの DP CPU が 50% を超えています。
Answer: B,C (メーッセージを残す**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet-captures/disable-hardware-offload

最新問題**: 14**
ICMP パケットの送信元アドレスは何になりますか?
A. 10.46.72.93
B. 10.30.0.93
C. 10.46.64.94
D. 192.168.93.1
Answer: C (メーッセージを残す**)**

最新問題**: 15**
ネットワーク設計では、VLAN 間ルーティングを実行する PA-5060 による 〝ルーター オン ア スティック」実装が必要です。すべての VLAN タグ付きトラフィックは、単一の dot1q トランク インターフェイスを介して PA-5060 に転送されます。どのインターフェイス タイプと構成設定がサポートされますか。このデザイン?
A. VLAN が割り当てられているレイヤー 2 インターフェースのタイプ
B. 指定されたタグを持つトランクインターフェースタイプ
C. 指定されたタグを持つレイヤ 3 サブインターフェイス タイプ
D. 指定されたタグを持つレイヤー 3 インターフェースのタイプ
Answer: C (メーッセージを残す**)**

最新問題**: 16**
管理者は、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する外部ホストから保護するために、パロ アルト ネットワーク NGFW を構成するように依頼されました。
この攻撃を防ぐセキュリティ プロファイルのタイプはどれですか?
A. 脆弱性保護

B. スパイウェア対策
C. URLフィルタリング
D. ウイルス対策
Answer: A (メーッセージを残す)
参照：
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-security-profile vulnerability-protection

最新問題**: 17**
証明書の失効ステータスを検証するために構成できる 2 つの方法はどれですか? (2つお選びください。)
A. CRL
B. ブラウン管
C. OCSP
D. 証明書検証プロファイル
E. SSL/TLS サービス プロファイル
Answer: (解答を表示する)
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/certificate-management/set-up-verification-for-certificate-revocation-status

最新問題**: 18**
ファイアウォール管理者は、会社の syslog サーバーがトラフィック ログで溢れることを避けたいと考えています。
DNS トラフィック ログが syslog に転送されないようにするには、管理者は何をすべきですか?
A. DNS を許可するセキュリティ ルールのログ記録を無効にします。
B. トラフィック ログを syslog に転送するために使用されるログ転送プロファイルに移動します。次に、トラフィック ログの一致リストの下で、アプリケーションが DNS と等しくない新しいフィルターを作成します。
C. 宛先の syslog サーバーとの DNS トラフィックを拒否するセキュリティ ルールを作成します。

D. トラフィック ログを syslog に転送するために使用されるログ転送プロファイルに移動します。次に、トラフィック ログの一致リストの下で、アプリケーションが DNS と等しい新しいフィルターを作成します。
Answer: B (メーッセージを残す**)**
ログ転送プロファイルは、どのログをどの宛先に (syslog サーバーなど) 転送するかを定義します。DNS に等しくないアプリケーションを使用してフィルターを作成すると、ログ転送プロファイルにより、DNS トラフィック ログが syslog に転送されなくなります。DNS を許可するセキュリティ ルールのログを無効にすると、ファイアウォールが DNS トラフィックのログを生成できなくなりますが、これは望ましくない可能性があります。宛先の syslog サーバーとの DNS トラフィックを拒否するセキュリティ ルールを作成すると、ファイアウォールと syslog サーバー間の通信がブロックされ、他のログに影響を与える可能性があります。DNS と同等のアプリケーションを使用してフィルターを作成すると、DNS トラフィック ログのみが syslog に転送されます。これは、必要なこととは逆です。参照：
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/configure-log-forwarding
https://docs.paloaltonetworks.com/network-security/security-policy/objects/log-forwarding

最新問題**: 19**
どのパロアルトネットワーク VM シリーズ ファイアウォールが有効ですか?
A. VM-25
B. VM-800
C. VM-50
D. VM-400
Answer: (解答を表示する**)**
説明/参照:
参照: https://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation-firewall/vm-series

最新問題**: 20**
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. > システム状態の表示 filter-pretty sys.si.p8.stats
B. > システム状態の表示 filter-pretty sys.sl.p8.phy
C. > インターフェイス ethernet1/8 を表示
D. > システム状態フィルターを表示します–prettysys.sl.p8.med
Answer: B (メーッセージを残す**)**
出力例:
> システム状態の表示 filter-pretty sys.s1.p1.phy
sys.s1.p1.phy: {
リンクパートナー: { }、
メディア: CAT5、
タイプ: イーサネット、

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

最新問題**: 21**
Panorama を PAN-OS 8.1 より前のバージョンに戻すことを計画する場合、管理者は何を考慮する必要がありますか?
A. 変数がテンプレートまたはテンプレート スタックで使用されている場合、Panorama を以前の PAN-OS リリースに戻すことはできません。
B. 管理者は Expedition ツールを使用して、構成を PAN-OS 8.1 以前の状態に適合させる必要があります。
C. Panorama を以前の PAN-OS リリースに戻すと、テンプレートまたはテンプレート スタックで使用されている変数は自動的に削除されます。
D. 管理者は可変文字を PAN-OS 8.1 以前で使用されていた文字に手動で更新する必要があります。
Answer: A (メーッセージを残す**)**
説明
テンプレートまたはテンプレート スタック設定で変数が使用されている場合、PAN-OS 8.1 から以前の PAN-OS リリースにダウングレードすることはできません。ダウングレードするには、テンプレートおよびテンプレート スタック構成から変数を削除する必要があります。

最新問題**: 22**
次の図を考えてみます。
サイト A の Trust-L3 ゾーンからのトラフィックがサイト B の Trust-L3 ゾーンに到達できるようにする VPN 接続が作成されました。
各サイトは、VPN 接続に Untrust-L3 ゾーンのtunnel.1 を使用しています。
サイト A からのトラフィックがサイト B のすべてのワークステーションに到達できるようにするには、サイト A のファイアウォールのデフォルトの仮想ルーターに静的ルートを追加する必要があります。
どのスタティック ルート構成が要件を満たすでしょうか?
A. 名前: サイト B へのルート
宛先: 172.16.20.0/24
インターフェース :tunnel.1
ネクストホップ: なし
B. 名前: サイト B へのルート
宛先: 172.16.20.0/24
インターフェース: なし
ネクストホップ: 192.0.0.2
C. 名前: サイト B へのルート
宛先: 172.16.20.1/24
インターフェース :tunnel.1

ネクストホップ: なし
D. 名前: サイト B へのルート
宛先: 172.16.20.0/24
インターフェース: イーサネット1/1
ネクストホップ: 192.0.0.1
Answer: A (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/70/pan-os/pan-os/vpns/site-to-site-vpn-with-static-routing

最新問題**: 23**
PAN-OS バージョン 9.1 以降、グローバル ログ情報はどのファイアウォール ログに記録されるようになりましたか?
A. 認証
B. 構成
C. グローバルプロテクト
D. システム
Answer: D (メーッセージを残す**)**

最新問題**: 24**
ある企業は、ネットワークの冗長性を高めようとしています。これを実現するにはどのインターフェイス タイプが役立ちますか?
A. レイヤー2
B. 仮想ワイヤー
C. タップ
D. アグリゲートイーサネット
Answer: D (メーッセージを残す**)**
説明
集約グループは、結合されたインターフェイス全体でトラフィックの負荷を分散することにより、ピア間の帯域幅を増やします。冗長性も提供します
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/configure-an-aggr

最新問題**: 25**
管理者は、User-ID 導入のトラブルシューティングを行う必要がある 管理者は、LDAP 認証に関連する問題があると考えている 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る 設定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、管理者はどの CLI コマンドを使用する必要があるか^
A. > mgmt.pcap から <FTP ホスト> への ftp エクスポート mgmt-pcap
B. > scp import mgmt-pcap を mgmt.pcap から {usernameQhost:path> にエクスポートします
C. > scp エクスポート pcap-mgmt から pcap.mgmt へ (username@host:path)

D. > scp は pcap から (usernameQhost:path) に pcap をエクスポートします
Answer: (解答を表示する**)**
説明
さらに、SCP または TFTP 経由で PCAP を手動でエクスポートすることもできます。つまり、> scp import mgmt-pcap from mgmt.pcap to <value> Destination (username@host:path) 参照: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CleECAS

最新問題**: 26**
管理者はパロアルトネットワーク NGFW 上の仮想ルーターで BGP を有効にしましたが、新しいルートが仮想ルーターに設定されていないようです。
管理者がこの問題をトラブルシューティングするのに役立つ 2 つのオプションはどれですか? (2 つお選びください。)
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。
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEWCA0

最新問題**: 27**
トラフィック ログを分析しているときに、アプリケーション列に「unknown-tcp」と表示されているエントリがあることがわかります。これらの発生を最もよく説明しているものは何ですか?
A. ハンドシェイクが行われましたが、タイムアウト前にデータ パケットは送信されませんでした。
B. 握手が行われました。ただし、アプリケーションを識別するのに十分なパケットがありませんでした。
C. ハンドシェイクは行われましたが、アプリケーションを識別できませんでした。
D. ハンドシェイクが行われず、アプリケーションを識別できなかった。
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC#:~:text=unknown% Unknown-tcp は、ファイアウォールが 3 ウェイ TCP ハンドシェイクをキャプチャしたが、アプリケーションが識別されなかったことを意味します。これは、ファイアウォールに署名がないカスタム アプリケーションの使用が原因である可能性があります。

最新問題**: 28**

管理者のパロアルトネットワークス NGFW 宛ての VPN トラフィックが、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とき、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
Answer: (解答を表示する**)**
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/vpns/set-up-site-to-site-vpn/set-up-an-ipsec-tunnel

最新問題**: 29**
ファイアウォール管理者は、企業ネットワークの 1 つのセグメントを可視化したいと考えています。セグメント上のトラフィックはバックボーン スイッチ上でルーティングされます。管理者は、可視性を取得した後、セグメント X にセキュリティ ルールを適用することを計画しています。L3 モードでインターネット ゲートウェイとして使用される PAN-OS ファイアウォールがすでに存在しており、ファイアウォール上で追加のトラフィックを取得するのに十分なシステム リソースがあります。管理者は、サービスの中断を最小限に抑え、IP を変更せずにこの操作を完了する必要があります。
管理者がとるべき最善の選択肢は何ですか?
A. ファイアウォール上のセグメント X の TAP インターフェイスを構成します。
B. ファイアウォール上のセグメント X の vwire インターフェイスを構成します。
C. ファイアウォール上のセグメント X のレイヤー 3 インターフェイスを構成します。
D. ファイアウォール上のセグメント X に新しい vsys を構成します。
Answer: A (メーッセージを残す**)**
TAP インターフェイスは、スイッチ SPAN またはミラー ポートに接続して、ネットワーク全体のトラフィック フローを受動的に監視できるファイアウォール上の専用インターフェイスです。TAP インターフェイスは、ネットワーク トラフィックのフローに影響されることなく、アプリケーションの可視性と脅威の検出を提供します。TAP インターフェイスでは、IP の変更やネットワーク セグメント上のサービスの中断は必要ありません1。オプション B は不正解です。vwire インターフェイスは、2 つのネットワーク セグメントを透過的に接続する仮想ワイヤの作成に使用されます。Vwire インターフェイスでは物理的なケーブル接続の変更が必要であり、ネットワーク セグメント 2 でサービスが中断される可能性があります。オプション C は、異なるサブネット間のトラフィックのルーティングにレイヤー 3 インターフェイスが使用されるため、不正解です。レイヤ 3 インターフェイスでは IP の変更が必要であり、ネットワーク セグメント 2 でサービスが中断される可能性があります。オプション D は不正解です。新しい vsys を使用して、独自のポリシーとオブジェクトのセットを持つことができる仮想システムが作成されます。新しい vsys は、特定のネットワーク セグメントの可視性やセキュリティを提供しません3。

最新問題**: 30**

PAN-OS SD-WAN の転送エラー訂正 (FEC) を構成する場合、管理者はどのタイプの SD-WAN プロファイル内の機能を有効にしますか?
A. 証明書プロファイル
B. パス品質プロファイル
C. SD-WAN インターフェイス プロファイル
D. トラフィック分散プロファイル
Answer: (解答を表示する**)**
説明
PAN-OS SD-WAN の前方誤り訂正 (FEC) を有効にするには、誤り訂正プロファイルのインターフェイス選択に適格であることを指定する SD-WAN インターフェイス プロファイルを作成し、そのプロファイルを 1 つ以上のインターフェイスに適用する必要があります。次に、FEC またはパケット複製を実装するためのエラー修正プロファイルを作成する必要があります。
参考文献:
https://docs.paloaltonetworks.com/sd-wan/2-0/sd-wan-admin/configure-sd-wan/create-an-error-correction-profile

最新問題**: 31**
AutoFocus へのファイアウォールの接続を確認するために使用できる 2 つの方法はどれですか? (2つお選びください。)
A. CLI を使用してオートフォーカスのステータスを確認します。
B. WebUI ダッシュボードの AutoFocus ウィジェットを確認します。
C. WildFire 転送ログを確認します。
D. ライセンスを確認する
E. [デバイス管理] タブで AutoFocus が有効になっていることを確認します。
Answer: B,D (メーッセージを残す**)**
参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-autofocus-threat-intelligence

最新問題**: 32**
SSL フォワード プロキシを有効にせずに、信頼できない証明書を持つサイトをブロックする自動ソリューションの一部となる 2 つのアクションはどれですか? (2つお選びください。)
A. 復号化を行わない復号化ポリシー ルールを作成します。

B. CRL から解決された既知のサイトの IP アドレスを取得するように EDL を構成します。
C. 信頼できないサイト用の動的アドレス グループを作成する
D. 脆弱性セキュリティ プロファイルが添付されたセキュリティ ポリシー ルールを作成します。
E. 「信頼できない発行者とのセッションをブロックする」設定を有効にします。
Answer: A,E (メーッセージを残す)
https://www.paloaltonetworks.com/documentation/71/pan-os/web-interface-help/objects/objects-decryption-profile

最新問題**: 33**
ファイアウォールにリンク監視構成がある場合、フェイルオーバーは何が原因で発生しますか?
A. ethernet1/6 がダウンします
B. ethernet1/3 または Ethernet1/6 がダウン中
C. ethernet1/3 がダウンします
D. ethernet1/3 と ethernet1/6 がダウンします
Answer: D (メーッセージを残す)

最新問題**: 34**
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つお選びください)
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 request system system-mode logger 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. Panorama 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 Enable 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. 専用ログ コレクターの Panorama CLI にログインします。
Answer: (解答を表示する)
(https://www.paloaltonetworks.com/documentation/60/panorama/panorama_adminguide/set-up-panorama/set-up-the-m-100-appliance)

最新問題**: 35**
基本的な WildFire サービスの一部として、分析のために WildFire に転送できる 3 つのファイル タイプはどれですか?
（3つお選びください。）
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf

F. .jar
Answer: B,D,E (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/getting-started/enable-basic-wildfire-forwarding

最新問題**: 36**
トラフィック ログのセッションでは、アプリケーションが 「不完全」であると報告されています。 「不完全」とはどういう意味ですか？
A. 3 ウェイ TCP ハンドシェイクは確認されましたが、アプリケーションを識別できませんでした。
B. 3 ウェイ TCP ハンドシェイクが完了しませんでした。
C. トラフィックは UDP 経由で送信されており、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、即座に破棄されました。
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClibCAC

最新問題**: 37**
管理者は、同じサブネット内に 2 ペアのファイアウォールを持っています。ファイアウォールの両方のペアは、アクティブ/パッシブの高可用性モードを使用するように構成されています。アップストリーム ルートの ARP テーブルには、これらのファイアウォールの一部で共有されている同じ MAC アドレスが表示されます。
競合しないように MAC アドレスを変更するには、1 つのファイアウォール ペアで何を構成できますか?
A. ファイアウォール ペア間にフローティング IP を構成します。
B. 高可用性設定のグループ ID を、同じサブネット上の他のファイアウォール ペアとは異なるように変更します。
C. MAC アドレスが競合するインターフェースのインターフェースタイプを L3 から VLAN に変更します。
D. ファイアウォールの 1 つのペアで、CLI コマンド set network interface vlan arp を実行します。
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS 高可用性設定のグループ ID を、同じサブネット上の他のファイアウォール ペアとは異なるように変更します。これにより、MAC アドレスの競合が防止され、ファイアウォールがトラフィックを適切にルーティングできるようになります。必要に応じて、ファイアウォール ペア間にフローティング IP を構成することもできます。

最新問題**: 38**

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、パケットが既存のセッションの一部であるかを、どの種類の一致を使用して判断しますか?
A. 6 タプルの一致:
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、および送信元セキュリティ ゾーン
B. 5 タプルの一致:
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 タプルの一致:
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、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 タプルの一致:
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、送信元ユーザー、送信元セキュリティ ゾーン、
Answer: A (メーッセージを残す**)**
宛先セキュリティ ゾーン、アプリケーション、および URL カテゴリ
Explanation:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVECA0

最新問題**: 39**
パノラマの次の画像で、一部の値が赤で表示されているのはなぜですか?
A. uk3 のロギング レートは、計算された 7 日間のベースラインから逸脱しています。
B. sg2 セッション数が他の管理対象デバイスと比較して最も少ない。
C. sg2 のセッションしきい値の設定が間違っています。
D. us3 のロギング レートが、管理者が設定したしきい値から逸脱しています。
Answer: A (メーッセージを残す**)**

最新問題**: 40**
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. デュオ
C. 半径
D. PingID
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/authentication/authentication-types/multi-factor-authentication

最新問題**: 41**
ある企業は、VLAN トランク リンク上の 2 つのコア スイッチ間に PA-3060 ファイアウォールをインストールしたいと考えています。各 VLAN を独自のゾーンに割り当て、タグなし (ネイティブ)

トラフィックを独自のゾーンに割り当てる必要があります。複数の VLAN を個別のゾーンに区別するオプションはどれですか?
A. 2 つの V-Wire インターフェイスを持つ V-Wire オブジェクトを作成し、V-Wire オブジェクトの「タグ許可」フィールドに「0 ～ 4096」の範囲を定義します。
B. 2 つの V-Wire サブインターフェイスを持つ V-Wire オブジェクトを作成し、V-Wire オブジェクトの [タグ許可] フィールドに 1 つの VLAN ID だけを割り当てます。追加の VLAN ごとにこの手順を繰り返し、タグなしトラフィックには VLAN ID 0 を使用します。. 各インターフェイス/サブインターフェイスを一意のゾーンに割り当てます。
C. 単一の VLAN ID と共通の仮想ルーターにそれぞれ割り当てられるレイヤー 3 サブインターフェイスを作成します。
物理レイヤー 3 インターフェイスは、タグなしのトラフィックを処理します。各インターフェイス/サブインターフェイス tA を割り当てます。
ユニークなゾーン。どのインターフェイスにも IP アドレスを割り当てないでください。
D. VLAN ごとに VLAN オブジェクトを作成し、各 VLAN ID に一致する VLAN インターフェイスを割り当てます。追加の VLAN ごとにこの手順を繰り返し、タグなしトラフィックには VLAN ID 0 を使用します。各インターフェイス/サブインターフェイスを一意のゾーンに割り当てます。
Answer: B (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa 仮想ワイヤー インターフェイスは、デフォルトですべてのタグなしトラフィックを許可します。ただし、仮想ワイヤを使用して 2 つのインターフェイスを接続し、どちらかのインターフェイスが仮想 LAN (VLAN) タグに基づいてトラフィックをブロックまたは許可するように設定できます。
VLAN タグ 0 は、タグなしのトラフィックを示します。また、複数のサブインターフェイスを作成し、それらを異なるゾーンに追加して、VLAN タグまたは VLAN タグと IP 分類子 (アドレス、範囲、またはサブネット) の組み合わせに従ってトラフィックを分類して、詳細な分類子を適用することもできます。特定の VLAN タグ、または特定の送信元 IP アドレス、範囲、またはサブネットからの VLAN タグに対するポリシー制御。

最新問題**: 42**
ファイアウォールがパケット フロー シーケンスの一部としてパケットを破棄する理由を 2 つ挙げてください。(2つお選びください)
A. 等コストマルチパス
B. 受信処理エラー
C. アクション「allow」と一致するルール
D. アクション「拒否」と一致するルール
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVHCA0

トラフィックを拒否するとパケットが破棄されます。パケットは、不正な形式または不正なフレーム、データグラム、またはパケットが原因で廃棄されることもあります。

最新問題: **43**
Web サーバーは、ポート 8080 で HTTP トラフィックをリッスンするように構成されています。クライアントは、TCP ポート 80 の IP アドレス 1.1.1.100 を使用して Web サーバーにアクセスします。宛先 NAT ルールは、IP アドレスとレポートの両方を 10.1.1.100 に変換するように構成されています。TCP ポート 8080。
ファイアウォールでどの NAT ルールとセキュリティ ルールを設定する必要がありますか? (2つお選びください)
A. service-http サービスを使用する、untrust-l3 ゾーンの送信元から dmz-zone の 10.1.1.100 の宛先までの NAT ルール。
B. Web ブラウジング アプリケーションを使用した、untrust-l3 ゾーンのソースから dmz-l3 ゾーンの 1.1.100 の宛先までのセキュリティ ポリシー。
C. Web ブラウジング アプリケーションを使用した、送信元が untrust-l3 ゾーン、宛先が dmz-l3 ゾーンの 10.1.1.100 であるセキュリティ ポリシー
D. service-http サービスを使用する、untrust-l3 ゾーンの送信元から untrust-l3 ゾーンの 1.1.1.100 の宛先までの NAT ルール。
Answer: B,D (メーッセージを残す**)**

最新問題: **44**
顧客は従来のリモート アクセス VPN ソリューションを置き換えようとしています。代替として Prisma Access が選択されました。オンボーディング中に、次のオプションとライセンスが選択され、有効になりました。
顧客は、Prisma Access for Mobile Users に接続しているユーザーによって生成されたログを Splunk SIEM に転送したいと考えています。顧客が構成する必要がある 2 つの設定はどれですか? (2つお選びください)
A. ログ転送プロファイルを設定し、syslog チェックボックスを選択して、Splunk syslog サーバーを追加します。Mobie_User_Device_Group 内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. ログ転送プロファイルを構成し、[Panorama/Cortex Data Lake] チェックボックスを選択します。Mobile_User_Device_Group 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。
C. Panorama Collector グループのデバイス ログ転送を設定して、ログを Splunk syslog サーバーに送信します。
D. Cortex Data Lake ログ転送を構成し、Splunk syslog サーバーを追加します。
Answer: (解答を表示する**)**

最新問題: **45**

URL フィルタリングでは、どのコンポーネントが URL パターンに一致しますか?
A. データプレーンでのシングルパスパターンマッチング
B. 管理プレーン上のライブ URL フィード
C. データプレーン上のセキュリティ処理
D. データプレーンでの署名の照合
Answer: A (メーッセージを残す**)**

最新問題**: 46**
ネットワーク管理者は、Windows 10 エンドポイントにログオン前で GlobalProtect を展開し、パロ アルト ネットワークのベスト プラクティスに従いたいと考えています。
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つお選びください。)
A. サーバー証明書
B. 地元のコンピュータ ストア
C. 秘密鍵
D. 自己署名証明書
E. マシン証明書
Answer: B,D,E (メーッセージを残す**)**
https://docs.paloaltonetworks.com/globalprotect/9-0/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-with-pre-logon.html

最新問題**: 47**
復号化ポリシー ルールの一致に有効な 3 つの修飾子は何ですか? (3つお選びください)
A. デスティネーションゾーン
B. アプリID
C. ユーザーID
D. カスタム URL カテゴリ
E. ソースインターフェイス
Answer: A,C,E (メーッセージを残す**)**

最新問題**: 48**

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

最新問題**: 49**
展示を参照してください。
管理者は、Panoram a 上のパロアルトネットワーク NGFW からのトラフィック ログを表示できません。設定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には、パロアルトネットワーク NGFW のどこが最適ですか?
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
Answer: D (メーッセージを残す**)**
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/manage-log-collection/configure-log-forwarding-to-panorama.html#

最新問題**: 50**
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、識別されるすべてのトラフィックは Content-ID エンジンによって検査される必要があると述べました。パロアルトネットワークデバイス上のこのトラフィックに即座に対処するには、company.com はどの方法を使用する必要がありますか?
A. 署名なしでカスタム アプリケーションを作成し、トラフィックの送信元、宛先、宛先ポート/プロトコル、およびカスタム アプリケーションを含むアプリケーション オーバーライド ポリシーを作成します。

B. パロアルトネットワークスから正式なアプリケーション署名が提供されるまで待ちます。
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. 社内アプリケーション トラフィックの一意の識別子と一致する署名を持つカスタム アプリケーションを作成します。
Answer: D (メーッセージを残す**)**
署名付きのカスタム アプリケーションを作成してセキュリティ ポリシーに添付するか、カスタム アプリケーションを作成してアプリケーション オーバーライド ポリシーを定義します。カスタム アプリケーションを使用すると、内部アプリケーションの定義 (特性、カテゴリ、サブ) をカスタマイズできます。-カテゴリ、リスク、ポート、タイムアウト - ネットワーク上の未確認トラフィックの範囲を最小限に抑えるために、詳細なポリシー制御を実行します。カスタム アプリケーションを作成すると、ACC およびトラフィック ログでアプリケーションを正確に識別できるようになり、ネットワーク上のアプリケーションの監査/レポートに役立ちます。カスタム アプリケーションの場合、アプリケーションを一意に識別する署名とパターンを指定し、それをアプリケーションを許可または拒否するセキュリティ ポリシーに添付できます。
あるいは、ファイアウォールで高速パス (レイヤー 7 検査に App-ID を使用する代わりにレイヤー 4 検査) を使用してカスタム アプリケーションを処理する場合は、アプリケーション オーバーライド ポリシー ルールでカスタム アプリケーションを参照できます。カスタム アプリケーションによるアプリケーション オーバーライドにより、レイヤー 7 検査である App-ID エンジンによるセッションの処理が妨げられます。代わりに、ファイアウォールがレイヤー 4 で通常のステートフル検査ファイアウォールとしてセッションを処理するように強制されるため、アプリケーションの処理時間が節約されます。
たとえば、ホスト ヘッダー www.mywebsite.com でトリガーされるカスタム アプリケーションを構築する場合、パケットは最初に Web ブラウジングとして識別され、次にカスタム アプリケーション (親アプリケーションが Web ブラウジング) として照合されます。親アプリケーションは Web ブラウジングであるため、カスタム アプリケーションはレイヤー 7 で検査され、コンテンツと脆弱性がスキャンされます。
アプリケーション オーバーライドを定義すると、ファイアウォールはレイヤー 4 での処理を停止します。ログ内で識別しやすいように、カスタム アプリケーション名がセッションに割り当てられ、トラフィックの脅威はスキャンされません。
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/app-id/manage-custom-or-unknown-applications.html#id74b58a78-164f-4dc5-aa4e-31ce62f2af0d

最新問題**: 51**
キャプティブ ポータル ポリシーを検証するにはどのコマンドを使用できますか?
A. cp-policy-eval をリクエスト <基準>
B. デバッグ cp-policy <基準>
C. cp-policy-match をテストします <基準>
D. キャプティブ ポータル ポリシーの評価 <基準>

Answer: C (メーッセージを残す)

最新問題: **52**
テンプレート スタックがデバイスに割り当てられており、そのスタックに重複する 3 つのテンプレートが含まれている場合
設定、テンプレート スタックがプッシュされたときにどの設定がデバイスに公開されますか?
A. ファイアウォールの場所に応じて、Panorama が送信する設定を決定します。
B. すべてのテンプレートで構成されているすべての設定。
C. スタックの最上位にあるテンプレートに割り当てられた設定。
D. 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求められます。
Answer: C (メーッセージを残す)

最新問題: **53**
ファイアウォールにリンク監視構成がある場合、フェイルオーバーは何が原因で発生しますか?
A. ethernet1/6 がダウンします
B. ethernet1/3 と ethernet1/6 がダウンします
C. ethernet1/3 がダウンします
D. ethernet1/3 または Ethernet1/6 がダウン中
Answer: B (メーッセージを残す)

最新問題: **54**
スクリーンショットを表示します。QoS プロファイルとポリシー ルールは次のように設定されています。この情報に基づいて、正しい 2 つの記述はどれですか? (2つお選びください。)
A. DNS は SSH よりも優先度が高く、帯域幅が広くなります。
B. Google ビデオは WebEx よりも優先度が高く、帯域幅も広くなります。
C. SMTP は Zoom よりも優先度が高くなりますが、帯域幅は低くなります。
D. Facetime の優先度は高くなりますが、帯域幅は Zoom よりも低くなります。
Answer: A,B (メーッセージを残す)
説明
QoS プロファイルは、さまざまなクラスと保証された帯域幅の割合をさまざまなアプリケーションに割り当てます。QoS ポリシー ルールは、送信元ゾーンと宛先ゾーンに基づいて QoS プロファイルをトラフィックに適用します。クラスの優先順位はその番号によって決まり、番号が小さいほど優先順位が高くなります。クラスの帯域幅は、保証されたパーセンテージによって決まり、パーセンテージが高いほど帯域幅が広くなります。この情報に基づくと、DNS は最も高い優先順位 (1) と最も多くの帯域幅 (40%) を持つクラス 1 に属します。SSH はクラス 4 に属し、優先度が最も低く (4)、帯域幅が最小 (5%) です。したがって、DNS は SSH よりも優先順位が高く、帯域幅が広くなります。同様に、Google ビデオはクラス 2 に属し、優先度が 2 番目に高く (2)、帯域幅が 2 番目に多く (30%) あります。WebEx は、3 番目に高い優先順位 (3) と 3 番目に広い帯域幅 (25%) を持

つクラス 3 に属します。したがって、Google ビデオは WebEx よりも優先度が高く、帯域幅も広くなります。参考文献:
:https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/quality-of-service/qos-concepts/qos-profiles

最新問題: **55**
管理者は、デバイス グループ内の 1 つのファイアウォールに特定の DNS サーバーを割り当てる必要があります。管理者はデバイス レベルでテンプレート変数を編集するにはどこにアクセスすればよいでしょうか?
A. [パノラマ] > [テンプレート] の下の変数 CSV エクスポート
B. [パノラマ] > [テンプレート] の下の [PDF エクスポート]
C. パノラマ > テンプレートで変数を管理します。
D. 管理対象デバイス > デバイスの関連付け
Answer: C (メーッセージを残す**)**
説明
デバイス レベルでテンプレート変数を編集するには、[パノラマ] > [テンプレート] の [変数の管理] に移動する必要があります。これにより、特定のデバイスまたはデバイス グループの変数のデフォルト値をオーバーライドできます。たとえば、
そのデバイスの ${dns-primary} 変数。
参考資料:https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templ

最新問題: **56**
管理者がアプリケーション オーバーライド ポリシーを使用すると、どのイベントが発生しますか?
A. 脅威IDの処理時間が短縮されます。
B. パロアルトネットワークス NGFW は、レイヤー 4 で App-ID 処理を停止します。
C. セキュリティ ルールによってトラフィックに割り当てられたアプリケーション名がトラフィック ログに書き込まれます。
D. App-IDの処理時間が増加します。
Answer: A (メーッセージを残す**)**
参照：
https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an-Application-Override
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/app-id/manage-custom-or-unknown-applications#

最新問題: **57**
トラフィック ログにアプリケーションが 「適用不可」としてリストされるのはなぜですか?
A. アプリケーションの照合が実行される前に、ファイアウォールがトラフィックを拒否しました。

B. 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
C. TCP接続確立後にアプリケーションデータが不足しました
D. アプリケーションは既知の Palo Alto Networks App-ID ではありません。
Answer: A (メーッセージを残す**)**
説明
ドキュメントによると、 適用されない」とは、トラフィックが受信するポートまたはサービスが許可されていないか、そのポートまたはサービスを許可するルールやポリシーがないために、パロアルト デバイスが破棄されるデータを受信したことを意味します。これは、アプリケーションの照合が実行される前にトラフィックがドロップまたは拒否されたために発生します。参考資料: 1 トラフィック ログには適用されません - Palo Alto Networks 2 アプリケーション フィールドの適用されない、不完全、不十分なデータ - Palo Alto Networks
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClspCAC

最新問題**: 58**
GlobalProtect 構成の画面キャプチャを表示します。
この構成の目的は何ですか?
A. すべての内部クライアントのトンネル アドレスを 192.168.10.1 から始まる IP アドレス範囲に設定します。
B. 内部クライアントが IP アドレス 192.168.10.1 の内部ゲートウェイに接続するように強制されます。
C. クライアントが 192.168.10.1 に対して逆 DNS ルックアップを実行して、内部クライアントであることを検出できるようにします。
D. ファイアウォールに動的 DNS 更新の実行を強制し、内部ゲートウェイのホスト名と IP アドレスを DNS サーバーに追加します。
Answer: C (メーッセージを残す**)**
参照：
https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-por the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations
GlobalProtect エージェントが企業ネットワーク内にあるかどうかを判断できるようにするには、このオプションを選択します。このオプションは、内部ゲートウェイと通信するように構成されているエンドポイントにのみ適用されます。ユーザーがログインしようとすると、エージェントは逆引き DNS ルックアップを実行します。指定された IP アドレスへの指定されたホスト名を使用する内部ホスト。ホストは、エンドポイントが企業ネットワーク内にある場合に到達可能な参照ポイントとして機能します。エージェントがホストを見つけた場合、エンドポイントはネットワーク内にあり、エージェントは接続します。内部ゲートウェイ。エージェントが内部ホストを見つけられなかった場合、エンドポイントはネットワークの外側にあり、エージェントは外部ゲートウェイの 1 つへのトンネルを確立します。」

最新問題**: 59**

Web サーバーは DMZ でホストされており、サーバーは TCP ポート 443 で受信接続をリッスンするように構成されています。Web ブラウズ アクセスを許可するには、信頼ゾーンから DMZ ゾーンへのアクセスを許可するセキュリティ ポリシー ルールを構成する必要があります。Web サーバーは、そのコンテンツを HTTP(S) 経由でホストします。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 ルールを使用して復号化されます。
tcp/443 上のこのサーバーへのクリアテキスト Web ブラウジング トラフィックを許可するには、サービスとアプリケーションのどの組み合わせ、およびセキュリティ ポリシー ルールの順序を構成する必要があります。
A. ルール #1: アプリケーション: Web ブラウジング。サービス: アプリケーションのデフォルト; アクション: 許可ルール #2: アプリケーション: ssl; サービス: アプリケーションのデフォルト; アクション: 許可する
B. ルール 1: アプリケーション: Web ブラウジング。サービス: サービス-httpsアクション: 許可ルール #2: アプリケーション: ssl; サービス: アプリケーションのデフォルト; アクション: 許可する
C. ルール # 1: アプリケーション: ssl; サービス: アプリケーションのデフォルト; アクション: 許可ルール #2: アプリケーション: Web ブラウジング; サービス: アプリケーションのデフォルト; アクション: 許可する
D. ルール #1: アプリケーション: Web ブラウジング。サービス: サービス-httpアクション: 許可ルール #2: アプリケーション: ssl; サービス: アプリケーションのデフォルト; アクション: 許可する
Answer: A (メーッセージを残す**)**
復号化されたトラフィックが Web ブラウジング アプリケーションと一致する場合。その後、ファイアウォールはこれを ssl (443) 経由の Web ブラウジングとしてログに記録し、 &pplication-default」に設定されている場合は一致しません。
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClEyCAK

最新問題**: 60**
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、ドロップ
B. 受信、ファイアウォール、送信、および非同期
C. 受信管理、送信、非同期
D. 受信、ファイアウォール、送信、ドロップ
Answer: D (メーッセージを残す**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClTJCA0
docs.paloaltonetworks.com/pan-os/8-1/pan-os-web-interface-help/monitor/monitor-packet-capture/packet-capture -概要.html

最新問題**: 61**
エンタープライズ PKI を使用する管理者は、Panorama と管理対象ファイアウォールおよびログコレクタの間の相互認証を確保するために、独自の信頼チェーンを確立する必要があります。

管理者は信頼の連鎖をどのように確立しますか?
A. LDAP または RADIUS 統合を有効にする
B. カスタム証明書を使用する
C. 強力なパスワード認証を設定します。
D. 多要素認証を設定する
Answer: (解答を表示する**)**

最新問題**: 62**
顧客は、レイヤー 2 イーサネット ポートの VLAN インターフェイスをセットアップしたいと考えています。
VLAN インターフェイスの設定に使用される必須オプションはどれですか? (2つお選びください。)
A. 仮想ルータ
B. セキュリティゾーン
C. ARP エントリ
D. Netflow プロファイル
Answer: A,B (メーッセージを残す**)**
参照: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/network/network-interfaces/pa-7000-series-layer-2-interface#idd2bcaacc-54b9-4ec9-あ、追加-8064499f5b9d

最新問題**: 63**
ゾーン保護プロファイルでのみ使用できる保護機能はどれですか?
A. SYN フラッド Cookie を使用した SYN フラッド防御
B. ICMP フラッド保護
C. ポートスキャン保護
D. UDP フラッド保護
Answer: C (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/network/network-network-profiles-zone-protection

最新問題**: 64**

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、管理者がパロ アルト ネットワーク NGFW に管理者を認証するために使用できる 3 つの認証サービスはどれですか? (3つお選びください。)
A. ケルベロス
B. パップ
C. SAML
D. TACACS+
E. 半径
F. LDAP
Answer: C,D,E (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/firewall-administration/manage-firewall-administrat 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。サーバーは認証と認可の両方を実行します。認可のために、TACACS+ または RADIUS サーバー上でベンダー固有属性 (VSA) を定義するか、SAML サーバー上で SAML 属性を定義します。
PAN-OS は、ファイアウォール上で定義した管理者ロール、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

最新問題: **65**
tcpdump キャプチャをエクスポートするにはどの CLI コマンドを使用できますか?
A. scp は mgmt.pcap から <username@host:path> に tcpdump をエクスポートします
B. scp は mgmt.pcap から mgmt-pcap を <username@host:path> に抽出します。
C. scp import mgmt-pcap を mgmt.pcap から <username@host:path> にエクスポートします。
D. mgmt-pcap をダウンロードします。
Answer: C (メーッセージを残す)
説明/参照:
参照: https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-管理インターフェイス上/ta-p/55415

最新問題: **66**
SD-WAN 構成計画時にインポートを考慮すべき 3 つの項目はどれですか? (3つお選びください。)
A. IP アドレス
B. ブランチおよびハブの場所
C. リンク要件
D. ISP の名前
Answer: A,B,C (メーッセージを残す)

最新問題: **67**

管理者はパロアルトネットワーク NGFW 上の仮想ルーターで BGP を有効にしましたが、新しいルートは
仮想ルーターに実装されていないようです。
管理者がこの問題をトラブルシューティングするのに役立つ 2 つのオプションはどれですか? (2つお選びください。)
A. ランタイム統計を表示し、BGP 構成の問題を探します。
B. [ACC] タブを表示して、ルーティングの問題を特定します。
C. 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。
D. NGFW でトラフィック pcap を実行して、BGP の問題を確認します。
Answer: A,B (メーッセージを残す**)**

最新問題**: 68**
company.com は、アプリケーション オーバーライドを有効にしたいと考えています。次のスクリーンショットを考えてみます。
送信元トラフィックと宛先トラフィックがアプリケーション オーバーライド ポリシーに一致する場合、正しい 2 つのステートメントはどれですか?
(2つお選びください)
A. UDP ポート 16384 を利用するトラフィックは ftp-base」として識別されるようになります。
B. トラフィックは UDP ポート 16384 経由で強制的に動作します。
C. UDP ポート 16384 を利用するトラフィックは、App-ID エンジンと Content-ID エンジンをバイパスします。
D. ftp-base」に一致するトラフィックは、App-ID エンジンと Content-ID エンジンをバイパスします。
Answer: A,D (メーッセージを残す**)**

最新問題**: 69**
ファイアウォール上でローカルにのみ構成でき、Panorama テンプレートまたはテンプレート スタックからプッシュできない 2 つの設定はどれですか? (2つお選びください)
A. HA1 IP アドレス
B. ネットワークインターフェースの種類
C. マスターキー
D. ゾーン保護プロファイル
Answer: A,C (メーッセージを残す**)**
https://docs.paloaltonetworks.com/panorama/7-1/panorama-admin/manage-firewalls/template-capabilities-and-Exceptions.html#
テンプレートとテンプレート スタックを使用してさまざまな設定を定義できますが、次のタスクは各管理対象ファイアウォールでローカルにのみ実行できます。
デバイスブロックリストを設定します。
ログをクリアします。
通常モード、multi-vsys モード、FIPS-CC モードなどの動作モードを有効にします。

HA ペア内のファイアウォールの IP アドレスを構成します。
マスターキーと診断を構成します。
構成ファイルを比較します (構成監査)。
マルチ vsys ファイアウォール上の vsys の名前を変更します。

最新問題: **70**
PAN-OS 7.0 でサポートされている 3 つのセキュリティ ポリシー ルール タイプの分類は何ですか? (3つお選びください。)
A. デフォルト
B. グローバル
C. インターゾーン
D. イントラゾーン
E. ユニバーサル
F. 外部ゾーン
Answer: (解答を表示する**)**
https://live.paloaltonetworks.com/t5/Management-Articles/What-are-Universal-Intrazone-and-Interzone-Rules/ta-p/57491

最新問題: **71**
管理者が SMTP トラフィックを復号化する必要があり、サーバーの証明書を所有している場合、パロアルトネットワークス NGFW はどの SSL 復号化モードでサーバーへのトラフィックを検査できますか?
A. SSH フォワード プロキシ
B. TLS 双方向検査
C. SSL インバウンド検査
D. SMTP インバウンド復号化
Answer: C (メーッセージを残す**)**

最新問題: **72**
管理者は、Palo Alto Networks NGFW のペアに対してアクティブ/パッシブ HA を構成するように求められました。
管理者は、アクティブなファイアウォールに優先度 100 を割り当てます。
パッシブ ファイアウォールの優先順位はどれが正しいですか?
A. 0
B. 99
C. 1
D. 255
Answer: (解答を表示する**)**
参照：

https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/71/pan-os/pan-os/section_5.p (9 ページ)

最新問題**: 73**
Panorama によって生成されたログを外部のセキュリティ情報およびイベント管理 (SIEM) システムに転送できるのは、どの Panorama 機能ですか?
A. パノラマログ設定
B. パノラマ ログ テンプレート
C. パノラマデバイスグループログ転送
D. コレクター グループのコレクター ログ転送
Answer: A (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/61/panorama/panorama_admiHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manag e-log-collection/enable-log-forwarding-from-panorama-to-external-destinations"nguidHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/enable-log-forwarding-from-panorama-to-external-destinations」e/manage-log-collection/パノラマから外部宛先へのログ転送を有効にするHYPERLINK "https://www.paloaltonetworks.com/documentation/61/panorama/panorama_adminguide/manage-log-collection/enable-log-forwarding-from-panorama-to-external-destinations」

最新問題**: 74**
仮想ルーターでは、どのオブジェクトにすべての潜在的なルートが含まれていますか?
A. MIB
B. リブ
C. SIP
D. FIB
Answer: B (メーッセージを残す**)**
説明/参照:
参考: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/virtual-routers

最新問題**: 75**
パロアルトネットワークスの NGFW のすぐに使用できる構成について正しい 2 つの記述はどれですか? (2つお選びください)
A. デバイスは、最初の 2 つのインターフェイスから仮想ワイヤ ペアを使用して事前設定されています。
B. デバイスにはライセンスが付与されており、導入の準備ができています。
C. 管理インターフェイスの IP アドレスは 192.168.1.1 で、SSH および HTTPS 接続が可能です。
D. Untrust ゾーンのトラフィックが Trust ゾーンに送信されることを許可するデフォルトの双方向ルールが構成されています。

E. インターフェイスは ping 可能です。
Answer: (解答を表示する**)**
https://popravak.wordpress.com/2014/07/31/initial-setup-of-palo-alto-networks-next-generation-firewall/

最新問題**: 76**
ユーザーが企業資格情報を誤ってフィッシング Web サイトに送信しないようにするには、どの機能を設定する必要がありますか?
A. URLフィルタリングプロファイル
B. ゾーン保護プロファイル
C. スパイウェア対策プロファイル
D. 脆弱性保護プロファイル
Answer: A (メーッセージを残す**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-credential-phishing

最新問題**: 77**
管理者は、デバイス グループ内の 1 つのファイアウォールに特定の DNS サーバーを割り当てる必要があります。管理者はデバイス レベルでテンプレート変数を編集するにはどこにアクセスすればよいでしょうか?
A. [パノラマ] > [テンプレート] の下の変数 CSV エクスポート
B. [パノラマ] > [テンプレート] の下の [PDF エクスポート]
C. パノラマ > テンプレートで変数を管理します。
D. 管理対象デバイス > デバイスの関連付け
Answer: C (メーッセージを残す**)**
説明
デバイス レベルでテンプレート変数を編集するには、[パノラマ] > [テンプレート] の [変数の管理] に移動する必要があります。これにより、特定のデバイスまたはデバイス グループの変数のデフォルト値をオーバーライドできます。たとえば、
そのデバイスの ${dns-primary} 変数。参考文献:

https://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/manage-firewalls/manage-templates/use-tem

最新問題: **78**
テンプレートとテンプレート スラックをより簡単に再利用するには、構成内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. @パノラマ
B. #パンクラマ
C. パノラマ(&P)
D. $パノラマ
Answer: (解答を表示する**)**
オブジェクトの変数名を使用して、テンプレートとテンプレート スタックを作成します。変数名はドル記号 ("$") 記号で始める必要があります。たとえば、$Panorama を、複数の管理対象ファイアウォールおよびアプライアンスに設定する Panorama IP アドレスの変数として使用できます。
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-new-features/panorama-features/configuration-reusability-for-templates-and-template-stacks.html

最新問題: **79**
ethernetl/8 に接続されている物理メディアを表示する CLI コマンドはどれですか?
A. > システム状態の表示 filter-pretty sys.si.p8.stats
B. > インターフェイス ethernetl/8 を表示
C. > システム状態の表示 filter-pretty sys.sl.p8.phy
D. > システム状態の表示 filter-pretty sys.si.p8.med
Answer: D (メーッセージを残す**)**
説明
出力例:
> システム状態の表示 filter-pretty sys.s1.p1.phy
sys.s1.p1.phy: {
リンクパートナー: { }、
メディア: CAT5、
タイプ: イーサネット、
}
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cld3CAC

最新問題: **80**
展示を参照してください。
転送された信頼証明書として使用できる証明書はどれですか?
A. ドメインサブCA
B. ドメイン ルート証明書

C. フォワード_トラスト
D. デフォルトの信頼証明機関からの証明書
Answer: A (メーッセージを残す**)**

最新問題**: 81**
IP アドレス 65.124.57.5 を持つ外部システムのユーザーは、4.2.2.2 の DNS サーバーに Web サーバーの IP アドレス www,xyz.com をクエリします。DNS サーバーはアドレス 172.16.15.1 を返します。Ire 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 NAT ルールを設定する必要がありますか?
A.
B.
C.
D.
Answer: C (メーッセージを残す**)**
宛先 NAT ルールで使用されるアドレスは、常にパケット内の元の IP アドレス (つまり、事前変換されたアドレス) を参照します。NAT ルールの宛先ゾーンは、元のパケットの宛先 IP アドレス (つまり、NAT 前の宛先 IP アドレス) のルート検索後に決定されます。セキュリティ ポリシー内のアドレスは、元のパケット内の IP アドレス (つまり、NAT 前のアドレス) も参照します。ただし、宛先ゾーンは、エンドホストが物理的に接続されているゾーンです。つまり、セキュリティ ルールの宛先ゾーンは、NAT 後の宛先 IP アドレスのルート検索後に決定されます。https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/nat/nat-configuration-examples/destination-nat-exampleone-to-one-mapping

最新問題**: 82**
セキュリティ第一のネットワークでは、アプリと脅威が動的に更新されるための推奨しきい値はどれくらいですか?
A. 36時間
B. 24時間
C. 1〜4時間
D. 6〜12時間
Answer: B (メーッセージを残す**)**

最新問題**: 83**
A/P ファイアウォール クラスターが IPsec トンネル セキュリティ アソシエーション (SA) を同期するとどうなりますか?
A. フェーズ 1 およびフェーズ 2 SA は HA3 リンク経由で同期されます。
B. フェーズ 1 SA は HA1 リンク経由で同期されます。
C. フェーズ 2 SA は HA2 リンク経由で同期されます。
D. フェーズ 1 およびフェーズ 2 SA は HA2 リンク経由で同期されます。
Answer: C (メーッセージを残す**)**

説明
以下の Palo Alto のドキュメントから、「VPN が Palo Alto ファイアウォール HA ペアで終端されると、すべての IPSEC 関連情報がファイアウォール間で同期されるわけではありません...これは予期される動作です。IKE フェーズ 1 SA 情報は、ファイアウォール間で同期されません。HA ファイアウォール。」2 番目のリンクから、「データ リンク (HA2) は、HA ペア内のファイアウォール間でセッション、転送テーブル、IPSec セキュリティ アソシエーション、および ARP テーブルを同期するために使用されます。HA2 リンク上のデータ フローは常に単方向です (HA2 キープを除く)。-alive)。アクティブ ファイアウォールからパッシブ ファイアウォールに流れます。」
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAuZCAW&lang=en_US%E
https://help.aryaka.com/display/public/KNOW/Palo+Alto+Networks+NFV+Technical+Brief

最新問題**: 84**
次のオブジェクトとポリシーは、デバイス グループ階層で定義されます。
Dallas-Branch は Dallas-Branch デバイス グループのメンバーとして Dallas-FW を持っています
NYC-DC は NYC-DC デバイス グループのメンバーとして NYC-FW を持っています　共有が未使用の場合、Dallas-FW はどのようなオブジェクトとポリシーを受け取るか」アドレスとサービス オブジェクト」は Panorama で有効になっていますか?
A. アドレスオブジェクト
- 共有アドレス1
- 支店住所1
ポリシー
- 共有ポリシー1
- ブランチポリシー1
B. アドレスオブジェクト
- 共有アドレス1
- 共有アドレス2
- 支店住所1
ポリシー
- 共有ポリシー1
- 共有ポリシー2
- ブランチポリシー1
C. アドレスオブジェクト
- 共有アドレス1
- 共有アドレス2
- 支店住所1
- DC アドレス 1
ポリシー
- 共有ポリシー1
- 共有ポリシー2

- ブランチポリシー1
D. アドレスオブジェクト
- 共有アドレス1
- 共有アドレス2
- 支店住所1
ポリシー
- 共有ポリシー1
- ブランチポリシー1
Answer: (解答を表示する**)**
Panorama は、Data-Centers グループから何もプッシュしません。つまりCは除外されます。
Panorama はすべてのオブジェクトを 共有」からプッシュするため、A は除外されます。
共有ポリシー 2」のターゲットは NYC-FW であるため、このポリシーは Dallas-FW にはプッシュされないことに注意してください。これによりBは除外されます。
したがって、答えはDです。

最新問題**: 85**
接続されているデバイスに動的更新をプッシュするように Panorama を設定するときに利用できる 2 つのサブスクリプションはどれですか? (2つお選びください。)
A. コンテンツID
B. アプリケーションと脅威
C. ウイルス対策
D. ユーザーID
Answer: (解答を表示する**)**

最新問題**: 86**
管理者が Facebook チャットをブロックし、Facebook を一般的に許可するセキュリティ ポリシー ルールはどれですか?
A. アプリケーション Facebook を許可する前に、アプリケーション Facebook-chat を拒否します。
B. Facebook のアプリケーションを上部で拒否します
C. アプリケーション Facebook を上部に許可する
D. アプリケーション facebook-chat を拒否する前に、アプリケーション facebook を許可します。
Answer: (解答を表示する**)**
参照：
https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-Consistently/ta-p/115673

最新問題**: 87**
アクティブ ファイアウォールが HA ピアとの通信を失ったときに、パッシブ ファイアウォールが引き継ぐまでに待機する時間を決定するのはどれくらいですか?

A. ハートビート間隔
B. 追加のマスターホールドアップ時間
C. プロモーション保留時間
D. 落下ホールドアップ時間の監視
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/high-availability/ha-concepts/ha-timers

最新問題**: 88**
管理者は、パロアルトネットワークス NGFW の管理インターフェイ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. debug dataplane packet-diag set capture stage firewall file 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 (TX、RX、DROP、ファイアウォール) をすべて有効にします。
C. debug dataplane packet-diag set Capture Stage Management File コマンドを使用します。
D. tcpdump コマンドを使用します。
Answer: D (メーッセージを残す**)**
参照：
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/monitoring/take-packet-captures/take-a-packet-capture-on-the-management-interface.html

最新問題**: 89**
ファイアウォール管理者は、ファイアウォール GUI に対して認証できません。
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るファイアウォール上の 2 つのログはどれですか? (2つお選びください。)
A. システムログ
B. ミリ秒ログ
C. dp-monitor .log
D. 認証ログ
E. トラフィックログ
Answer: A,D (メーッセージを残す**)**

最新問題**: 90**
ポリシーベース転送 (PBF) ポリシーを作成するときにアクションとして使用できるものは何ですか?
A. 次の VR
B. 許可する
C. 拒否
D. 破棄
Answer: (解答を表示する**)**

最新問題: **91**
管理者は認証強制を構成しており、特定のグループを認証から除外する除外ルールを作成したいと考えています。どの認証強制オブジェクトを選択する必要がありますか?
A. デフォルトブラウザチャレンジ
B. デフォルト認証バイパス
C. デフォルトの Web 形式
D. デフォルトのキャプティブポータルなし
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-web-interface-help/objects/objects-authentication.html

最新問題: **92**
管理者は、パロアルトネットワーク NGFW と集中管理パノラマ 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 プラクティスは何だと考えられますか?
A. パノラマとファイアウォールのアップグレードを同時に実行します。
B. まずファイアウォールをアップグレードし、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。
C. Panorama 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。
D. デバイス状態をエクスポートし、更新を実行してからデバイス状態をインポートします
Answer: C (メーッセージを残す**)**
Panorama は、ファイアウォールと同じバージョンまたはそれ以降のバージョンの機能リリースを実行している必要があります (3 つ以上の機能バージョンがサポートされていますが、推奨されません)。

最新問題: **93**
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、Panorama 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. ユニバーサル
B. マスター

C. グローバル
D. 共有
Answer: D (メーッセージを残す**)**
デバイス グループ階層で作成しているデバイス グループのすぐ上にある親デバイス グループ (デフォルトは共有) を選択します。
https://www.paloaltonetworks.com/documentation/70/panorama/panorama_adminguide/manage-firewalls/add-a-device-group#_26700

最新問題**: 94**
サイト A とサイト B の間にはサイト間 VPN が設定されています。OSPF は、サイト間のルートを動的に作成するように構成されています。サイト A の OSPF 構成は適切に構成されていますが、チューナーのルートが確立されていません。図のサイト B インターフェイスはブロードキャスト リンク タイプを使用しています。管理者は、サイト B の OSPF 構成でインターフェイスの 1 つに対して間違ったリンク タイプが使用されていると判断しました。
どのリンク タイプ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. イーサネット 1/1 を p2p に設定します
C. イーサネット 1/1 を p2mp に設定します
D. トンネルを設定します。1からp2pへ
Answer: D (メーッセージを残す**)**

最新問題**: 95**
復号化プロファイルを復号化ポリシー ルールに「いいえ」で割り当てることで得られる 2 つの利点はどれですか?
「復号化」アクション? (2 つ選択してください。)
A. 期限切れの証明書を持つセッションをブロックします。
B. クライアント認証によるセッションのブロック
C. サポートされていない暗号スイートを使用した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します。
E. 認証情報フィッシングをブロックします。
Answer: (解答を表示する**)**
説明/参照:
参考: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traffic-復号化/復号化プロファイルの作成

最新問題**: 96**
企業は、最小限の事前構成でリモート サイトにファイアウォールを送信できるように事前構成する必要があります。
導入後、各ファイアウォールは、将来の地域データ センターを含めるために、複数の地域データ センターへの安全なトンネルを確立する必要があります。

事前に構成された VPN 構成のうち、将来のサイトに展開するときに変更に適応できるのはどれですか?
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
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/globalprotect/network-globalprotect-portals/globalprotect-portals-satellite-configuration-tab.html

最新問題**: 97**
ある企業は、VLAN トランク リンク上の 2 つのコア スイッチ間に PA-3060 ファイアウォールをインストールしたいと考えています。各 VLAN を独自のゾーンに割り当て、タグなし (ネイティブ) トラフィックを独自のゾーンに割り当てる必要があります。複数の VLAN を個別のゾーンに区別するオプションはどれですか?
A. 2 つの V-Wire インターフェイスを持つ V-Wire オブジェクトを作成し、V-Wire オブジェクトの「タグ許可」フィールドに「0 ～ 4096」の範囲を定義します。
B. 2 つの V-Wire サブインターフェイスを持つ V-Wire オブジェクトを作成し、V-Wire オブジェクトの [タグ許可] フィールドに 1 つの VLAN ID だけを割り当てます。追加の VLAN ごとにこの手順を繰り返し、タグなしトラフィックには VLAN ID 0 を使用します。. 各インターフェイス/サブインターフェイスを一意のゾーンに割り当てます。
C. 単一の VLAN ID と共通の仮想ルーターにそれぞれ割り当てられるレイヤー 3 サブインターフェイスを作成します。物理レイヤー 3 インターフェイスは、タグなしのトラフィックを処理します。各インターフェイス/サブインターフェイス tA を割り当てます。ユニークなゾーン。どのインターフェイスにも IP アドレスを割り当てないでください。
D. VLAN ごとに VLAN オブジェクトを作成し、各 VLAN ID に一致する VLAN インターフェイスを割り当てます。追加の VLAN ごとにこの手順を繰り返し、タグなしトラフィックには VLAN ID 0 を使用します。各インターフェイス/サブインターフェイスを一意のゾーンに割り当てます。
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/networking/configure-interfaces/virtual-wire-interfaces/vlan-tagged-traffic
仮想ワイヤ インターフェイスはデフォルトですべてのタグなしトラフィックを許可します。ただし、仮想ワイヤを使用して 2 つのインターフェイスを接続し、どちらかのインターフェイスが仮想 LAN (VLAN) タグに基づいてトラフィックをブロックまたは許可するように設定できます。VLAN タグ 0 は、タグなしのトラフィックを示します。また、複数のサブインターフェイスを作成し、それらを異なるゾーンに追加して、VLAN タグまたは VLAN タグと IP 分類子 (アドレス、範囲、またはサブネット) の組み合わせに従ってトラフィックを分類し、特定の VLAN タグに対してきめ細かいポリシー制御を適用することもできます。特定の送信元 IP アドレス、範囲、またはサブネットからの VLAN タグの場合。

最新問題: **98**
管理者は、インターネット トラフィックにどの NAT ポリシーが使用されているかを特定する必要があります。
管理者は、ファイアウォール GUI の [監視] タブから、トラフィック フローにどの NAT ポリシーが使用されているかをどのように識別できますか?
A. [トラフィック ビュー] をクリックします。送信元または宛先 NAT 列が含まれていることを確認し、詳細ログ ビューで情報を確認してください。
B. [セッション ブラウザ] をクリックして、セッションの詳細を確認します。
C. [アプリ スコープ] > [ネットワーク モニター] をクリックし、NAT ルールのレポートをフィルターします。
D. [トラフィック ビュー] をクリックし、詳細ログ ビューで情報を確認します。
Answer: (解答を表示する**)**

最新問題: **99**
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. セッション情報
B. HA 状態情報
C. ユーザーID情報
D. 心拍数
Answer: (解答を表示する**)**

最新問題: **100**
示す：
図に示されている時間中に、トラフィックの入力インターフェイスが ethernet1/6 で送信元が 192.168.111.3 で、宛先が 10.46.41.113 である場合、出力インターフェイスはどうなりますか?
A. イーサネット1/5
B. イーサネット1/6
C. イーサネット1/3
D. イーサネット1/7
Answer: C (メーッセージを残す**)**

最新問題: **101**
ファイアウォール管理者は、会社のファイアウォールでのパケット バッファの使用率が高いことを調査しています。脅威ログを調べ、ファイアウォールによってドロップされる単一のソースからの多数のフラッド攻撃を確認した後、管理者は、同様の攻撃から保護するためにパケット バター保護を有効にすることを決定します。
管理者はファイアウォールでパケット バッファ保護をグローバルに有効にしていますが、それでもパケット バッファの使用率が高いことがわかります。
パケット バッファのオーバーフローを防ぐために、管理者は他に何をする必要がありますか?

A. 外部からのトラフィックを許可するすべてのセキュリティ ルールに、デフォルトの脆弱性保護プロファイルを追加します。
B. 影響を受けるゾーンのパケット バッファ保護を有効にします。
C. 影響を受けるゾーンにゾーン保護プロファイルを追加します。
D. 外部からのトラフィックを許可するセキュリティ ルールに DOS プロファイルを適用します。
Answer: B (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/zone-protection-and-dos-protection/zone-defense/p

最新問題**: 102**
出品物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 Palo Alto Networks NGFW があります。ネットワーク チームは、企業 WAN 上の過剰なトラフィックを報告しました。
パロアルトネットワークスの NGFW 管理者は、既存のすべての監視プラットフォームのサポートを維持しながら、どのようにして WAN トラフィックを削減できるのでしょうか?
A. 外部ソースからログを Panorama に転送して関連付けを行い、Panorama から NGFW に送信します。
B. M-500 上のどの構成でも、帯域幅不足の問題に対処できます。
C. すべてのリモート ファイアウォールでログ圧縮および最適化機能を構成します。
D. ファイアウォールからのログを Panorama にのみ転送し、Panorama が他の外部サービスにログを転送するようにします。
Answer: C (メーッセージを残す**)**

最新問題**: 103**
パロアルトネットワーク管理ポートとその接続先のスイッチ ポートの間で速度/デュプレックス ネゴシエーションの不一致が発生しています。
管理者はインターフェイスを 1Gbps にどのように設定しますか?
A. deviceconfig インターフェイス速度=二重 1Gbps-全二重を設定します。
B. deviceconfig システム速度=デュプレックス 1Gbps-デュプレックスを設定します。
C. deviceconfig システム速度=二重 1Gbps-全二重を設定します。
D. deviceconfig インターフェイス速度=二重 1Gbps-半二重を設定します。
Answer: (解答を表示する**)**
説明/参照: https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034

最新問題**: 104**
company.com は、アプリケーション オーバーライドを有効にしたいと考えています。次のスクリーンショットを考えてみます。

送信元トラフィックと宛先トラフィックがアプリケーション オーバーライド ポリシーに一致する場合、正しい 2 つのステートメントはどれですか?
(2つお選びください)
A. UDP ポート 16384 を利用するトラフィックは「ftp-base」として識別されるようになります。
B. トラフィックは UDP ポート 16384 上で強制的に動作します。
C. 「ftp-base」に一致するトラフィックは、App-ID エンジンと Content-ID エンジンをバイパスします。
D. UDP ポート 16384 を利用するトラフィックは、App-ID エンジンと Content-ID エンジンをバイパスします。
Answer: A,C (メーッセージを残す)

最新問題**: 105**
示す：
図に示されている時間中に、トラフィックの入力インターフェイスが ethernet1/6 で送信元が 192.168.111.3 で、宛先が 10.46.41.113 である場合、出力インターフェイスはどうなりますか?
A. イーサネット1/3
B. イーサネット1/5
C. イーサネット1/7
D. イーサネット1/6
Answer: (解答を表示する)

最新問題**: 106**
管理者は、パノラマ レポートでパロ アルト ネットワーク NGFW からのトラフィック ログを表示できません。構成の問題はファイアウォールにあるようです。正しく構成されていない場合、NGFW から Panorama へのトラフィック ログのみの送信を停止する可能性が最も高い設定はどれですか?
A)
B)
C)
A. オプション B
B. オプション C
C. オプション D
D. オプション A
Answer: (解答を表示する)

最新問題: 107
クライアントは、データセンター内に機密性の高いアプリケーション サーバーを備えており、分散型サービス拒否攻撃によるリソースの枯渇を特に懸念しています。
複数の IP アドレスから発生するリソース枯渇 (DDoS 攻撃) からこのサーバーを特別に保護するように、パロ アルト ネットワーク NGFW を構成するにはどうすればよいですか?
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. 攻撃をブロックする脆弱性保護プロファイルを追加します。
C. QoS プロファイルを追加して受信リクエストを抑制します。
D. セッション数が定義された DoS 保護プロファイルを追加します。
Answer: D (メーッセージを残す)
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/policy/dos-protection-profiles

最新問題: 108
ネットワーク セキュリティ管理者は、組織内に User-ID を導入する任務を負っています。
ネットワークでユーザー ID 情報を収集する 3 つの有効な方法は何ですか? （3つお選びください。）
A. Windows ユーザー ID エージェント
B. グローバルプロテクト
C. XMLAPI
D. 外部動的リスト
E. 動的ユーザーグループ
Answer: A,B,C (メーッセージを残す)
ユーザー ID は、ファイアウォールが IP アドレス、ユーザー名、またはその他の属性に基づいてユーザーとグループを識別できるようにする機能です。
ネットワークでユーザー ID 情報を収集するには、次の 3 つの有効な方法があります。
Windows ユーザー ID エージェント: これは、Windows サーバー上で実行され、Active Directory、Exchange サーバー、またはその他のソースからユーザー マッピング情報を収集するソフトウェア エージェントです。
GlobalProtect: これは、ユーザーとデバイスに安全なリモート アクセスを提供する VPN ソリューションです。また、GlobalProtect を使用してファイアウォールに接続するエンドポイントからユーザー マッピング情報も収集します。
XMLAPI: これは、サードパーティのアプリケーションまたはスクリプトが XML 形式を使用してユーザー マッピング情報をファイアウォールに送信できるようにするアプリケーション プログラミング インターフェイスです。

最新問題: **109**
エンジニアは、パロ アルト ネットワーク ファイアウォールをインターネット ゲートウェイの VWire モードで実装したいと考えており、vwire インターフェイスでサポートされている機能を確認したいと考えています。VWire インターフェイスでサポートされている 3 つの機能は何ですか? (3つお選びください)
A. NAT
B. QoS
C. IPSec
D. OSPF
E. SSL 復号化
Answer: A,B,E (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/virtual-wire-interfa
仮想ワイヤーは、セキュリティ ポリシー ルール、App-ID、Content-ID、User-ID、復号化、LLDP、アクティブ/パッシブおよびアクティブ/アクティブ HA のサポートに加えて、仮想 LAN (VLAN) タグに基づいたトラフィックのブロックまたは許可をサポートします。、QoS、ゾーン保護 (一部の例外を除く)、非 IP プロトコル保護、DoS 保護、パケット バッファー保護、トンネル コンテンツ インスペクション、および NAT。

最新問題: **110**
管理者は PAN-OS SD-WAN を設定しており、すでに終了したセッションのセッション フェイルオーバーの理由を調べる要求を受け取りました。これは Panorama ログまたはファイアウォール ログのどこで見つかりますか?
A. セッションブラウザ
B. トラフィックログ
C. 閉じられたセッションではフェイルオーバーの詳細が見つかりません
D. システムログ
Answer: B (メーッセージを残す**)**

最新問題: **111**
スタック内の複数のテンプレートを使用して多数のファイアウォールを管理すると、どの 2 つの利点がありますか?
(2つお選びください。)
A. ファイアウォールの共通の標準テンプレート構成を定義します。
B. すべてのスタックにわたってサーバー プロファイルと認証構成を標準化します。
C. テンプレートからアドレス オブジェクトを継承します。
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します。
Answer: (解答を表示する**)**

最新問題: **112**
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つお選びください。）
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
Answer: A,B,D,F (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/8-0/pan-os-admin/authentication/authentication-types/multi-factor-authentication

最新問題: **113**
管理者は、DMZ とコア ネットワーク EIGRP の間に NGFW を実装する必要があります。2 つの環境間のルーティングが必要です。どのインターフェイス 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 3 インターフェイスですが、接続されている仮想ルータ上で EIGRP を設定しています
B. 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
C. レイヤ 3 または集約イーサネット インターフェイスですが、サブインターフェイスのみで EIGRP を設定します
D. IPsec トンネル上の EIGRP ルーティングを終了するトンネル インターフェイス (LSVPN 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)
Answer: (解答を表示する**)**
説明
EIGRP はシスコ独自のプロトコルです。PAN でサポートされている動的ルーティング プロトコルは、RIPv2、OSPF、および BGP です。

最新問題: **114**
管理者は、管理者の自宅で Cisco ASA への IPSec VPN を設定していますが、接続を完了する際に問題が発生しています。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. デッド ピア検出設定がパロ アルト ネットワーク ファイアウォールと ASA の間で一致しません。
B. パロアルトネットワーク 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. パブリック IP アドレスが、パロ アルト ネットワーク ファイアウォールと ASA の両方で一致しません。
D. 共有シークレットがパロアルトネットワークファイアウォールと ASA の間で一致しません。
Answer: (解答を表示する**)**

最新問題: **115**
あ
Palo Alto Networks NGFW を通過するユーザーのトラフィックは、http://www.company.com に到達する場合があります。それ以外の場合は、セッションがタイムアウトになります。NGFW は、ユーザーのトラフィックが http://www.company.com にアクセスするときに一致する PBF ルールを使用して構成されています。
ネクストホップがダウンした場合に PBF ルールを自動的に無効にするファイアウォールを構成するにはどうすればよいですか?
A. ファイアウォールの外部インターフェイスのリンク監視プロファイルを有効にして構成します。
B. 問題の PBF ルールに 回復を待つ」アクションを持つモニター プロファイルを作成して追加します。
C. 仮想ルータ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経路監視を設定します。
D. 問題の PBF ルールにフェイルオーバーのアクションを持つモニター プロファイルを作成して追加します。
Answer: (解答を表示する**)**

最新問題: **116**
管理者には、復号化されたトラフィックをパロアルトネットワーク 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という要件があります。
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. Threat Analysis ライセンスを使用した暗号化ミラー インターフェイス
B. 復号化ポート エクスポート ライセンスを備えた仮想ワイヤ インターフェイス
C. 復号化ポートミラーライセンスを持つタップインターフェース
D. 関連付けられた復号化ポート ミラー ライセンスを持つ復号化ミラー インターフェイス
Answer: D (メーッセージを残す**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption-concepts/decryption-mirroring

最新問題: **117**
decrypt-cert-validation エラーを受け取る正当な理由ではないものはどれですか?
A. サポートされていない HSM
B. 不明な証明書ステータス
C. クライアント認証
D. 信頼できない発行者
Answer: A (メーッセージを残す**)**
説明/参照: https://www.paloaltonetworks.com/documentation/71/pan-os/newfeaturesguide/networking-features/ssl-ssh-session-end-reasons

最新問題: **118**
上のスクリーンショットで、表示されている ACC 構成から判断できる 2 つの情報はどれですか? (2つお選びください)
A. [ネットワーク アクティビティ] タブには、FTP を含むすべてのアプリケーションが表示されます。
B. 重大度が 「高」の脅威は、常に脅威名リストの先頭に表示されます。
C. ACC は FTP アプリケーションのみを表示するようにフィルターされています。
D. 安全でない認証情報、ブルート フォース、およびプロトコル異常はすべて、脆弱性の脅威タイプの一部です。
Answer: A,D (メーッセージを残す**)**

最新問題: **119**
[アプリケーション] 列のどの値が、App-ID 署名と一致しなかった UDP トラフィックを示していますか?
A. 該当なし
B. 未完了
C. 不明な IP
D. 不明な UDP
Answer: (解答を表示する**)**
説明
アプリケーションを安全に有効にするには、すべてのポートにわたるすべてのトラフィックを常に分類する必要があります。App-ID を使用すると、ACC およびトラフィック ログで通常、不明なトラフィック (tcp、udp、または非 syn-tcp) として分類されるアプリケーションは、App-ID にまだ追加されていない市販のアプリケーション、内部またはネットワーク上のカスタム アプリケーションや潜在的な脅威。
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/app-id/use-application-objects-in-policy/create-a-cu

最新問題: **120**
管理者は Panorama と複数の Palo Alto Networks NGFW 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が Panorama に表示されません。
どのアクションにより、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なりますか?
A. ACC を使用して既存のログを統合します。
B. CLI コマンドは、既存のログを Panorama に転送します。
C. インポート オプションを使用して、ログを Panorama にプルします。

D. ログ データベースはファイアウォールからエクスポートし、Panorama に手動でインポートする必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 121**
ユーザー名を動的ユーザー グループに含めるためにタグ付けするために使用できる 2 つの機能はどれですか? (2つお選びください)
A. ログ転送の自動タグ付け
B. GlobafProtect エージェント
C. ユーザー ID Windows ベースのエージェント
D. XML API
Answer: A,C (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/register-ip-addresses-and-tags-dynamically。
次のオプションのいずれかを使用して、動的登録プロセスを有効にできます。
Windows 用ユーザー ID エージェント*
VM 情報ソース
パノラマプラグイン
VMware サービス マネージャー
XML API*
自動タグ*
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/education/pcnse-study-guide.p ログ転送の自動タグ付け機能を使用して、ユーザー名にタグを付けたりタグを外したりすることもできます。プロフィール。また、別のユーティリティをプログラムして、PAN-OS XML API コマンドを呼び出して、ユーザー名をタグ付けまたはタグ解除することもできます。

最新問題**: 122**
エンジニアはダイナミック 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必要がなく、ユーザーをメンバーとして自動的に含めます。

B. DUG は、管理者にパロアルトネットワークファイアウォール上の管理インターフェイスへのアクセスのみを許可するために使用されます。
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. 定期的な間隔でコミットをスケジュールし、指定されたタグに一致する新しいユーザーで DUG を更新します
Answer: (解答を表示する**)**
動的ユーザー グループは、ユーザーの可視性を維持しながら、異常なユーザーの動作や悪意のあるアクティビティを自動修復するポリシーを作成するのに役立ちます。以前は、不審なアクティビティに応じてユーザーを隔離するには、時間とリソースを消費してグループのすべてのメンバーを更新したり、IP アドレスとユーザー名のマッピングをラベルに更新して、ユーザーの可視性を犠牲にしてポリシーを適用したりする必要がありました。ファイアウォールがトラフィックをチェックするまで待機します。動的ユーザー グループを構成して、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、ユーザーを自動的にメンバーとして含めることができ、ファイアウォールがトラフィックをスキャンする前でもデバイス レベルでユーザーとデータの相関関係を維持できるようになりました。
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html

最新問題**: 123**
ネットワーク セキュリティ エンジニアは、BGP プロトコルを使用して、PAN-OS ファイアウォール上の仮想ルーターと外部ルーターのピアリングを試みています。仲間関係が確立されていない。2 つのデバイス間の BGP 状態の現在の状態を確認するには、エンジニアはどのようなコマンドを実行できますか?
A. ルーティングプロトコルの bgp 状態を表示
B. ルーティング プロトコルの BGP 概要を表示します。
C. ルーティング プロトコル bgp rib-out を表示します。
D. ルーティング プロトコルの BGP ピアを表示します。
Answer: (解答を表示する**)**

最新問題**: 124**
管理者は、NGFW を PAN-OS ソフトウェアの最新バージョンにアップグレードする必要があります。
次のようなことが起こっています。
- ファイアウォールは e 1/1 を介してインターネットに接続します。
- デフォルトのセキュリティ ルールとすべての SSL および Web を許可するセキュリティ ルール
-
任意のゾーンとの間で送受信されるトラフィックの閲覧。
- サービス ルートが設定され、e1/1 から更新トラフィックを供給します。
- アップデート時に通信エラーがシステムログに記録される

実行されました。
・ダウンロードが完了しない。
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. 静的ルート ポインティング アプリケーション PaloAlto がアップデート サーバーにアップデートします
B. PAN-OS ソフトウェアの時間指定ダウンロードのスケジューラー
C. 解決に使用するファイアウォールの DNS 設定
D. PaloAlto アップデート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
Answer: C (メーッセージを残す)

最新問題**: 125**
すべての IP アドレスからユーザーへのマッピングが常に明示的に知られている必要がある高セキュリティ環境では、どのユーザー ID マッピング方法を使用する必要がありますか?
A. LDAP サーバー プロファイルの構成
B. グローバルプロテクト
C. Windows ベースのユーザー ID エージェント
D. PAN-OS 統合 User-ID エージェント
Answer: (解答を表示する)

最新問題**: 126**
上のスクリーンショットで、表示されている ACC 構成から判断できる 2 つの情報はどれですか? (2つお選びください)
A. [ネットワーク アクティビティ] タブには、FTP を含むすべてのアプリケーションが表示されます。
B. 重大度が 「高」の脅威は、常に脅威名リストの先頭に表示されます。
C. 安全でない認証情報、ブルート フォース、およびプロトコル異常はすべて脆弱性の脅威タイプの一部です。
D. ACC は FTP アプリケーションのみを表示するようにフィルターされています。
Answer: C,D (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/threat-prevention/threat-signature

最新問題**: 127**
パノラマの次の画像で、一部の値が赤で表示されているのはなぜですか?
A. sg2 のセッションしきい値の設定が間違っています。
B. us3 のロギング レートが、管理者が設定したしきい値から逸脱しています。
C. uk3 のロギング レートは、計算された 7 日間のベースラインから逸脱しています。
D. sg2 セッション数が他の管理対象デバイスと比較して最も少ない。
Answer: D (メーッセージを残す)

最新問題: **128**
Web サーバーは、ポート 8080 で HTTP トラフィックをリッスンするように構成されています。クライアントは、TCP ポート 80 の IP アドレス 1.1.1.100 を使用して Web サーバーにアクセスします。宛先 NAT ルールは、IP アドレスとレポートの両方を 10.1.1.100 に変換するように構成されています。TCP ポート 8080。
ファイアウォールでどの NAT ルールとセキュリティ ルールを設定する必要がありますか? (2つお選びください)
A. Web ブラウジング アプリケーションを使用した、untrust-l3 ゾーンのソースから dmz-l3 ゾーンの 1.1.100 の宛先までのセキュリティ ポリシー。
B. service-http サービスを使用する、untrust-l3 ゾーンの送信元から untrust-l3 ゾーンの 1.1.1.100 の宛先までの NAT ルール。
C. service-http サービスを使用する、untrust-l3 ゾーンの送信元から dmz-zone の 10.1.1.100 の宛先までの NAT ルール。
D. Web ブラウジング アプリケーションを使用した、untrust-l3 ゾーンのソースから dmz-l3 ゾーンの 10.1.1.100 の宛先までのセキュリティ ポリシー
Answer: A,C (メーッセージを残す**)**

最新問題: **129**
ファイアウォールのペアでアクティブ/パッシブ モードで HA を構成した後、管理者は次の詳細を含む失敗したコミットを受け取ります。
この種の問題について 2 つの説明は何ですか? (2つお選びください)
A. 管理インターフェイスまたはデータ プレーン インターフェイスのいずれかが HA1 バックアップとして使用されます。
B. ピア IP は管理インターフェイス設定の許可リストに含まれていません
C. コミットの発行時にバックアップ ピア HA1 IP アドレスが構成されていませんでした
D. ファイアウォールの 1 つがサスペンド状態になりました
Answer: (解答を表示する**)**

最新問題: **130**
管理者は、DMZ とコア ネットワークの間に NGFW を実装する必要があります。
2 つの環境間の EIGRP ルーティングが必要です。このビジネス要件をサポートするインターフェイス タイプはどれですか?
A. EIGRP ルーティングがコアと DMZ の間に留まるようにするための仮想ワイヤ インターフェイス
B. IPsec トンネル上の EIGRP ルーティングを終了するトンネル インターフェイス (LSVPN 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. レイヤ 3 または集約イーサネット インターフェイス、ただしサブインターフェイスのみで EIGRP を設定
D. レイヤ 3 インターフェイスですが、接続された仮想ルータ上で EIGRP を設定します

Answer: C (メーッセージを残す)

最新問題: **131**
次の図に基づいて、ルート、中間、およびエンドユーザー証明書の正しいパスはどれですか?
A. シマンテック > ベリサイン > パロアルトネットワークス
B. ベリサイン > シマンテック > パロアルトネットワークス
C. ベリサイン > パロアルトネットワークス > シマンテック
D. パロアルトネットワークス > シマンテック > ベリサイン
Answer: (解答を表示する)

最新問題: **132**
HA プロモーションの保持時間を最もよく表すものは何ですか?
A. 隣接デバイスが時折発生する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の待機時間
D. デバイス優先度の低いパッシブ ファイアウォールが、ファイアウォールが再び動作可能になった場合に、アクティブ ファイアウォールとして引き継ぐまでに待機する時間
Answer: C (メーッセージを残す)
説明
HA プロモーション ホールド タイムは、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です。: PAN-OS 新機能ガイド

最新問題: **133**
エンジニアは、ファイアウォールとスイッチ間の帯域幅と冗長性を高めるために集約インターフェイスを構成したいと考えています。集約インターフェイス グループに割り当てられたインターフェイスの設定について正しいのはどれですか?
A. 異なる帯域幅を持つことができます。
B. レイヤ 3 やレイヤ 2 など、異なるインターフェイス タイプを持つことができます。
C. 集約インターフェイス グループとは異なるインターフェイス タイプを持つことができます。
D. 光ファイバーと銅線を混在させる機能など、さまざまなハードウェア メディアを搭載できます。
Answer: D (メーッセージを残す)
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/networking/configure-interfaces/configure-an-aggregate-interface-group

最新問題: **134**

ゾーン保護プロファイルでのみ使用できる保護機能はどれですか?
A. SYN フラッド Cookie を使用した SYN フラッド防御
B. ICMP フラッド保護
C. ポートスキャン保護
D. UDP フラッド保護
Answer: (解答を表示する**)**
説明
https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-web-interface-help/network/network-network-profiles-zone

最新問題**: 135**
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設定が行われるのはどのアクションですか?
A. 脆弱性のシグネチャが検出されない限り、この構成では一致したセッションが許可されます。の 「拒否」アクションは、関連する脆弱性で定義された重大度ごとに定義されたアクションよりも優先されます。
保護プロファイル。
B. 設定が不正です。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。警告が表示されます
コミット中に表示されます。
C. 設定が不正です。アクションが 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"。
D. 設定は有効です。これにより、ファイアウォールは一致するセッションを拒否します。任意の設定済み
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、セキュリティ プロファイルは効果がありません。
Answer: A (メーッセージを残す**)**

最新問題**: 136**
システム管理者は、脆弱性チェックの一環として、会社のツールを使用してポート スキャンを実行します。管理者は、スキャンが脅威として識別され、ファイアウォールによってドロップされたことに気づきました。管理者はログをさらに調査した結果、スキャンが脅威ログに記録されていないことを発見しました。
ツールがファイアウォールを通過できるようにするには、管理者は何をすべきですか?
A. ゾーン設定からゾーン保護プロファイルを削除します。
B. DoS 保護プロファイルの偵察保護ソース アドレス除外にツールの IP アドレスを追加します。

C. ツールの IP アドレスを、ゾーン保護プロファイルの偵察保護ソース アドレス除外に追加します。
D. ゾーン保護プロファイルの TCP ポート スキャン アクションをブロックからアラートに変更します。
Answer: B (メーッセージを残す**)**

最新問題**: 137**
ファイアウォール上でローカルにのみ構成でき、Panorama テンプレートまたはテンプレート スタックからプッシュできない 2 つの設定はどれですか? (2つお選びください。)
A. ネットワークインターフェースのタイプ
B. ゾーン保護プロファイル
C. HA1 IP アドレス
D. マスターキー
Answer: C,D (メーッセージを残す**)**

最新問題**: 138**
管理者のパロアルトネットワークス NGFW 宛ての VPN トラフィックが、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とき、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. リプレイ
B. Web アプリケーション
C. DoS 保護
D. ゾーン保護
Answer: A (メーッセージを残す**)**

最新問題**: 139**
管理者は Panorama と複数の Palo Alto Networks NGFW 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が PanoramA に表示されません。

どのアクションにより、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なりますか?
A. インポート オプションを使用してログを取得します。
B. ログデータベースをエクスポートします。
C. scp logdb エクスポート 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。
Answer: C (メーッセージを残す**)**
コマンド:
ログデータベースをリクエストする
パノラマへの移行開始終了時間開始時間タイプ
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/merge-panorama-logs-to-new-ログ形式

最新問題**: 140**
管理者は、トラフィック ログで、unknown-tcp として識別されるいくつかの受信セッションを確認します。の
管理者は、これらのセッションが会社の専有情報にアクセスする外部ユーザーからのものであると判断します。
会計アプリケーション。管理者は、このトラフィックを自分のアカウントとして確実に識別したいと考えています。
アプリケーションを削除し、このトラフィックの脅威をスキャンします。
どのオプションを選択するとこの結果が得られますか?
A. カスタム App-ID を作成し、 順序付けされた条件」チェック ボックスを使用します。
B. アプリケーション オーバーライド ポリシーとアプリケーションのカスタム脅威シグネチャを作成します。
C. カスタム App-ID を作成し、詳細タブでスキャンを有効にします。
D. アプリケーション オーバーライド ポリシーを作成します。
Answer: C (メーッセージを残す**)**

最新問題**: 141**
パロアルトネットワーク管理ポートと、それに接続されているスイッチ ポートの間で速度/デュプレックス ネゴシエーションの不一致が発生しています。管理者はインターフェイスを 1Gbps にどのように設定しますか?
A. deviceconfig インターフェイス速度二重 1Gbps-全二重を設定します。
B. deviceconfig システム速度デュプレックス 1Gbps-デュプレックスを設定します。
C. deviceconfig システム速度二重 1Gbps-全二重を設定します。
D. deviceconfig インターフェイス速度二重 1Gbps-半二重を設定します。
Answer: C (メーッセージを残す**)**
参照：

<https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-Duplex-of-the-Management-Port/ta-p/59034> user@PA# set deviceconfig システム速度二重 100Mbps-全二重 100Mbps-全二重 100Mbps-半二重 100Mbps-半二重 10Mbps-全二重 10Mbps-全二重 10Mbps-半二重 10Mbps-半二重 1Gbps-全二重1Gbps-全二重 1Gbps-半二重 1Gbps-半二重 自動ネゴシエート 自動ネゴシエート

最新問題: **142**
管理者は、レイヤー 7 署名を含むカスタム アプリケーションを作成します。最新のアプリケーションと
脅威の動的アップデートは同じ NGFW にダウンロードされます。アップデートには、次のアプリケーションが含まれています。
カスタム アプリケーションと同じトラフィック シグネチャと一致します。
NGFW を通過するトラフィックを識別するにはどのアプリケーションを使用する必要がありますか?
A. カスタムおよびダウンロードされたアプリケーション署名ファイルがマージされ、両方が使用されます。
B. カスタムアプリケーション
C. システム ログにはアプリケーション エラーが示されており、どちらの署名も使用されていません。
D. ダウンロードしたアプリケーション
Answer: B (メーッセージを残す**)**

最新問題: **143**
テンプレート スタックがデバイスに割り当てられており、そのスタックに重複する設定を持つ 3 つのテンプレートが含まれている場合、テンプレート スタックがプッシュされたときにどの設定がデバイスに公開されますか?
A. スタックの最上位にあるテンプレートに割り当てられた設定。
B. 管理者は、選択したファイアウォールの設定を選択するように求められます。
C. すべてのテンプレートで構成されているすべての設定。
D. ファイアウォールの場所に応じて、Panorama が送信する設定を決定します。
Answer: (解答を表示する**)**
参照：
https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/manage-firewalls/manage-templates-and-template-stacks/configure-a-template-stack

最新問題: **144**
ある企業がネットワーク内で WildFire を利用し始めました。
サポートされている 3 つのファイル タイプはどれですか? (3つお選びください。)
A. JAR
B. PST

C. PDF
D. JPG
E. EXE
Answer: (解答を表示する**)**
https://www.paloaltonetworks.com/documentation/70/wildfire/wf_admin/wildfire-overview/wildfire-concepts.html

最新問題**: 145**
変数名はどの記号で始める必要がありますか?
A. $
B. &
C. #
D. !
Answer: A (メーッセージを残す**)**

最新問題**: 146**
管理者は、パロアルトネットワークス NGFW の管理インターフェイ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. debug dataplane packet-diag set capture stage firewall file 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 (TX、RX、DROP、ファイアウォール) をすべて有効にします。
C. debug dataplane packet-diag set Capture Stage Management File コマンドを使用します。
D. topdumpコマンドを使用します。
Answer: (解答を表示する**)**
https://live.paloaltonetworks.com/t5/Management-Articles/How-To-Packet-Capture-tcpdump-On-Management-Interface/ta-p/55415

最新問題**: 147**
パロアルトネットワークスのデバイス テレメトリ データは、デバイス証明書がインストールされているファイアウォール上のどこに保存されますか?
A. Cortex データ レイク
B. パノラマ
C. パロアルトネットワーク更新サーバー上
D. M600 ログ コレクター
Answer: A (メーッセージを残す**)**
デバイス テレメトリ データは、ファイアウォールやその他のソースからログを収集して保存するクラウドベースのサービスである Cortex Data Lake3 に保存されます。Cortex Data Lake では、さまざまなアプリケーションを使用してデータを分析および視覚化することもできます。

デバイス テレメトリを使用するには、ファイアウォールにデバイス証明書をインストールする必要があります3。この証明書は、ファイアウォールを Cortex Data Lake に対して認証し、転送中のデータを暗号化します。

最新問題: **148**
WildFire が分析サンプルに対して提供できる 3 つの可能な判定は何ですか? (3つお選びください)
A. きれい
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
Answer: B,E,F (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict

最新問題: **149**
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ことで得られる 2 つの利点はどれですか。
「復号化なし」アクションはありますか? (2つお選びください。)
A. 期限切れの証明書を持つセッションをブロックします。
B. クライアント認証によるセッションのブロック
C. サポートされていない暗号スイートを使用した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します。
E. 認証情報フィッシングをブロックします。
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/pan-os/8-1/pan-os-admin/decryption/decryption-concepts/no-decryption-decryption-profile

最新問題: **150**
サービス ルートと仮想システムを正確に説明しているのはどれですか?
A. 仮想システムは、ファイアウォールのすべてのグローバル サービスおよびサービス ルートに対して 1 つのインターフェイスのみを使用できます。
B. インターフェイスは、必要な外部サービスへのトラフィックに使用する必要があります。
C. 特定のサービス ルートが構成されていない仮想システムは、ファイアウォールのグローバル サービスおよびサービス ルート設定を継承します。
D. 仮想システムには専用のサービス ルートを構成することはできません。仮想システムは常にファイアウォールのグローバル サービスとサービス ルート設定を使用します。
Answer: C (メーッセージを残す**)**
説明

複数の仮想システムに対してファイアウォールが有効になっている場合、仮想システムはグローバル サービスおよびサービス ルート設定を継承します。」したがって、必要に応じて特定のサービス ルートを定義できますが、それらはグローバル設定から継承されたものとして開始されます。

最新問題: **151**
ある企業は、パロアルトネットワークスの次世代ファイアウォールの背後で、次の構成情報を備えたパブリックにアクセス可能な Web サーバーをホストしています。
※社外のユーザーは「Untrust-L3」ゾーンに入ります。
* Web サーバーは物理的に「Trust-L3」ゾーンに存在します。
※Webサーバーのパブリック IPアドレス :23.54.6.10
※Webサーバーのプライベート IPアドレス :192.168.1.10
Untrust-L3 ゾーンのユーザーが Web サーバーにアクセスできるようにするには、NAT ポリシーに含める必要がある 2 つの項目はどれですか?
(2つお選びください。)
A. 宛先 IP 23.54.6.10
B. 送信元ゾーンと宛先ゾーンの両方に UntrustL3
C. 送信元ゾーンには UntrustL3、宛先ゾーンには Trust-L3
D. 宛先IP 192.168.1.10
Answer: A,B (メーッセージを残す**)**

最新問題: **152**
展示を参照してください。
転送された信頼証明書として使用できる証明書はどれですか?
A. デフォルトの信頼証明機関からの証明書
B. ドメインサブ CA
C. フォワード_トラスト
D. ドメイン ルート証明書
Answer: B (メーッセージを残す**)**

最新問題: **153**
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. セッション情報

B. 心拍数
C. HA 状態情報
D. ユーザーID情報
Answer: (解答を表示する**)**
説明/参照: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts/ha-links-and-backup-links

最新問題**: 154**
パノラマとログ コレクターを 10.2 x にアップグレードしました。Panorama を使用してファイアウォール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. パノラマ/マスター キーと診断でマスター キーを更新します。
B. パノラマ/管理対象デバイス/概要でファイアウォールを再度関連付けます。
C. Palo Alto Network Support - パノラマ/ライセンス/ライセンス サーバーからのライセンス キーの取得を使用してライセンスを更新します。
D. 構成をコミットしてファイアウォールにプッシュします。
Answer: (解答を表示する**)**

最新問題**: 155**
ファイアウォール管理者がセッションが復号化されたかどうかを判断できるログはどれですか?
A. 相関イベント
B. 交通状況
C. 復号化
D. セキュリティポリシー
Answer: C (メーッセージを残す**)**
説明
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/d 復号ログ (モニター ログ復号) は、一致するセッションに関する包括的な情報を提供します。復号化ポリシー。そのトラフィックに関するコンテキストを取得して、復号化の問題を正確かつ簡単に診断して解決できるようにします。トラフィックが復号化ポリシーに一致しない場合、ファイアウォールはトラフィックをログに記録しません。

最新問題**: 156**
管理者は、NGFW 自体を経由しない専用パスを介してインターネットに接続するようにパロアルトネットワーク NGFW の管理インターフェイスを構成しました。
ファイアウォールがアプリケーション署名を自動的に更新できるようにするには、どの構成設定または手順を選択しますか?
A. アプリケーション署名用にスケジューラを構成する必要があります。

B. ファイアウォールからアップデート サーバーへのアップデート リクエストを許可するようにセキュリティ ポリシー ルールを構成する必要があります。
C. 脅威対策ライセンスをインストールする必要があります。
D. サービスルートを設定する必要があります。
Answer: D (メーッセージを残す**)**
説明
ファイアウォールはサービス ルートを使用してアップデート サーバーに接続し、新しいコンテンツ リリース バージョンを確認し、利用可能なアップデートがある場合はリストの先頭に表示します。
参照：
https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-dynamic-updates

最新問題**: 157**
ファイアウォールのデフォルトの TCP および UDP 設定では、次のセッションで識別されるアプリケーションは何になりますか?
A. 不明な TCP
B. データ不足
C. 適用外
D. 未完了
Answer: (解答を表示する**)**

最新問題**: 158**
管理者は、NGFW 上の仮想ルーターで 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ません。管理者がこの問題をトラブルシューティングできるようにする 2 つのオプションはどれですか? (2つお選びください。)
A. BGP アップデートとして転送する再配布プロファイルを追加します。
B. システムログを表示します。
C. 仮想ルーターの実行時統計を表示します。
D. ルーティング段階でトラフィック pcap を実行します。
Answer: B,C (メーッセージを残す**)**

最新問題**: 159**
基本的な WildFire サービスの一部として、分析のために WildFire に転送できる 3 つのファイル タイプはどれですか?
（3つお選びください。）
A. .dll
B. .exe
C. .src
D. .apk

E. .pdf
F. .jar
Answer: (解答を表示する**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/wildfire-file-type-support

最新問題**: 160**
管理者は、すべての管理サービスにデフォルト ポートを使用するようにファイアウォールを解除しました。データ プレーンによって実行される 3 つの機能はどれですか? (3つお選びください。)
A. ウイルス対策
B. NAT
C. ファイルのブロック
D. NTP
E. WildFire のアップデート
Answer: (解答を表示する**)**

最新問題**: 161**
SAML SLO は、どの 2 つのファイアウォール機能でサポートされていますか? (2つお選びください。)
A. GlobalProtect ポータル
B. キャプティブポータル
C. WebUI
D. CLI
Answer: A,B (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-saml-authentication

最新問題**: 162**
ターミナル サーバー経由で接続しているユーザーのユーザー名に IP アドレスをマップするには、どのユーザー ID メソッドを構成する必要がありますか?
A. ポートマッピング
B. サーバー監視
C. クライアントのプローブ
D. XFF ヘッダー
Answer: A (メーッセージを残す**)**
説明/参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user-mapping-for-terminal-server-users

最新問題**: 163**

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には、構成内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テンプレート変数を作成できます。
どれが正しい構成ですか
A. パノラマ(&P)
B. @パノラマ
C. $パノラマ
D. #パノラマ
Answer: C (メーッセージを残す**)**
新しい変数を追加します。
変数名はドル記号 ($) で始まる必要があります。
新しい変数に名前を付けます。この例では、変数の名前は $DNS-primary および $DNS-Secondary です。

。
変数のタイプを選択します
をクリックし、選択した変数タイプに対応する値を入力します。
この例では、「IP ネットマスク」を選択します。

。
(オプション
) 変数の説明を入力します。
「OK」をクリックします
そして閉じる
https://docs.paloaltonetworks.com/panorama/10-0/panorama-admin/manage-firewalls/manage-templates-and-template-stacks/configure-template-or-template-stack-variables.html#id17B8D0PG0TA

最新問題**: 164**
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何ですか?
A. Microsoft Exchange、Microsoft Active Directory、および Novell eDirectory
B. Novell eDirectory、Microsoft ターミナル サーバー、および Microsoft Active Directory
C. Microsoft ターミナル サーバー、Red Hat Linux、および Microsoft Active Directory
D. Microsoft Active Directory、Red Hat Linux、および Microsoft Exchange
Answer: D (メーッセージを残す**)**

最新問題**: 165**
パケット バッファ保護に関する情報はどこに記録されますか?
A. アラート エントリはアラーム ログにあります。ドロップされたトラフィック、破棄されたセッション、およびブロックされた IP アドレスのエントリは、脅威ログに記録されます。
B. すべてのエントリはシステム ログにあります

C. アラート エントリはシステム ログにあります。ドロップされたトラフィック、破棄されたセッション、およびブロックされた IP アドレスのエントリは、脅威ログに記録されます。
D. すべてのエントリはアラーム ログにあります
Answer: D (メーッセージを残す**)**

最新問題**: 166**
出品物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 Palo Alto Networks NGFW があります。ネットワーク チームは、企業 WAN 上の過剰なトラフィックを報告しました。
パロアルトネットワークスの NGFW 管理者は、既存のすべての監視/セキュリティ プラットフォームのサポートを維持しながら、どのようにして WAN トラフィックを削減できるのでしょうか?
A. ファイアウォールからのログを Panorama にのみ転送し、Panorama が他の外部サービスにログを転送するようにします。
B. 外部ソースからログを Panorama に転送して関連付けを行い、Panorama から NGFW に送信します。
C. すべてのリモート ファイアウォールでログ圧縮および最適化機能を構成します。
D. M-500 上のどの構成でも、帯域幅不足の問題に対処できます。
Answer: (解答を表示する**)**
https://docs.paloaltonetworks.com/panorama/8-1/panorama-admin/panorama-overview/centralized-logging-and-reporting

最新問題**: 167**
インターネット ゾーン上のユーザーが DMZ ゾーンでホストされている Web サーバーに正常に接続できるのは、どのゾーン ペアとルール タイプですか? Web サーバーは、パロアルトネットワークファイアウォールの宛先 NAT ポリシーを使用して到達可能です。
A.
B.
C.
D.
Answer: B (メーッセージを残す**)**

最新問題: **168**
管理者は、パロアルトネットワークス NGFW の管理インターフェイスを、
NGFW 自体を経由しない専用パスを介してインターネットに接続します。
ファイアウォールがアプリケーション署名を自動的に更新できるようにするには、どの構成設定または手順を選択しますか?
A. アプリケーション署名用にスケジューラを構成する必要があります。
B. ファイアウォールからファイアウォールへの更新リクエストを許可するようにセキュリティ ポリシー ルールを構成する必要があります。
サーバーを更新します。
C. 脅威対策ライセンスをインストールする必要があります。
D. サービスルートを設定する必要があります。
Answer: (解答を表示する**)**
説明/参照:
Explanation:
ファイアウォールはサービス ルートを使用してアップデート サーバーに接続し、新しいコンテンツのリリースを確認します。
バージョンを確認し、利用可能なアップデートがある場合はリストの先頭に表示します。
参考: https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-
動的更新

最新問題: **169**
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. セッション情報
B. 心拍数
C. HA 状態情報
D. ユーザーID情報
Answer: A (メーッセージを残す**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha-links-and-backup-links

最新問題: **170**
アクティブ/パッシブ HA ペアのパッシブ PA-7050 ファイアウォール上で、集約イーサネット インターフェイスがダウンしていると表示されます。HA パッシブ リンク状態は、[デバイス] > [高可用性] > [一般] > [アクティブ/パッシブ設定] で 自動」に設定されます。AE インターフェイスは LACP が有効になるように構成されており、アクティブなファイアウォール上でのみ稼働します。AE インターフェイスがパッシブ ファイアウォールでダウンしていると表示されるのはなぜですか?

A. AE インターフェイスの [LACP] タブの [高可用性オプション] で [HA パッシブ状態で有効にする] が選択されていない限り、事前ネゴシエーション LACP は実行されません。
B. AE インターフェイスの [LACP] タブの [LACP を有効にする] 選択で高速フェイルオーバーが選択されていない限り、LACP ネゴシエーションに参加しません。
C. AE インターフェイスの [LACP] タブの [LACP を有効にする] 選択で [伝送速度] に [高速] が選択されている場合、LACP ネゴシエーションに参加します。
D. AE インターフェイスの LACP タブの LACP を有効にする選択でパッシブ モードが選択されている場合、LACP の事前ネゴシエーションを実行します。
Answer: A (メーッセージを残す**)**
説明
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/high-availability/set-up-activepassive-ha/configure

最新問題**: 171**
マルウェアに感染したホストが既知のコマンド アンド コントロール サーバーを解決しようとすると、トラフィックは DNS シンホールが有効になっているセキュリティ ポリシーと一致し、トラフィック ログが生成されます。
そのログ エントリの宛先 IP アドレスは何になりますか?
A. sinkhole.paloaltonetworks.com の IP アドレス
B. コマンドアンドコントロールサーバーのIPアドレス
C. シンクホール構成で指定された IP アドレス
D. スパイウェア対策データベースで識別された外部 DNS サーバーの 1 つの IP アドレス
Answer: C (メーッセージを残す**)**
https://live.paloaltonetworks.com/t5/Management-Articles/How-to-Verify-DNS-Sinkhole-Function-is-Working/ta-p/65864

最新問題**: 172**
クライアントは、データセンター内に機密性の高いアプリケーション サーバーを備えており、分散型サービス拒否攻撃によるリソースの枯渇を特に懸念しています。
複数の IP アドレスから発生するリソース枯渇 (DDoS 攻撃) からこのサーバーを特別に保護するように、パロ アルト ネットワーク NGFW を構成するにはどうすればよいですか?
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. 攻撃をブロックする脆弱性保護プロファイルを追加します。
C. QoS プロファイルを追加して受信リクエストを抑制します。
D. セッション数が定義された DoS 保護プロファイルを追加します。
Answer: D (メーッセージを残す**)**
説明/参照: https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/zone-protection-and-dos- protection/zone-defense/dos-protection-profiles-and-policy-ルール/DOS プロテクション プロファイル

最新問題: **173**
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さらにファイアウォールを購入するための資金を持っています。
パートナー SE は、保護するリソースのできるだけ近くにファイアウォールを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、またその理由は何ですか?
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 には拡張できません。
B. いいえ 境界 DDoS デバイスの前面にファイアウォールを配置すると、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 システムの構成を通じて、保護するリソースに合わせて調整できます。
D. ファイアウォールなし。設置場所に関係なく、サイバー攻撃のライフサイクルのあらゆる段階で攻撃者を防ぐための新たな防御力と回復力を提供します。
Answer: A (メーッセージを残す**)**
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/zone-protection-and-dos-protection/zone-defense/firewall-placement-for-dos-protection

最新問題: **174**
GlobalProtect 構成の画面キャプチャを表示します。
この構成の目的は何ですか?
A. すべての内部クライアントのトンネル アドレスを 192.168.10.1 から始まる IP アドレス範囲に設定します。
B. 内部クライアントが IP アドレス 192.168.10.1 の内部ゲートウェイに接続するように強制されます。
C. クライアントが 192.168.10.1 に対して逆 DNS ルックアップを実行して、内部クライアントであることを検出できるようにします。
D. ファイアウォールに動的 DNS 更新の実行を強制し、内部ゲートウェイのホスト名と IP アドレスを DNS サーバーに追加します。
Answer: (解答を表示する**)**
説明/参照:
参照: https://www.paloaltonetworks.com/documentation/80/globalprotect/globalprotect-admin-guide/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-agent-configurations

最新問題: **175**
HA2 リンクを通じて何が交換されますか?
A. こんにちは、心拍数です
B. ユーザーID情報
C. セッションの同期
D. HA 状態情報

Answer: C (メーッセージを残す)
参照：
データ リンク - HA2 リンクは、HA ペア内のデバイス間でセッション、転送テーブル、IPSec セキュリティ アソシエーション、ARP テーブルを同期するために使用されます。HA2 リンク上のデータ フローは常に単方向です (HA2 キープアライブを除く)。アクティブデバイスからパッシブデバイスへ。」https://docs.paloaltonetworks.com/vm-series/9-0/vm-series-deployment/set-up-the-vm-series-firewall-on-aws/high-availability-for-vm-series- firewall-on-aws/ha-links#:~:text=%E2%80%94The%20HA1%20link%20is%20used,port%20is%20used%20for%20HA1

最新問題**: 176**
ネットワーク セキュリティ管理者は、複数の認証形式を備えた環境を持っています。ワイヤレス ユーザー、複数の Windows ドメイン コントローラー、会社支給のスマートフォン用の MDM ソリューションのアクセスを認証および制限するネットワーク アクセス制御システムが導入されています。これらのデバイスはすべて、認証イベントがログに記録されます。
情報を踏まえた上で、最大限のカバレッジを確保するには、User-ID を導入するための最良の選択は何でしょうか?
A. Syslog リスナー
B. 再配布を伴うエージェントレスユーザーID
C. スタンドアロンの User-ID エージェント
D. キャプティブ ポータル
Answer: C (メーッセージを残す)
説明
syslog リスナーは、ネットワーク アクセス コントロール システム、ドメイン コントローラー、MDM ソリューションなどのユーザー マッピング情報を含むネットワーク デバイスからの syslog メッセージをリッスンするユーザー ID エージェントです。ファイアウォールまたは Panorama で syslog リスナーを設定し、syslog 形式とフィルタを指定することにより、User-ID は syslog メッセージを解析し、複数のソースからユーザー マッピング情報を抽出できます。再配布を伴うエージェントレス User-ID は、既存のファイアウォールを User-ID エージェントとして使用し、ユーザー マッピングを他のファイアウォールまたは Panorama に再配布する方法です。この方法には syslog メッセージは含まれません。スタンドアロンの User-ID エージェントは、Windows サーバー上で実行され、Active Directory サーバーまたはその他のソースからユーザー マッピングを収集するソフトウェア アプリケーションです。この方法では、別のエージェント ソフトウェアをインストールして管理する必要があります。キャプティブ ポータルは、特定のネットワーク リソースにアクセスする前にユーザーに認証を求める Web ページです。この方法には syslog メッセージは含まれません。参考文献:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/syslog-mon
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/user-id/map-ip-addresses-to-users/user-id-age

最新問題: **177**
すでにパロアルト ファイアウォールを導入している企業が、最初の Panorama サーバーを購入しました。セキュリティ チームは、すでにすべてのファイアウォールに Panorama IP アドレスを設定し、すべてのファイアウォールのシリアル番号を Panorama に追加しています。ファイアウォールから Panorama に設定を移行するには、次の手順は何ですか?
A. API 呼び出しを使用して、管理対象デバイスから構成を直接取得します。
B. 各ファイアウォールで名前付き構成スナップショットをエクスポートし、続いて Panorama で名前付き構成スナップショットをインポートします。
C. デバイス構成を Panorama にインポートし、続いて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ます
D. ファイアウォール移行プラグインを使用して、管理対象デバイスから設定を直接取得します。
Answer: C (メーッセージを残す**)**
説明
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CloRCAS

最新問題: **178**
管理者には、復号化されたトラフィックをパロアルトネットワーク 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という要件があります。
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. 復号化ポート エクスポート ライセンスを備えた仮想ワイヤ インターフェイス
B. 復号化ポートミラーライセンスを持つタップインターフェース
C. 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
D. 関連付けられた復号化ポート ミラー ライセンスを持つ復号化ミラー インターフェイス
Answer: D (メーッセージを残す**)**

最新問題: **179**
WildFire サブスクリプションに基づいて、1 日に WildFire に送信できるサンプルの最大数はどれですか?
A. 7,500
B. 15,000
C. 5,000
D. 10,000
Answer: D (メーッセージを残す**)**

最新問題: **180**
次の図に基づいて、ルート、中間、およびエンドユーザー証明書の正しいパスはどれですか?
A. シマンテック > ベリサイン > パロアルトネットワークス
B. ベリサイン > パロアルトネットワークス > シマンテック
C. パロアルトネットワークス > シマンテック > ベリサイン
D. ベリサイン > シマンテック > パロアルトネットワークス

Answer: A (メーッセージを残す**)**

最新問題**: 181**
GlobalProtect アプリの PanGPA ログからの次のメッセージを考慮すると、正しいのはどれですか?
ポート47 67でサーバーに接続できませんでした
A. PanGPS プロセスがポート 4767 で PanGPA プロセスに接続できませんでした。
B. GlobalProtect アプリがポート 4767 で GlobalProtect ポータルに接続できませんでした。
C. PanGPA プロセスがポート 4767 で PanGPS プロセスに接続できませんでした。
D. GlobalProtect アプリがポート 4767 で GlobalProtect ゲートウェイに接続できませんでした。
Answer: (解答を表示する**)**
説明
https://knowledgebase.paloaltonetworks.com/kCSArticleDetail?id=kA10g000000PMiD
GlobalProtect アプリの PanGPA ログには、ユーザー アクション、メッセージ、通知など、アプリのユーザー インターフェイスに関連するイベントが記録されます。PanGPS ログには、接続試行、認証、トンネル確立など、アプリのサービスまたはデーモン プロセスに関連するイベントが記録されます2。PanGPA プロセスは、ポート 4767 で PanGPS プロセスと通信します。したがって、
ポート:4767 でサーバーに接続できませんでした」というメッセージは、PanGPA プロセスがポート上の PanGPS プロセスに接続できなかったことを示します。
4767. これは、ファイアウォールのブロック、ウイルス対策の干渉、ファイルの破損、不正なアクセス許可など、さまざまな要因によって発生する可能性があります4。参考文献:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClUkCAK 2:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClcCCAS 3:
https://live.paloaltonetworks.com/t5/general-topics/pangps-vs-pangpa-logs-on-globalprotect/td-p/298259 4:
https://live.paloaltonetworks.com/t5/globalprotect-Discussions/pangpa-and-pangps-logs/td-p/459846

最新問題**: 182**
WildFire が分析サンプルに対して提供できる 3 つの可能な判定は何ですか?
(3つお選びください)
A. きれい

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
Answer: (解答を表示する**)**
説明: https://www.paloaltonetworks.com/documentation/70/pan-os/newfeaturesguide/wildfire-features/wildfire-grayware-verdict

最新問題**: 183**
アプリケーションオーバーライドを実装するには、どの 3 つの項目を構成する必要がありますか? (3つお選びください)
A. カスタムアプリ
B. セキュリティポリシールール
C. アプリケーションオーバーライドポリシールール
D. 復号化ポリシールール
E. アプリケーションフィルター
Answer: (解答を表示する**)**
説明
Palo Alto Networks のドキュメント 1 によると、アプリケーション オーバーライドでは、ファイアウォールを通過する特定のトラフィックの通常のアプリケーション ID (App-ID) をオーバーライドするようにファイアウォールが構成されます。アプリケーション オーバーライドを実装するには、次の項目を構成する必要があります。
カスタム アプリ: これは、オーバーライドする必要があるトラフィックを識別するために使用されるユーザー定義のアプリケーションです。異なるデフォルト ポートや脅威検査機能を持つ事前定義アプリを使用するのではなく、applicationoverride ポリシー用のカスタム アプリを作成することをお勧めします2。
セキュリティ ポリシー ルール: これは、カスタム アプリに一致するトラフィックがファイアウォールを通過することを許可するルールです。セキュリティ ポリシー ルールは、カスタム アプリをアプリケーション フィルターとして使用し、必要に応じて送信元ゾーンと宛先ゾーン、アドレス、およびユーザーを指定する必要があります。アプリケーション オーバーライド ポリシー ルール: これは、トラフィックの App-ID をオーバーライドするための基準を定義するルールです。アプリケーション オーバーライド ポリシー ルールでは、カスタム アプリをアプリケーション フィルターとして使用し、必要に応じて送信元ゾーンと宛先ゾーン、アドレス、ポート、およびプロトコルを指定する必要があります2。
他のオプションは、アプリケーション オーバーライドの実装には必須ではなく、関連性もありません。
復号化ポリシー ルール: これは、暗号化されたトラフィックを復号化するための基準を定義するルールです。暗号化を使用する一部のアプリケーションを識別するために復号化が必要になる場合がありますが、これはアプリケーションのオーバーライドとは関係ありません。

アプリケーション フィルター: これは、カテゴリ、サブカテゴリ、テクノロジー、リスクなどのさまざまな基準に基づいてアプリケーションをグループ化するオブジェクトです。これは、アプリケーション オーバーライド用に構成する必要がある項目ではありませんが、セキュリティ ポリシー ルールまたはカスタム アプリの参照として使用できます。
参考文献: 1:
https://live.paloaltonetworks.com/t5/blogs/tips-amp-tricks-how-to-create-an-application-override/ba-p/451872
2: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0 :
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/decryption/decryption-concepts/how-decryption-wo
:
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/app-id/manage-custom-or-unknown-applications/cre

最新問題**: 184**
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は 2 つの新しい場所でレポートされるようになりました。(2つお選びください。)
A. [オブジェクト] > [アプリケーション] ブラウザ ページ上
B. Policy Optimizer の [ルールの使用法] ページ
C. [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
D. 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] タブ上
Answer: C,D (メーッセージを残す**)**

最新問題**: 185**
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. 認証ポリシー
B. 復号化ポリシー
C. アプリケーションオーバーライドポリシー
D. セキュリティポリシー
Answer: (解答を表示する**)**

最新問題**: 186**
「復号化なし」アクションを含む復号化ポリシー ルールに復号化プロファイルを割り当てることで得られる 2 つの利点はどれですか? (2つお選びください。)
A. 期限切れの証明書を持つセッションをブロックします。
B. クライアント認証によるセッションのブロック
C. サポートされていない暗号スイートを使用した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します。

E. 認証情報フィッシングをブロックします。
Answer: A,D (メーッセージを残す**)**
https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/decryption/configure-decryption-Exceptions

最新問題**: 187**
Web サーバーは DMZ でホストされており、サーバーは TCP ポート 8080 でのみ受信接続をリッスンするように構成されています。信頼ゾーンから DMZ ゾーンへのアクセスを許可するセキュリティ ポリシー ルールを構成して、Web サーバーへの参照アクセスを有効にする必要があります。サーバ。
TCP/8080 上のシン サーバーへのクリアテキスト Web ブラウジング トラフィック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: アプリケーションのデフォルト
B. アプリケーション: Web ブラウジング; サービス: サービス-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)
Answer: (解答を表示する**)**
説明
FW をチェックインすると、Web ブラウジングのデフォルト ポートは TCP 80 になるため、カスタム アプリが必要になります。
admin@PA-LAB-01# 定義済みアプリケーションの表示 web-browsing web-browsing { category 一般インターネット; サブカテゴリインターネットユーティリティ。ブラウザ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。当初は HTML 形式の情報を表示するために使用されていましたが、Web ブラウザはクライアントとなり、ユーザーはこれを介して、単純な情報の閲覧をはるかに超えた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るようになりました。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。単純な 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事実上影が薄くなってしまいました。} デフォルト { ポート tcp/80; トンネルアプリケーション http-プロキシ; リスク4; }
[編集]

最新問題**: 188**
展示を参照してください。
上の ACC のスクリーンショットを使用して、グローバル フィルターを設定し、ブロックされたユーザー アクティビティを絞り込み、ボットネットによって侵害される可能性のあるユーザーを特定するための最良の方法は何ですか?
A. Zero Access.Gen 脅威の横にある左矢印をクリックします。
B. 脅威数が最も多い送信元ユーザーをクリックします。
C. Zero Access.Gen 脅威のハイパーリンクをクリックします。

D. ホットポート脅威カテゴリのハイパーリンクをクリックします。
Answer: A (メーッセージを残す**)**

最新問題**: 189**
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 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します
Answer: (解答を表示する**)**
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClZuCAK

最新問題**: 190**
管理者は、DMZ 内の複数の Web サーバーがインターネットから開始された接続を受信できるようにし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 のサーバーに転送する必要があります。画像に示されている情報に基づいて、どの NAT ルールが Web ブラウジング トラフィックを正しく転送しますか?
A.
B.
B:
C.
D.
Answer: A (メーッセージを残す**)**

最新問題**: 191**
各 GlobalProtect コンポーネントをそのコンポーネントの目的に適合させる
Answer:
説明
GlobalProtect ポータルは、GlobalProtect インフラストラクチャの管理機能を提供します。
GlobalProtect ゲートウェイは、GlobalProtect アプリからのトラフィックにセキュリティを適用します。GlobalProtect アプリ ソフトウェアは、エンドポイント上で実行され、ネットワーク リソースへのアクセスを可能にします。

最新問題**: 192**
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、WildFire の署名と評定は世界的に共有されません。

B. パロアルトネットワークスは、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. 各 WildFire クラウドは、他の WildFire クラウドとは独立してサンプルを分析し、マルウェアのシグネチャと判定を生成します。
D. WildFire Global Cloud はベア メタル分析のみを提供します。
Answer: B (メーッセージを残す**)**
説明
パロアルトネットワークスの Web サイト 1 によると、顧客は場所とデータ プライバシー要件に基づいて選択できる 5 つの WildFire パブリック クラウドがあります。WildFire Global Cloud (US)、WildFire Europe Cloud、WildFire Japan Cloud、WildFire Singapore Cloud、WildFire United です。キングダムクラウド。さらに、PAN-OS 10.0 の時点で利用できるリージョン パブリック クラウドがさらに 3 つあります。
WildFire カナダ クラウド、WildFire オーストラリア クラウド、および WildFire ドイツ Cloud2。したがって、正解は B です。参考文献: 1: https://www.paloaltonetworks.com/network-security/wildfire 2:
https://docs.paloaltonetworks.com/wildfire/9-1/wildfire-admin/wildfire-overview/wildfire-deployments/wildfire-

最新問題**: 193**
管理者はパロアルトネットワーク NGFW 上の仮想ルーターで BGP を有効にしましたが、新しいルートが仮想ルーターに設定されていないようです。
管理者がこの問題をトラブルシューティングするのに役立つ 2 つのオプションはどれですか? (2 つお選びください。)
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. ランタイム統計を表示し、BGP 構成の問題を探します。
C. [ACC] タブを表示して、ルーティングの問題を特定します。
D. NGFW でトラフィック pcap を実行して、BGP の問題を確認します。
Answer: A,B (メーッセージを残す**)**

最新問題**: 194**
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さらにファイアウォールを購入するための資金を持っています。
パートナー SE は、保護するリソースのできるだけ近くにファイアウォールを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、またその理由は何ですか?
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 には拡張できません。
B. 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 システムの構成を通じて、保護するリソースに合わせて調整できます。
C. ファイアウォールなし。設置場所に関係なく、サイバー攻撃のライフサイクルのあらゆる段階で攻撃者を防ぐための新たな防御力と回復力を提供します。

D. いいえ 境界 DDoS デバイスの前面にファイアウォールを配置すると、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。
Answer: C (メーッセージを残す**)**

最新問題**: 195**
パロアルトネットワーク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. パロアルトネットワーク NGFW では AutoFocus が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 > ログおよびレポート設定
Answer: B (メーッセージを残す**)**
説明/参照:
参考: https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/getting-started/enable-オートフォーカス脅威インテリジェンス

最新問題**: 196**
PAN-OS のアクティブ/アクティブ高可用性 (HA) をサポートする 2 つの仮想化環境はどれですか 8.0? (2つお選びください。)
A. VMware ESX
B. AWS
C. VMware NSX
D. KVM
Answer: A,D (メーッセージを残す**)**

最新問題**: 197**
PAN-OS イメージを管理対象デバイスに展開するときに Panorama が実行できる 3 つのアクションはどれですか? (3つお選びください。)
A. アップロードのみ
B. アップロードしてインストールし、再起動します
C. 確認してインストールします

D. アップロードしてインストールします
E. インストールして再起動します
Answer: A,B,E (メーッセージを残す)
説明
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/panorama-web-interface/panorama-de

最新問題**: 198**
新しい NGFW を実装した後、ファイアウォール エンジニアは、ファイアウォールを通過する VoIP トラフィックの問題に気づきました。トラブルシューティングの後、エンジニアは、ファイアウォールが音声パケット ペイロードに対して NAT を実行し、メディア ポートに動的ピンホールを開いていることを発見しました。VoIP トラフィックを解決するためにエンジニアは何ができるでしょうか問題？
A. H.323 アプリケーションで ALG を無効にする
B. H.323 アプリケーションでの TCP タイムアウトを増やします。
C. SIP アプリケーションでの TCP タイムアウトを増やします。
D. SIP アプリケーションで ALG を無効にする
Answer: D (メーッセージを残す)
Palo Alto Networks のドキュメント 1 によると、アプリケーション レベル ゲートウェイ (ALG) は、ファイアウォールが SIP などの一部のプロトコルのペイロードを検査および変更して、NAT トラバーサルとファイアウォール ポリシーの適用を可能にする機能です。ただし、ALG は、SIP ヘッダーを誤って変更したり、メディア ポートに不要なピンホールを開いたりするなど、一部の VoIP 実装で問題を引き起こす可能性もあります。したがって、SIP アプリケーションで ALG を無効にすると、ファイアウォールによる音声パケット ペイロードの変更や動的ピンホール 2 の発生を防ぐことができ、VoIP トラフィックの問題の解決に役立ちます。したがって、正解は D です。
他のオプションは、VoIP トラフィックの問題の解決には関係がなく、役に立ちません。
H.323 アプリケーションで ALG を無効にする: このオプションは、別の VoIP プロトコルである H.323 プロトコルの ALG を無効にしますが、このシナリオで使用されるものではありません。このシナリオではシグナリング プロトコルとして SIP について言及しているため、H.323 アプリケーションで ALG を無効にしても VoIP トラフィックの問題には影響しません。
H.323 アプリケーションで TCP タイムアウトを増やす: このオプションは、別の VoIP プロトコルである H.323 プロトコルの TCP タイムアウトを増やしますが、このシナリオで使用されるものではありません。このシナリオでは、デフォルトで UDP を使用するシグナリング プロトコルとして SIP について言及しているため、H.323 アプリケーションで TCP タイムアウトを増やしても、VoIP トラフィックの問題には影響しません。
SIP アプリケーションで TCP タイムアウトを増やす: このオプションは、このシナリオで使用されるシグナリング プロトコルである SIP プロトコルの TCP タイムアウトを増やします。ただし、SIP はデフォルトで UDP を使用するため、TCP タイムアウトを増やしても VoIP トラフィッ

クの問題には影響しません。さらに、TCP タイムアウトを増やしても、音声パケット ペイロードの NAT やメディア ポートの動的ピンホールの問題は解決されません。