

CheckPoint.156-215.80.v2023-02-18.q308

試験コード:	156-215.80
試験名称:	Check Point Certified Security Administrator R80
認定資格:	CheckPoint
無料問題数:	308
バージョン:	v2023-02-18
アクセス数:	3413
ページビュー数:	3080
https://www.jpnpdf.com/CheckPoint.156-215.80.v2023-02-18.q308-mondaishu.html	

最新問題: 1

NAT の優先順位は何ですか？

- A. スタティック NAT、IP プール NAT、Hide NAT
- B. IP プール NAT、静的 NAT、非表示 NAT
- C. 静的 NAT、自動 NAT、非表示 NAT
- D. スタティック NAT、Hide NAT、IP プール NAT

Answer: A (メッセージを残す)

解説 参考：

Explanation:

NAT の優先順位は次のとおりです。

- 1.静的NAT
- 2. IP プール NAT
- 3.NATを隠す

スタティック NAT には IP プール NAT のすべての利点などがあるため、他の NAT 方式よりも優先度が高くなります。

参照: https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm#o6919

最新問題: 2

Lilly は、先週の VPN 履歴カウンターを確認する必要があります。

彼女はどこでこれをしますか？

- A. SmartView モニター > システム カウンター > VPN 履歴
- B. SmartView Monitor > システム カウンター > ファイアウォール セキュリティ履歴
- C. SmartView モニター > トンネル > VPN 履歴
- D. SmartView モニター > システム カウンター > VPN

Answer: A (メッセージを残す)

最新問題: 3

管理者 Dave は、R80 Management Server にログインして確認し、いくつかのルールを変更します。彼は、ルール ベースの DNS ルールの横に南京錠の記号があることに気付きました。

これについて考えられる説明は何ですか？

- A. DNS ルールは R80 の新機能の 1 つを使用しており、管理者はルールに南京錠のアイコンを付けて、そのルールが重要であることを他の管理者に知らせることができます。
- B. これは、Rule Base に重複したルールがある場合の R80 の正常な動作です。
- C. 別の管理者が管理にログインし、現在 DNS ルールを編集しています。
- D. DNS ルールは、過去に存在したが削除されたルールのプレースホルダー ルールです。

Answer: C ([メッセージを残す](#))

最新問題: 4

統合ポリシーとは何ですか？

- A. セキュリティ ポリシー、アドレス変換、および IPS ポリシーの総称。
- B. SmartDashboard に記述された特定のポリシーで、どのログ データをどのログ データに保存するかを構成します。SmartReporter データベース。
- C. 複数の Security Gateway に対して共通の実施ポリシーを共有するために使用されるグローバル ポリシー。
- D. SmartReporter によって生成されたログの総称。

Answer: B ([メッセージを残す](#))

最新問題: 5

セキュリティ ルールの追跡オプションとして 「フル ログ」を有効にしました。ただし、データ型の情報はまだ表示されていません。最も可能性の高い理由は何ですか？

- A. ログにはディスク容量の問題があります。ログ サーバーのログ ストレージ オプションを変更するか、Security Management Server のプロパティとインストール データベース。
- B. データ認識が有効になっていません。
- C. Identity Awareness が有効になっていません。
- D. R80 より前のゲートウェイからログが到着しています。

Answer: A ([メッセージを残す](#))

ログ データが停止する最も可能性の高い理由は、ロギング デバイス (管理サーバーまたはゲートウェイ サーバー) のディスク容量が少ないことです。

最新問題: 6

空白を埋める: トンネル テスト パケットが応答を呼び出さなくなった場合、SmartView Monitor は指定された VPN トンネルに対して _____ を表示します。

- A. 下
- B. 無反応
- C. 非アクティブ
- D. 失敗

Answer: A ([メッセージを残す](#))

最新問題: 7

最後のポリシーのインストール以降に受け入れられたパケットの数を確認するには、どの R77 GUI を使用しますか？

- A. SmartView モニター
- B. SmartView トラッカー
- C. スマートダッシュボード
- D. SmartView ステータス

Answer: A ([メッセージを残す](#))

説明

最新問題: 8

R80.10 コードの一部として現在利用可能な Check Point API のタイプは何ですか？

- A. Security Gateway API、Management API、Threat Prevention API、Identity Awareness Web Services API
- B. Management API、Threat Prevention API、Identity Awareness Web Services API、OPSEC SDK API
- C. OSE API、OPSEC SDK API、脅威対策 API、ポリシー エディター API
- D. CPMI API、管理 API、脅威対策 API、ID 認識 Web サービス API

Answer: B ([メッセージを残す](#))

説明

参考文献:

最新問題: 9

セキュリティ ゲートウェイの CPU レベルが 100% に達し、トラフィックに問題が発生しています。問題は脅威対策の設定にある可能性があると思われます。

次の脅威対策プロファイルが作成されました。

適切なレベルのセキュリティを維持しながら CPU 負荷を下げるために、プロファイルをどのように調整できますか？ ベストアンサーを選択してください。

- A. 脅威対策プロファイルに問題はありません。アプライアンスにメモリを追加することを検討してください。
- B. パフォーマンスへの影響を中以下に設定します。
- C. 回避するには、パフォーマンスへの影響を非常に低い信頼度に設定します。
- D. 高信頼度を低に、低信頼度を非アクティブに設定します。

Answer: ([解答を表示する](#))

最新問題: 10

R80 では、Unified Policy は

- A. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、およびエンドポイント ポリシー。
- B. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、および脅威対策ポリシー。
- C. ファイアウォール ポリシー、アドレス変換、アプリケーションおよび URL フィルタリング、QoS ポリシー、デスクトップ セキュリティ ポリシー、脅威対策ポリシー。
- D. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、および VPN ポリシー。

Answer: D ([メッセージを残す](#))

説明

選択肢から考えると D が最良の答えです。

統一されたポリシー

R80 では、アクセス コントロール ポリシーは、これらの R80 より前の Software Blade のポリシーを統合します。

ファイアウォールと VPN

アプリケーション制御と URL フィルタリング

アイデンティティの認識

データ認識

モバイルアクセス

セキュリティ ゾーン

参考文献:

最新問題: 11

どの VPN コミュニティがサテライト VPN ゲートウェイであるか、別のサテライトとの VPN トンネルの作成が許可されていない VPNゲートウェイ？

A. 五角形

B. 組み合わせ

C. メッシュ

D. スター

Answer: ([解答を表示する](#))

説明

VPN コミュニティは、スター トポロジとメッシュ トポロジに基づいています。メッシュ コミュニティには、VPN 接続があります。各 Security Gateway 間。スターコミュニティでは、サテライトはセンターとの VPN 接続を持っています Security Gateway ですが、相互にはありません。

最新問題: 12

SIC の 3 つの認証方法は何ですか？

A. セキュリティ チャンネルを作成するためのパスワード、ユーザー、および標準ベースの SSL

B. 証明書、安全なチャンネルを作成するための標準ベースの SSL、および暗号化のための 3DES または AES128

C. パケット フィルタリング、証明書、および暗号化のための 3DES または AES128

D. 証明書、パスワード、およびトークン

Answer: ([解答を表示する](#))

Secure Internal Communication (SIC)Secure Internal Communication (SIC) により、チェック ポイントのプラットフォームと製品が相互に認証されます。SIC 手順により、ゲートウェイ、管理サーバー、およびその他のチェック ポイント コンポーネント間に信頼できるステータスが作成されます。ゲートウェイにポリシーをインストールし、ゲートウェイと管理サーバー間でログを送信するには、SIC が必要です。これらのセキュリティ対策により、SIC の安全性が確保されます。

最新問題: 13

ログを表示してセキュリティの脅威を検出し、すべてのネットワーク デバイスからの潜在的な攻撃パターンを一元的に表示する SmartConsole のタブはどれですか？

- A. ゲートウェイとサーバー
- B. ログと監視
- C. 管理と設定
- D. セキュリティ ポリシー

Answer: ([解答を表示する](#))

解説 参考 :

最新問題: 14

次のうち、VPN 簡易モードと VPN コミュニティの要素ではないものはどれですか？

- A. ルール ベースの 暗号化」アクション
- B. 常設トンネル
- C. ルール ベースの VPN」列
- D. 構成チェックボックス すべての暗号化されたトラフィックを受け入れる」

Answer: A ([メッセージを残す](#))

説明

従来モードから簡易モードへの移行

トラディショナル モードの VPN から簡易モードに移行するには:

1. グローバル プロパティ > VPN」ページで、次のいずれかのオプションを選択します。

* すべての新しいファイアウォール ポリシーの簡易モード

* 新しいファイアウォール ポリシーごとに従来型または簡易型

2. [OK] をクリックします。

3. R80 SmartConsole メニューから、[ポリシーの管理] を選択します。

[ポリシーの管理] ウィンドウが開きます。

4. [新規] をクリックします。

[新しいポリシー] ウィンドウが開きます。

5. 新しいポリシーに名前を付けて、[アクセス制御] を選択します。

セキュリティ ポリシー ルール ベースで、VPN とマークされた新しい列が表示され、[アクション] 列で [暗号化] オプションが使用できなくなります。現在、簡易モードで作業しています。

最新問題: 15

クラスター メンバーのフェイルオーバーはどこでトリガーできますか？

1. Security Gateway CLI にログインし、コマンド clusterXL_admin down を実行します。

2. SmartView Monitor で、Security Gateway メンバーを右クリックし、[Cluster member down] を選択します。

3. Security Gateway CLI にログインし、コマンド cphaprob down を実行します。

A. 1、2、および 3

B. 2 と 3

C. 1 と 2

D. 1 と 3

Answer: C ([メッセージを残す](#))

解説 参考 :

Explanation:

フェイルオーバーを開始する方法

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

最新問題: 16

Tina は新しい管理者で、現在新しい Check Point R80 管理コンソール インターフェイスをレビューしています。ゲートウェイ ビューで、彼女は下のスクリーンショットのように [概要] 画面を確認しています。オープンサーバーとは？

- A. チェック ポイント以外のアプライアンスに導入されたチェック ポイントのソフトウェア。
- B. Open Server Consortium が承認した、セキュリティと可用性の目的で使用されるサーバー ハードウェア。
- C. Open Systems Interconnection (OSI) サーバーおよびセキュリティ展開モデルを使用して展開されたチェック ポイント管理サーバー。
- D. Open SSL を使用するチェック ポイント管理サーバー ソフトウェア。

Answer: ([解答を表示する](#))

解説 参考 :

Explanation:

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/index.html

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 17

Web Control Layer は、次のダイアログの設定を使用して設定されています。

以下の方針を考慮し、最良の回答を選択してください。

- A. サブポリシーのどのルールにも一致しないトラフィックはドロップされます。
- B. 全従業員が Youtube と Vimeo のみにアクセスできます。
- C. Youtube と Vimeo へのアクセスは 1 日 1 回のみ許可されます。
- D. 内部ネットワークの誰でもインターネットにアクセスできます。ドロップ ルール 5.2、5.5、および 5.6 で定義されたトラフィックを想定しています。

Answer: D ([メッセージを残す](#))

解説 参考 :

Explanation:

ポリシー層とサブポリシー

R80 では、レイヤーとサブポリシーの概念が導入され、ネットワーク セグメントまたはビジネス ユニット/機能に従ってポリシーをセグメント化できます。さらに、レイヤーまたはサブポリシーごとに詳細な権限を割り当てて、最も資格のある管理者にワークロードとタスクを

分散させることもできます。レイヤーを使用すると、ルール ベースは一連のセキュリティ ルールに編成されます。これらのルールまたはレイヤーのセットは、定義された順序で検査されるため、ルール ベース フローと優先されるセキュリティ機能を制御できます。レイヤー全体で「受け入れ」アクションが実行されると、検査は次のレイヤーに進みます。たとえば、コンプライアンス レイヤーを作成して、複数のルールにまたがってオーバーレイすることができます。

サブポリシーは、特定のネットワーク セグメント、ブランチ オフィス、またはビジネス用に作成された一連のルールです。そのため、ルールが一致した場合、インスペクションは次のルールに進む前に、このルールのサブセットを通じて続行されます。サブポリシーとレイヤーは、権限に応じて、特定の管理者が管理できます

プロファイル。これにより、タスクの委任とワークロードの分散が容易になります。

参照: <https://community.checkpoint.com/docs/DOC-1065>

最新問題: 18

分散展開オプションの代わりにスタンドアロン展開オプションを選択することの潜在的な欠点または欠点は何ですか？

- A. セキュリティ ポリシーのサイズが大きくなると、パフォーマンスが低下します。
- B. コストアップ
- C. 追加のソフトウェア サブスクリプションが必要です
- D. 追加の Check Point アプライアンスが必要です

Answer: ([解答を表示する](#))

最新問題: 19

DLP と地域ポリシーは、どのタイプのポリシーの例ですか？

- A. 標準ポリシー
- B. 共有ポリシー
- C. 検査ポリシー
- D. 統一ポリシー

Answer: ([解答を表示する](#))

解説 参考 :

Explanation:

共有ポリシーは、アクセス コントロール ポリシーと共にインストールされます。

参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMG/html_frameset.htm?topic=documents/R80/CP_R80_SecMG/126197

最新問題: 20

管理者は、R80 で信頼できる SmartConsole クライアントのリストをどこで編集できますか？

- A. Security Management Server にログインした WebUI クライアント、SmartDashboard: 管理および設定>アクセス許可と管理者>詳細設定>信頼できるクライアント、セキュリティのcpconfig経由ゲートウェイ。
- B. SmartConsole を使用する場合のみ: [管理と設定] > [権限と管理者] > [詳細設定] > 信頼できるクライアント。
- C. Security Management Server の cpconfig で、Security Management にログインした WebUI で

サーバー、SmartConsole: [管理と設定] > [権限と管理者] > [詳細設定] > [信頼済み]
クライアント。

D. Security Management Server にログインした WebUI で、Security Management Server の cpconfig。

Answer: ([解答を表示する](#))

最新問題: 21

組織のセキュリティ マネージャーは、Gaia オペレーティング システムのパラメーターのみをバックアップしたいと考えています。インターフェイスの詳細、静的ルート、プロキシ ARP エントリなどの Gaia オペレーティング システム パラメータのみをバックアップするために使用できるコマンドはどれですか？

- A. 構成を表示
- B. バックアップ
- C. エクスポートを移行
- D. アップグレード エクスポート

Answer: ([解答を表示する](#))

システム バックアップ (およびシステムの復元)

システム バックアップを使用して、現在のシステム構成をバックアップできます。バックアップは、ネットワークおよびオペレーティング システムのパラメータ (ルーティングやインターフェイス構成など) を含むチェック ポイントの構成を含む圧縮ファイルを作成しますが、スナップショットとは異なり、オペレーティング システム、製品バイナリ、およびホットフィックスは含まれません。

参考 [https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902)

最新問題: 22

脅威対策ポリシーを伴わないソフトウェア ブレードはどれですか？

- A. ウイルス対策
- B. IPS
- C. 脅威のエミュレーション
- D. アプリケーション制御と URL フィルタリング

Answer: D ([メッセージを残す](#))

解説 参考 https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92707.htm

最新問題: 23

次の図では、ポリシーのレイヤーが示されています。

定義されたポリシーのトラフィック インспекションの優先順位は？

- A. パケットがゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされ、暗黙のドロップルールはパケットをドロップします。パケットは IPS レイヤーの隣に来て、パケットを受け入れた後、脅威対策レイヤーに渡します。
- B. パケットがゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされ、パケットを受け入れるルールがあり、それは IPS レイヤーの隣にあり、パケットを受け入れた後脅威対策レイヤーに渡されます
- C. パケットがゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされ、

パケットを受け入れるルールがある場合、それは脅威防止レイヤーの隣に来て、その後 IPS 層に渡すパケットを受け入れます。

D. パケットはゲートウェイに到着し、IPS ポリシー レイヤーのルールと照合され、次に到着します。ネットワークポリシーレイヤーに送信され、パケットを受け入れた後、脅威防止レイヤーに渡されます。

Answer: B ([メッセージを残す](#))

説明

ポリシー管理を簡素化するために、R80 はポリシーをポリシー レイヤーに編成します。レイヤーは一連のルール、またはルールベース。

たとえば、以前のバージョンから R80 にアップグレードする場合:

ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

すべてのレイヤーが並行して評価されます

最新問題: 24

R80 では、SmartConsole を使用して複数の管理者が Security Management Server に同時に書き込み権限でログインできます。

A. いいえ、この機能はグローバル プロパティで有効にする必要があります。

B. 確かに、すべての管理者は、他の管理者から独立したセッションで作業します。

C. 確かに、すべての管理者は、他の管理者から独立した別のデータベースで作業しています。

D. False、1 人の管理者のみが書き込み権限でログインできます。

Answer: B ([メッセージを残す](#))

説明

複数の管理者が同時に Security Management Server に接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。

最新問題: 25

ヒット カウント データが保持されるデフォルトの期間は?

A. 3ヶ月

B. 4 週間

C. 12ヶ月

D. 6ヶ月

Answer: D ([メッセージを残す](#))

説明

ヒット カウント データを最大に保つ - 時間範囲オプションのいずれかを選択します。デフォルトは 6 か月です。データはこの期間の Security Management Server データベースであり、[ヒット数] 列に表示されます。

最新問題: 26

空欄を埋めてください: コマンド _____ は、R80 構成の最も完全な復元を提供します。

A. upgrade_import

B. cpconfig

C. fwm dbimport -p <エクスポート ファイル>

D. cpinfo -recover

Answer: A ([メッセージを残す](#))

解説 参考 :

Explanation:

(「migrate import」のほうです)

"migrate import" R80 バージョンのバックアップされた構成を復元します。以前のバージョンでは、このコマンドは "upgrade_import".

参考 :http://dl3.checkpoint.com/paid/08/08586e2852acc054809517b267402a35/CP_R80_Gaia_InstallationAndUpgradeGuide.pdf?HashKey=1479700086_4553ede4b53a7882cd8052eed7c347be&xtn=.pdf

最新問題: 27

OS と Check Point の構成のバックアップ コピーを作成できるオプションはどれですか。

チェック ポイントのプロセスを停止しますか？

- A. バックアップ
- B. スナップショット
- C. エクスポートを移行
- D. すべてのオプションでチェック ポイントのプロセスが停止します

Answer: B ([メッセージを残す](#))

最新問題: 28

Security Gateway がサポートする 2 つのタイプの NAT は何ですか？

- A. 宛先と非表示
- B. 非表示にして静的
- C. 静的およびソース
- D. ソースと宛先

Answer: (解答を表示する)

Security Gateway は、次の手順を使用して、ネットワーク内の IP アドレスを変換できます。

* 静的 NAT - 各内部 IP アドレスは、異なるパブリック IP アドレスに変換されます。ファイアウォールは、外部トラフィックが内部リソースにアクセスできるようにすることができます。

* Hide NAT - ファイアウォールはポート番号を使用して、指定されたすべての内部 IP アドレスを単一のパブリック IP アドレスに変換し、内部 IP 構造を隠します。接続は内部コンピューターからのみ開始でき、外部コンピューターは内部サーバーにアクセスできません。ファイアウォールは、外部のコンピューターおよびサーバーから同時に最大 50,000 の接続を変換できます。

* ポート変換で NAT を隠す - 1 つの IP アドレスを使用して、外部ユーザーが隠しネットワーク内の複数のアプリケーション サーバーにアクセスできるようにします。ファイアウォールは、要求されたサービス (または宛先ポート) を使用して、トラフィックを正しいサーバーに送信します。一般的な構成では、次のポートを使用できます: FTP サーバー (ポート 21)、SMTP サーバー (ポート 25)

25) および HTTP サーバー (ポート 80)。ポート変換を使用するには、手動で NAT ルールを作成する必要があります。

参照 :

https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/6724.htm

最新問題: 29

空欄に記入してください: ライセンスがアクティブ化されたら、_____ をインストールする必要があります。

- A. ライセンス管理ファイル
- B. Security Gateway コントラクト ファイル
- C. サービス契約ファイル
- D. ライセンス契約ファイル

Answer: C ([メッセージを残す](#))

説明

サービス契約ファイル

ライセンスのアクティベーションに続いて、サービス契約ファイルをインストールする必要があります。このファイルには、特定のデバイス用に購入したすべてのサブスクリプションに関する重要な情報が含まれており、SmartUpdate を介してインストールされます。サービス コントラクト ファイルの詳細な説明は、sk33089 にあります。

最新問題: 30

ウイルス シグネチャと ThreatCloud の異常ベースの保護を使用して、悪意のあるファイルがネットワークに侵入するのを防いでいる
チェック ポイントのソフトウェア ブレードはどれですか？

- A. ファイアウォール
- B. アプリケーション制御
- C. スпам対策とメール セキュリティ
- D. ウイルス対策

Answer: D ([メッセージを残す](#))

強化された Check Point Antivirus Software Blade は、リアルタイムのウイルス シグネチャと、サイバー犯罪と闘う最初の共同ネットワークである ThreatCloud の異常ベースの保護を使用して、ユーザーが影響を受ける前にゲートウェイでマルウェアを検出してブロックします。

参考 <https://www.checkpoint.com/products/antivirus-software-blade/>

最新問題: 31

チェック ポイントのセキュリティ管理アーキテクチャに不可欠な 3 つのコンポーネントは何ですか？

- A. SmartConsole、Security Management Server、Security Gateway
- B. SmartConsole、SmartUpdate、Security Gateway
- C. Security Management Server、Security Gateway、コマンドライン インターフェイス
- D. WebUI、SmartConsole、Security Gateway

Answer: A ([メッセージを残す](#))

解説 参考：

説明: デプロイメント

基本的な展開:

スタンドアロン展開 - Security Gateway と Security Management Server が
同じマシン。

分散展開 - Security Gateway と Security Management Server がインストールされています。

異なるマシン。

異なるサイトにゲートウェイがある環境を想定します。各 Security Gateway は一方をインターネットに接続し、もう一方を LAN に接続
します。

2 つの Security Gateway 間に Virtual Private Network (VPN) を作成して、その間のすべての通信を保護できます。

Security Management Server は LAN にインストールされ、Security Gateway によって保護されます。Security Management Server は Security Gateway を管理し、リモート ユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboard は、Security Management サーバーまたは別のコンピューターにインストールできます。

Security Management Server とその Security Gateway でネットワーク セキュリティを完成させるために、他の OPSEC パートナー モジュール (Anti-Virus Server など) が存在する場合があります。

参考 https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/118037

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 32

ルールを確認します。暗黙のルールでドメイン UDP が有効になっているとします。

内部ネットワークのユーザーが HTTP を使用してインターネットを閲覧しようとするときどうなりますか? ユーザー :

- A. インターネットに正常に接続する前に 3 回プロンプトが表示されます。
- B. 認証後、インターネットに正常に接続できます。
- C. 認証を求められることなく、インターネットにアクセスできます。
- D. クライアント認証デーモンのポート 259 に Telnet で接続すると、インターネットに接続できます。

Answer: C (メッセージを残す)

最新問題: 33

R80 管理プラグインについて正しい説明は次のうちどれですか?

- A. 管理プラグインのインストールには、アップグレード プロセスと同様に、スナップショットが必要です。
- B. 管理プラグインは、Security Management Server と対話して新しい機能を提供し、新製品のサポート。
- C. プラグインを使用すると、特定の機能に特別なライセンスが適用されている場合にのみ、完全な中央管理が提供されます。プラグイン。
- D. プラグインは、Security Gateway にインストールされるパッケージです。

Answer: B (メッセージを残す)

最新問題: 34

空欄に記入してください: ブラウザベースの認証は、ユーザーを Web ページに送り、次を使用して ID を取得します。

_____。

- A. ユーザー ディレクトリ
- B. キャプティブ ポータルと透過的な Kerberos 認証

C. キャプティブ ポータル

D. ユーザーチェック

Answer: B ([メッセージを残す](#))

説明

ID 認識を有効にするには:

* SmartDashboard にログインします。

* Network Objects ツリーから、Check Point ブランチを展開します。

* Identity Awareness を有効にする Security Gateway をダブルクリックします。

* [Software Blades] セクションで、[Network Security] タブの [Identity Awareness] を選択します。

Identity Awareness 設定ウィザードが開きます。

* 1 つまたは複数のオプションを選択します。これらのオプションは、管理対象アセットと管理対象外アセットの ID を取得する方法を設定します。

* AD Query - Security Gateway が Active Directory ユーザーとコンピュータをシームレスに識別できるようにします。

* ブラウザベースの認証 - ユーザーを Web ページに送り、未確認のユーザーから ID を取得します。透過的な Kerberos 認証が構成されている場合、AD ユーザーは透過的に識別されます。

参考文献:

最新問題: 35

スタンドアロン インストールを行う場合、Security Management Server を他のどのチェック ポイント アーキテクチャ コンポーネントとともにインストールしますか?

A. なし。Security Management Server は単独でインストールされます。

B. スマートコンソール

C. SecureClient

D. セキュリティ ゲートウェイ

Answer: ([解答を表示する](#)**)**

解説 参考 :

Explanation:

チェック ポイントのソフトウェア製品には、さまざまな導入シナリオがあります。

スタンドアロン展開 - Security Management Server と Security Gateway がインストールされています

同じコンピュータまたはアプライアンス上。

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/86429.htm

最新問題: 36

次の Windows セキュリティ イベントのうち、Identity Awareness でユーザー名を IP アドレスにマップしないものはどれですか?

A. Kerberos チケットが要求されました

B. Kerberos チケットが更新されました

C. Kerberos チケットがタイムアウトしました

D. アカウント ログオン

Answer: C ([メッセージを残す](#))

最新問題: 37

独自の例外セクションを持つポリシーの種類はどれですか？

- A. スレッド防止
- B. アクセス制御
- C. 脅威のエミュレーション
- D. デスクトップ セキュリティ

Answer: A ([メッセージを残す](#))

説明

[例外グループ] ペインでは、例外グループを定義できます。必要に応じて、ルール ベースで使用する例外グループを作成できます。例外グループには、定義済みの例外が 1 つ以上含まれています。このオプションは使いやすさを促進するため、一般的に必要な例外に対して複数のルールで例外を手動で定義する必要はありません。例外グループを追加するルールを選択できます。これは、必要に応じて、いくつかのルールに追加でき、他のルールには追加できないことを意味します。

最新問題: 38

次の図では、ポリシーのレイヤーが示されています。

定義されたポリシーのトラフィック インспекションの優先順位は？

- A. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされます。その後、暗黙的なドロップルールによってパケットがドロップされた場合、パケットは IPS レイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。
- B. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合され、パケットを受け入れるルールがあれば、IPS レイヤーの次の場所に到着し、パケットを受け入れた後、Threat に渡されます。防止層
- C. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合されます。パケットを受け入れるルールがあれば、次に脅威防御レイヤーに到達し、パケットを受け入れた後、次のレイヤーに渡されます。IPS レイヤー。
- D. パケットはゲートウェイに到着し、IPS ポリシー レイヤーのルールに対してチェックされ、次にネットワーク ポリシー レイヤーに到着し、パケットを受け入れた後、脅威防御レイヤーに渡されます。

Answer: B ([メッセージを残す](#))

説明

ポリシー管理を簡素化するために、R80 はポリシーをポリシー レイヤーに編成します。レイヤーは一連のルール、つまりルール ベースです。

たとえば、以前のバージョンから R80 にアップグレードする場合：

* ファイアウォールとアプリケーション コントロール ソフトウェア ブレードが有効になっているゲートウェイでは、アクセス コントロール ポリシーがネットワークとアプリケーションの 2 つの順序付けられたレイヤーに分割されます。

ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

* IPS および Threat Emulation Software Blade が有効になっているゲートウェイでは、脅威対策ポリシーが 2 つの並列レイヤー (IPS と脅威対策) に分割されます。

すべてのレイヤーが並行して評価されます

ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

すべてのレイヤーが並行して評価されます

参考文献:

最新問題: 39

デフォルトでは、WebUI はどのポートでリッスンしますか？

- A. 80
- B. 4434
- C. 443
- D. 8080

Answer: C ([メッセージを残す](#))

説明

Gaia で Security Management Server を設定するには:

* WebUI へのブラウザーを開きます: [https://<Gaia 管理 IP アドレス>](https://<Gaia%20管理%20IP%20アドレス>)

最新問題: 40

SmartUpdate でユーザー センターへの通信に使用されるポートは？

- A. HTTPS 443
- B. CPMI 200
- C. HTTP 80
- D. TCP 8080

Answer: ([解答を表示する](#))

最新問題: 41

ゲートウェイから管理サーバーにログを配信するために使用されるポートは？

- A. ポート 981
- B. ポート 257
- C. ポート 18209
- D. ポート 258

Answer: B ([メッセージを残す](#))

最新問題: 42

Gaia で構成ロックを取得するために使用されるコマンドはどれですか？

- A. ロック データベース オーバーライド
- B. データベース オーバーライドのロック解除
- C. データベース ロックのロックを解除します。
- D. データベース ユーザーのロック

Answer: A ([メッセージを残す](#))

解説 参考 :

説明: 構成ロックの取得

ロック データベース オーバーライド

データベースのロックを解除

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/75697.htm#o73091

最新問題: 43

Tina は新しい管理者で、現在新しい Check Point R80 管理コンソール インターフェイスをレビューしています。ゲートウェイ ビューで、彼女は下のスクリーンショットのように [概要] 画面を確認しています。何として「オープンサーバー」？

- A. チェック ポイント以外のアプライアンスに導入されたチェック ポイントのソフトウェア。
- B. Open Server Consortium が承認した、セキュリティと可用性の目的で使用されるサーバー ハードウェア。
- C. Open Systems Interconnection (OSI) サーバーおよびセキュリティ展開モデルを使用して展開されたチェック ポイント管理サーバー。
- D. Open SSL を使用するチェック ポイント管理サーバー ソフトウェア。

Answer: ([解答を表示する](#))

説明

最新問題: 44

パケットから詳細な情報を抽出し、その情報を状態テーブルに格納するテクノロジーは次のうちどれですか？

- A. INSPECT エンジン
- B. ステートフル インспекション
- C. パケットフィルタリング
- D. アプリケーション層ファイアウォール

Answer: ([解答を表示する](#))

解説 参考 <https://www.checkpoint.com/smb/help/utm1/8.2/7080.htm>

最新問題: 45

メジャー アップグレードを実行しようとしています。そのデバイスでデータベースを確実に復元できるようにするには、どのバックアップ ソリューションを使用する必要がありますか？

- A. バックアップ
- B. ログスイッチ
- C. データベースのリビジョン
- D. スナップショット

Answer: D ([メッセージを残す](#))

説明

スナップショットは、ルート (lv_current) ディスク パーティション全体のバイナリ イメージを作成します。これには、チェック ポイントの製品、構成、およびオペレーティング システムが含まれます。

R77.10 以降、あるマシンからのイメージのエクスポートと、同じタイプの別のマシンへのそのイメージのインポートがサポートされています。

ログ パーティションはスナップショットに含まれません。したがって、ローカルに保存された FireWall ログは保存されません。

最新問題: 46

契約ファイルをインストールするには、どのアプリケーションを使用する必要がありますか？

- A. SmartView モニター
- B. WebUI
- C. SmartUpdate

D. SmartProvisioning

Answer: C (メッセージを残す)

SmartUpdate の使用: すでに NGX R65 (またはそれ以降) のセキュリティ管理を使用している場合 /

Provider-1 / Multi-Domain Management Server、SmartUpdate を使用すると、手順 3 でダウンロードしたサービス契約ファイルをインポートできます。

SmartUpdate を開き、起動メニューから [ライセンスと契約] -> [更新] を選択します。

Contracts' -> 'From File...' をクリックし、手順 3 でダウンロードしたファイルへのパスを指定します。

注: SmartUpdate がインターネットに接続されている場合は、ダウンロードおよびインポートの手順を実行しなくても、UserCenter からサービス契約ファイルを直接ダウンロードできます。

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 47

Web Control Layer は、次のダイアログの設定を使用して設定されています。

以下の方針を考慮し、最良の回答を選択してください。

A. サブポリシーのどのルールにも一致しないトラフィックはドロップされます。

B. 全従業員が Youtube と Vimeo のみにアクセスできます。

C. Youtube と Vimeo へのアクセスは 1 日 1 回のみ許可されます。

D. 内部ネットワークの誰でもインターネットにアクセスできます。ドロップ ルール 5.2、5.5、および 5.6 で定義されたトラフィックを想定しています。

Answer: D (メッセージを残す)

解説 参考 :

Explanation:

ポリシー層とサブポリシー

R80 では、レイヤーとサブポリシーの概念が導入され、ネットワーク セグメントまたはビジネス ユニット/機能に従ってポリシーをセグメント化できます。さらに、レイヤーまたはサブポリシーごとに詳細な権限を割り当てて、最も資格のある管理者にワークロードとタスクを分散させることもできます。レイヤーを使用すると、ルール ベースは一連のセキュリティ ルールに編成されます。これらのルールまたはレイヤーのセットは、

定義された順序で検査されるため、ルール ベース フローと優先されるセキュリティ機能を制御できます。レイヤー全体で「受け入れ」アクションが実行されると、検査は次のレイヤーに進みます。たとえば、コンプライアンス レイヤーを作成して、複数のルールにまたがってオーバーレイすることができます。

サブポリシーは、特定のネットワーク セグメント、ブランチ オフィス、またはビジネス用に作成された一連のルールです。

そのため、ルールが一致した場合、インスペクションは次のルールに進む前に、このルールのサブセットを通じて続行されます。

サブポリシーとレイヤーは、権限に応じて、特定の管理者が管理できます

プロファイル。これにより、タスクの委任とワークロードの分散が容易になります。

参照: <https://community.checkpoint.com/docs/DOC-1065>

最新問題: 48

次のうち、SecureXL トラフィック フローでないものはどれですか？

- A. ミディアム パス
- B. 加速パス
- C. ファスト パス
- D. スローパス

Answer: ([解答を表示する](#))

SecureXL は、ファイアウォールのパフォーマンスを最大化し、セキュリティを損なうことのないアクセラレーション ソリューションです。Security Gateway で SecureXL が有効になっている場合、一部の CPU を集中的に使用する操作は、ファイアウォール カーネルではなく、仮想化されたソフトウェアによって処理されます。ファイアウォールは、接続をより効率的に検査および処理し、スループットと接続速度を加速できます。これらは SecureXL トラフィック フローです:

低速パス - ファイアウォールによって検査され、SecureXL によって処理されないパケットと接続。

加速パス - SecureXL にオフロードされ、ファイアウォールによって処理されないパケットと接続。

中程度のパス - より詳細な検査が必要なパケットは、高速化されたパスを使用できません。ファイアウォールがこれらのパケットを検査する必要はありません。これらのパケットはオフロードでき、低速パスを使用しません。たとえば、IPS によって検査されるパケットは高速パスを使用できず、IPS PSL (パッシブ ストリーミング ライブラリ) にオフロードできます。SecureXL は、これらのパケットを低速パスのパケットよりも高速に処理します。

最新問題: 49

デフォルトで R80 管理に含まれていない脅威対策プロファイルはどれですか？

- A. 基本 - ネットワーク パフォーマンスへの影響を最小限に抑えながら、さまざまな非 HTTP プロトコルで信頼性の高い保護をサーバーに提供します。
- B. 最適化 - 最近または一般的な攻撃に対して、一般的なネットワーク製品およびプロトコルに優れた保護を提供します。
- C. Strict - すべての製品とプロトコルを幅広くカバーし、ネットワーク パフォーマンスに影響を与えます。
- D. 推奨 - すべての一般的なネットワーク製品とサーバーにすべての保護を提供し、ネットワーク パフォーマンスに影響を与えます。

Answer: D ([メッセージを残す](#))

説明

参考文献:

最新問題: 50

読み取り/書き込みアクセスが有効になっていることを示すアイコンはどれですか？

- A. 鉛筆
- B. 南京錠
- C. 本
- D. めがね

Answer: ([解答を表示する](#))

解説 参考 :

最新問題: 51

このステートメントを完成させてください。アクティブ ログのブロック侵入者オプションが利用可能です_____。

- A. R75.40 リリース以降
- B. SmartView Tracker クライアント内
- C. SmartView Monitor クライアントで
- D. 少なくとも 1 つのゲートウェイで IPS ブレードが有効になっている場合のみ

Answer: B ([メッセージを残す](#))

最新問題: 52

R80 では、スプーフィングは次の方法として定義されています。

- A. ポート アドレス変換によって、許可された IP アドレスの背後に不正な IP アドレスを偽装する。
- B. 許可されていないユーザーからファイアウォールを隠します。
- C. 偽または間違った認証ログインを使用している人物の検出
- D. パケットが許可された IP アドレスから送信されたかのように見せかけます。

Answer: ([解答を表示する](#))

説明

IP スプーフィングは、信頼できない送信元 IP アドレスを偽の信頼できる IP アドレスに置き換えて、ネットワークへの接続をハイジャックします。攻撃者は IP スプーフィングを使用して、保護されたネットワークにマルウェアやボットを送信したり、DoS 攻撃を実行したり、不正アクセスを取得したりします。

最新問題: 53

SmartConsole に同時にログインしている 2 人の管理者がいて、編集のためにロックされているオブジェクトがある場合、他の管理者がそれらを使用できるようにするにはどうすればよいですか？

- A. セッションを発行または破棄します。
- B. セッションを元に戻します。
- C. ポリシーを保存してインストールします。
- D. 古いバージョンのデータベースを削除します。

Answer: A ([メッセージを残す](#))

説明

すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルールロックを解除するには、管理者はセッションを公開する必要があります。

他の管理者が変更を利用できるようにし、ポリシーをインストールする前にデータベースを保存するには、セッションを公開する必要があります。セッションを公開すると、新しいデータベース バージョンが作成されます。

[ポリシーのインストール] を選択すると、未公開のすべての変更を公開するように求められます。含まれている変更が公開されていない場合、ポリシーをインストールすることはできません。

最新問題: 54

内部ネットワーク 10.1.1.0/24、10.2.2.0/24、および 192.168.0.0/16 は Internet Security Gateway の背後にあります。

レイヤー 2 とレイヤー 3 のセットアップが正しいことを考慮して、接続を機能させるために SmartConsole で行う必要のある手順は何ですか？

- A.** 1. セキュリティ ポリシーで受け入れルールを定義します。
2. Security Gateway を定義して、ゲートウェイの外部 IP の背後にあるすべての内部ネットワークを非表示にします。
3. ポリシーを発行してインストールします。
- B.** 1. セキュリティ ポリシーで受け入れルールを定義します。
2. Security Gateway を定義して、ゲートウェイの外部 IP の背後にあるすべての内部ネットワークを非表示にします。
3. ポリシーを発行します。
- C.** 1. セキュリティ ポリシーで受け入れルールを定義します。
2. ネットワークごとに自動 NAT を定義して、パブリック IP の背後にあるネットワークを NAT します。
3. ポリシーを発行してインストールします。
- D.** 1. セキュリティ ポリシーで受け入れルールを定義します。
2. ネットワークごとに自動 NAT を定義して、パブリック IP の背後にあるネットワークを NAT します。
3. ポリシーを発行します。

Answer: ([解答を表示する](#))

最新問題: 55

SOLR データベースは何のためのものですか？

- A.** 全文検索に使用され、強力なマッチング機能を有効にします
- B.** データベースと全文検索にデータを書き込みます
- C.** 要求を DLE サーバーに転送する役割を担う GUI を提供します。
- D.** 強力な照合機能を有効にし、データベースにデータを書き込みます

Answer: A ([メッセージを残す](#))

解説 参考 https://en.wikipedia.org/wiki/Apache_Solr

最新問題: 56

通常、ユーザーがトークンを所有する必要がある、チェック ポイントがサポートする認証スキームはどれですか？

- A.** TACACS
- B.** SecurID
- C.** チェックポイントのパスワード
- D.** 半径

Answer: B ([メッセージを残す](#))

SecurID

SecurID では、ユーザーはトークン オーセンティケータを所有し、PIN またはパスワードを提供する必要があります。

最新問題: 57

Identity Awareness が有効になっている場合、Application Control にはどの ID ソースが使用されますか？

- A.** 半径
- B.** リモート アクセスと RADIUS
- C.** AD クエリ

D. AD クエリとブラウザベースの認証

Answer: D ([メッセージを残す](#))

説明

Identity Awareness は、次の取得ソースから ID を取得します。

AD クエリ

ブラウザベースの認証

エンドポイント ID エージェント

ターミナル サーバー アイデンティティ エージェント

リモートアクセス

参考文献:

最新問題: 58

ユーザー認証の失敗の原因となっているのはどのルールですか？

A. ルール 5

B. ルール 3

C. ルール 4

D. ルール 6

Answer: B ([メッセージを残す](#))

最新問題: 59

空欄を埋めてください: _____ は、VPN ゲートウェイが物理インターフェイスであるかのようにトラフィックを送信するために使用されます。

A. VPN トンネル インターフェイス

B. VPN コミュニティ

C. VPN ルーター

D. VPN インターフェース

Answer: A ([メッセージを残す](#))

ルートベース VPN

VPN トラフィックは、セキュリティのルーティング設定 (静的または動的) に従ってルーティングされます。

ゲートウェイ オペレーティング システム。Security Gateway は、VTI (VPN トンネル インターフェース) を使用して、物理インターフェースであるかのように VPN トラフィックを送信します。の Security Gateway の VTI

VPN コミュニティは接続し、動的ルーティング プロトコルをサポートできます。

最新問題: 60

あなたは Alpha Corp の管理者です。R80 管理サーバーにログインしています。ルール ベースにいくつかの変更を加えていると、ルール No.6 の横に鉛筆アイコンがあることがわかります。

これは何を意味するのでしょうか？

A. ルール No.6 は、管理セッションで削除対象としてマークされています。

B. ルール No.6 は、別の管理セッションで削除対象としてマークされています。

C. ルール No.6 は、別の管理セッションで編集するためにマークされています。

D. ルール No.6 は、管理セッションで編集するようにマークされています。

Answer: ([解答を表示する](#))

最新問題: 61

空欄に記入してください: RADIUS アカウンティングは、アカウンティング クライアントによって生成された要求から _____ データを取得します

A. 目的地

B. アイデンティティ

C. ペイロード

D. 場所

Answer: B ([メッセージを残す](#))

RADIUS アカウンティングと ID 認識の仕組み

RADIUS アカウンティングは、RADIUS アカウンティング クライアントによって生成された RADIUS アカウンティング要求から ID データを取得します。

参考 https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 62

R80 では、Unified Policy は

A. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、およびエンドポイント ポリシー。

B. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、および脅威対策ポリシー。

C. ファイアウォール ポリシー、アドレス変換とアプリケーションおよび URL フィルタリング、QoS ポリシー、デスクトップ セキュリティ

ポリシーと脅威防止ポリシー。

D. アクセス制御ポリシー、QoS ポリシー、デスクトップ セキュリティ ポリシー、および VPN ポリシー。

Answer: D ([メッセージを残す](#))

説明

選択肢から考えると D が最良の答えです。

統一されたポリシー

R80 では、アクセス コントロール ポリシーは、これらの R80 より前の Software Blade のポリシーを統合します。

最新問題: 63

分散展開オプションの代わりにスタンドアロン展開オプションを選択することの潜在的な欠点または欠点は何ですか？

- A. 追加の Check Point アプライアンスが必要です
- B. 追加のソフトウェア サブスクリプションが必要です
- C. コストアップ
- D. セキュリティ ポリシーのサイズが大きくなるにつれて、パフォーマンスが低下します。

Answer: ([解答を表示する](#))

最新問題: 64

レイヤーを編集するために、選択した管理者の権限を定義したいと考えています。ただし、「このレイヤーを編集できる追加のプロファイルを選択してください」の + 記号をクリックすると、何も表示されません。この問題の最も可能性の高い原因は何ですか？

- A. アクセス権限が制限された管理者権限プロファイルが定義されていません。
- B. 管理者権限プロファイルで Software Blade ごとにレイヤーを編集する」が選択されていない
- C. 利用可能な管理者権限プロファイルはありません。最初に作成する必要があります。
- D. すべての管理者権限プロファイルが使用されています。

Answer: C ([メッセージを残す](#))

最新問題: 65

Gaia Platform のユーザーを最もよく表しているものを選択してください。

- A. 削除できないデフォルト ユーザーが 1 つあります。
- B. 2 つのデフォルト ユーザーがあり、1 つは削除できません。
- C. 削除できるデフォルト ユーザーは 1 人です。
- D. 削除できないデフォルト ユーザーが 2 人、SmartConsole Administrator が 1 人います。

Answer: B ([メッセージを残す](#))

これらのユーザーはデフォルトで作成され、削除できません。

* admin - WebUI および CLI から、すべての Gaia 機能に対する完全な読み取り/書き込み機能を備えています。このユーザーのユーザー ID は 0 であるため、root ユーザーのすべての権限を持っています。

* モニター - WebUI および CLI のすべての機能に対して読み取り専用機能があり、独自のパスワードを変更できます。アカウントを使用する前に、このユーザーのパスワードを指定する必要があります。

参考 https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm

最新問題: 66

次の図では、ポリシーのレイヤーが示されています。

定義されたポリシーのトラフィック インспекションの優先順位は？

- A. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされます。その後、暗黙的なドロップルールによってパケットがドロップされた場合、パケットは IPS レイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。
- B. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合され、パケットを受け入れるルールがあれば、IPS レイヤーの次の場所に到着し、パケットを受け入れた後、Threat に渡されます。防止レイヤー
- C. パケットがゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合され、パケットを受け入れるルールがある場合は、[脅威] に続きます。

防御レイヤーを通過し、パケットを受け入れた後、IPS レイヤーに渡します。

D. パケットはゲートウェイに到着し、IPS ポリシー レイヤーのルールに対してチェックされ、次にネットワーク ポリシー レイヤーに到着し、パケットを受け入れた後、脅威防御レイヤーに渡されます。

Answer: B ([メッセージを残す](#))

ポリシー管理を簡素化するために、R80 はポリシーをポリシー レイヤーに編成します。レイヤーは一連のルール、つまりルール ベースです。

たとえば、以前のバージョンから R80 にアップグレードする場合:

ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

すべてのレイヤーが並行して評価されます

最新問題: 67

SmartConsole に表示される 不明な SIC ステータスは何を意味しますか?

A. SMS は Security Gateway に接続できますが、安全な内部通信を確立できません。

B. SIC アクティベーション キーはリセットが必要です。

C. SIC アクティベーション キーは、どの管理者にも知られていません。

D. Security Gateway と SMS の間に接続がありません。

Answer: D ([メッセージを残す](#))

説明

最も一般的なステータスは通信中です。その他のステータスは、SIC 通信が

問題あり。たとえば、SIC ステータスが不明の場合、ゲートウェイと

セキュリティ管理サーバー。SIC ステータスが Not Communicating の場合、Security Management Server は

ゲートウェイに接続できますが、SIC 通信を確立できません。

最新問題: 68

メッシュとスターは、2 種類の VPN トポロジです。これらのタイプのコミュニティについて正しいのは次のうちどれですか?

A. メッシュ コミュニティでは、メンバー ゲートウェイは互いに直接通信できません。

B. スター コミュニティでは、サテライト ゲートウェイは相互に通信できません。

C. メッシュ コミュニティでは、すべてのメンバーが他のメンバーとの間でトンネルを作成できます。

D. チェック ポイント独自のテクノロジーであるため、スター コミュニティにはチェック ポイントのゲートウェイが必要です。

Answer: ([解答を表示する](#))

最新問題: 69

帯域幅とトラフィック制御ルールを適用するために使用されるポリシーの種類はどれですか?

A. 脅威のエミュレーション

B. アクセス制御

C. QoS

D. 脅威対策

Answer: ([解答を表示する](#))

Check Point の QoS ソリューションQoS は、Check Point Software Technologies Ltd. が提供するポリシーベースの QoS 管理ソリューションであり、帯域幅管理ソリューションに対するお客様のニーズを満たします。QoS は、ネットワーク ハードウェアおよびソフトウェ

ア全体に適用を分散することにより、ネットワーク全体のトラフィックをエンド ツー エンドで管理する、独自のソフトウェア専用ベースのアプリケーションです。

最新問題: 70

チェック ポイントのセキュリティ管理アーキテクチャに不可欠な 3 つのコンポーネントは何ですか？

- A. SmartConsole、Security Management Server、Security Gateway
- B. SmartConsole、SmartUpdate、Security Gateway
- C. Security Management Server、Security Gateway、コマンドライン インターフェイス
- D. WebUI、SmartConsole、Security Gateway

Answer: A ([メッセージを残す](#))

解説 参考 :

説明: デプロイメント

基本的な展開:

スタンドアロン展開 - Security Gateway と Security Management Server が
同じマシン。

分散展開 - Security Gateway と Security Management Server がインストールされています。

異なるマシン。

異なるサイトにゲートウェイがある環境を想定します。各 Security Gateway は一方をインターネットに接続し、もう一方を LAN に接続します。

2 つの Security Gateway 間に Virtual Private Network (VPN) を作成して、その間のすべての通信を保護できます。

Security Management Server は LAN にインストールされ、Security Gateway によって保護されます。Security Management Server は Security Gateway を管理し、リモート ユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboard は、Security Management サーバーまたは別のコンピューターにインストールできます。

Security Management Server とその Security Gateway でネットワーク セキュリティを完成させるために、他の OPSEC パートナー モジュール (Anti-Virus Server など) が存在する場合があります。

参考 https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_SecurityManagement_WebAdminGuide/118037

最新問題: 71

空白を埋める: セキュリティ ポリシーは _____ で作成され、_____ に格納され、さまざまな _____ に配布されます。

- A. ルール ベース、セキュリティ管理サーバー、セキュリティ ゲートウェイ
- B. SmartConsole、Security Gateway、Security Management Server
- C. Check Point データベース、SmartConsole、Security Gateway
- D. SmartConsole、セキュリティ管理サーバー、セキュリティ ゲートウェイ

Answer: D ([メッセージを残す](#))

最新問題: 72

空欄に記入してください: RADIUS アカウンティングは、アカウンティング クライアントによって生成された要求から _____ データを取得します

- A. 目的地
- B. アイデンティティ
- C. ペイロード
- D. 場所

Answer: B ([メッセージを残す](#))

解説 参考 :

説明: RADIUS アカウンティングが Identity Awareness でどのように機能するか

RADIUS アカウンティングは、RADIUS アカウンティング クライアントによって生成された RADIUS アカウンティング要求から ID データを取得します。

参考 https://sc1.checkpoint.com/documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/html_frameset.htm?topic=documents/R77/CP_R77_IdentityAwareness_WebAdminGuide/62050

最新問題: 73

空欄に記入してください: R80 ユーティリティ ファームウェア モニターは、トラブルシューティングに使用されます _____

- A. ユーザー データベースの破損
- B. LDAP の競合
- C. トラフィックの問題
- D. フェーズ 2 のキー ネゴシエーション

Answer: C ([メッセージを残す](#))

説明

Check Point の FW Monitor は、ネットワーク トラフィックをパケット レベルでキャプチャするための強力な組み込みツールです。FW Monitor ユーティリティは、FireWall インスペクション チェーンに沿った複数のキャプチャ ポイントでネットワーク パケットをキャプチャします。

これらのキャプチャされたパケットは、後で WireShark を使用して検査できます。

最新問題: 74

CDT ユーティリティは、次のうちどれをサポートしていますか？

- A. R80.10 へのメジャー バージョン アップグレードのみ
- B. R77.30 へのメジャー バージョン アップグレード
- C. すべてのアップグレード
- D. ジャンボ HFA とホットフィックスのみ

Answer: ([解答を表示する](#))

最新問題: 75

会社のシステム管理者は、高速化がトラフィックに対して機能しない理由を見つけようとしています。トラフィックはルール ベースに従って許可され、ウイルス チェックが行われます。しかし、それは加速されていません。トラフィックが高速化されない最も可能性の高い理由は何ですか？

- A. ウイルスが見つかりました。トラフィックは引き続き許可されますが、加速されません
- B. 接続にはセキュリティ サーバーが必要でした
- C. アクセラレーションが無効

D. トラフィックはゲートウェイ自体から発信されています

Answer: D ([メッセージを残す](#))

説明

最新問題: 76

ルールを確認します。暗黙のルールでドメイン UDP が有効になっているとします。

内部ネットワークのユーザーが HTTP を使用してインターネットを閲覧しようとするとうどうなりますか? ユーザー :

A. クライアント認証デーモンのポート 259 に Telnet で接続すると、インターネットに接続できます。

B. 認証後、インターネットに正常に接続できます。

C. 認証を求められることなく、インターネットにアクセスできます。

D. インターネットに正常に接続する前に 3 回プロンプトが表示されます。

Answer: ([解答を表示する](#)**)**

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 77

お客様の R80 管理サーバーを R80.10 にアップグレードする必要があります。次の場合に最適なアップグレード方法は何ですか? 管理サーバーがインターネットに接続されていませんか?

A. CPUSE オフライン アップグレード

B. R80 構成をエクスポートし、R80.10 をクリーン インストールして、構成をインポートします。

C. SmartUpdate アップグレード

D. CPUSE オンラインアップグレード

Answer: A ([メッセージを残す](#))

最新問題: 78

ルール ベースとクライアント認証アクションのプロパティ画面を調べます。

Security Gateway によって認証された後、ユーザーは Web サイトへの HTTP 接続を開始します。ユーザーがコマンド ラインを使用して別のサイトに FTP で接続しようとするとうどうなりますか? :

A. ユーザーが正常に認証された後、FTP データ接続が切断されます。

B. ユーザーはその FTP サイトからのみ認証するように求められ、クライアント認証のためにユーザー名とパスワードを入力する必要はありません。

C. ユーザーは、Security Gateway によって再度認証を求められます。

D. FTP 接続はルール 2 によってドロップされます。

Answer: B ([メッセージを残す](#))

最新問題: 79

NAT の優先順位は何ですか？

- A. スタティック NAT、IP プール NAT、Hide NAT
- B. IP プール NAT、静的 NAT、非表示 NAT
- C. 静的 NAT、自動 NAT、非表示 NAT
- D. スタティック NAT、Hide NAT、IP プール NAT

Answer: A ([メッセージを残す](#))

説明

NAT の優先順位は次のとおりです。

スタティック NAT には IP プール NAT のすべての利点などがあるため、他の NAT 方式よりも優先度が高くなります。

最新問題: 80

ボブがオブジェクト検索でこの結果を得た場合、それはどういう意味ですか？ 下の画像を参照してください。最良の答えを選択する。

- A. 検索の詳細にサブネット マスクがありません。
- B. その名前またはその IP アドレスを持つオブジェクトはデータベースにありません。
- C. その IP アドレスを持つオブジェクトはデータベースにありません。
- D. オブジェクトに NAT IP アドレスがありません。

Answer: B ([メッセージを残す](#))

最新問題: 81

空白を埋めてください: User Directory Software Blade を使用すると、(an) 上に R80 ユーザ一定義を作成できます。
_____ サーバー。

- A. NT ドメイン
- B. SMTP
- C. LDAP
- D. SecurID

Answer: C ([メッセージを残す](#))

解説 参考：

参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

最新問題: 82

内部ネットワーク 10.1.1.0/24、10.2.2.0/24、および 192.168.0.0/16 は Internet Security Gateway の背後にあります。レイヤー 2 とレイヤー 3 のセットアップが正しいことを考慮して、接続を機能させるために SmartConsole で行う必要のある手順は何ですか？

- A. 1. セキュリティ ポリシーで受け入れルールを定義します。ネットワークごとに自動 NAT を定義して、パブリック IP の背後にあるネットワークを NAT します。3. ポリシーを発行してインストールします。
- B. 1. セキュリティ ポリシーで受け入れルールを定義します。Security Gateway を定義して、ゲートウェイの外部 IP の背後にあるすべての内部ネットワークを非表示にします。3. ポリシーを公開します。
- C. 1. セキュリティ ポリシーで受け入れルールを定義します。Security Gateway を定義して、ゲートウェイの外部 IP の背後にあるすべての内部ネットワークを非表示にします。3. ポリシーを発行してインストールします。

D. 1. セキュリティ ポリシーで受け入れルールを定義します。ネットワークごとに自動 NAT を定義して、パブリック IP の背後にあるネットワークを NAT します。3. ポリシーを公開します。

Answer: ([解答を表示する](#))

最新問題: 83

クラスター メンバーのフェイルオーバーはどこでトリガーできますか？

Security Gateway CLI にログインし、コマンド clusterXL_admin down を実行します。

SmartView Monitor で、Security Gateway メンバーを右クリックし、[Cluster member stop] を選択します。

Security Gateway CLI にログインし、コマンド cphaprob down を実行します。

A. 1、2、および 3

B. 2 と 3

C. 1 と 2

D. 1 と 3

Answer: C ([メッセージを残す](#))

解説 参考：

説明: フェイルオーバーを開始する方法

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7298.htm

最新問題: 84

チェックポイントのセキュリティ管理アーキテクチャに不可欠な 3 つのコンポーネントは何ですか？

A. SmartConsole、Security Management Server、Security Gateway

B. SmartConsole、SmartUpdate、Security Gateway

C. Security Management Server、Security Gateway、コマンドライン インターフェイス

D. WebUI、SmartConsole、Security Gateway

Answer: ([解答を表示する](#))

展開基本的な展開:

異なるサイトにゲートウェイがある環境を想定します。各 Security Gateway は一方をインターネットに接続し、もう一方を LAN に接続します。

2 つの Security Gateway 間に Virtual Private Network (VPN) を作成して、その間のすべての通信を保護できます。

Security Management Server は LAN にインストールされ、Security Gateway によって保護されます。Security Management Server は Security Gateway を管理し、リモート ユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboard は、Security Management サーバーまたは別のコンピューターにインストールできます。

Security Management Server とその Security Gateway でネットワーク セキュリティを完成させるために、他の OPSEC パートナー モジュール (Anti-Virus Server など) が存在する場合があります。

最新問題: 85

R80 Management のどのコンポーネントがインデックス作成に使用されますか？

A. DBSync

B. API サーバー

C. fwm

D. SOLR

Answer: D ([メッセージを残す](#))

解説 参考 :

参考 : <https://www.checkpoint.com/downloads/product-related/r80.10-mgmt-architecture-overview.pdf>

最新問題: 86

下のスクリーンショットを見てください。この出力を提供する CLISH コマンドはどれですか？

- A. 構成をすべて表示
- B. confd 構成を表示
- C. confd 構成をすべて表示
- D. 構成を表示

Answer: ([解答を表示する](#)**)**

解説 参考 :

Explanation:

参考 : http://dl3.checkpoint.com/paid/0c/0caa9c0daa67e0c1f2af3dd06790bc81/CP_R77_Gaia_AdminGuide.pdf?HashKey=1479835768_76058f0fc4209e38bc801cd58a85d7c5&xtn=.pdf

最新問題: 87

インターフェイスごとのマルチキューを有効または無効にするために使用できるコマンドはどれですか？

- A. cpmq セット
- B. Cpmqueue セット
- C. Cpmq 構成
- D. cpmq を有効に設定

Answer: A ([メッセージを残す](#))

参照 :

https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm

最新問題: 88

すべての構成を変更せずに監査するための完全なアクセス権を必要とする管理者に割り当てる必要がある事前定義済みのアクセス許可プロファイルはどれですか？

- A. 審査員
- B. すべて読み取り専用
- C. スーパーユーザー
- D. フルアクセス

Answer: B ([メッセージを残す](#))

解説 参考 :

説明: 新しい許可プロファイルを作成するには:

1. SmartConsole で、[管理と設定] > [権限と管理者] > [権限プロファイル] に移動します。
 2. [新しいプロファイル] をクリックします。
- [新しいプロファイル] ウィンドウが開きます。

3. プロファイルの一意の名前を入力します。

4. プロファイル タイプを選択します。

すべて読み取り/書き込み - 管理者は変更を加えることができます

監査者 (すべて読み取り専用) - 管理者は情報を表示できますが、変更はできません

カスタマイズ - カスタム設定の構成

5. [OK] をクリックします。

参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265

最新問題: 89

次のうち、推奨されるライセンス モデルはどれですか? ベスト アンサーを選択します。

A. パッケージ ライセンスをゲートウェイの IP アドレスに関連付け、Security Management Server に依存しないため、ローカル ライセンス。

B. パッケージ ライセンスをセキュリティの IP アドレスに関連付けるため、集中ライセンス Management Server であり、ゲートウェイの依存関係はありません。

C. パッケージ ライセンスをゲートウェイ管理インターフェイスの MAC アドレスに関連付け、Security Management Server に依存しないため、ローカル ライセンス。

D. パッケージ ライセンスをセキュリティの MAC アドレスに関連付けるため、集中ライセンス Management Server Mgmt インターフェイスであり、ゲートウェイに依存しません。

Answer: ([解答を表示する](#))

中央ライセンス

セントラル ライセンスは、ゲートウェイの IP アドレスではなく、Security Management サーバの IP アドレスに関連付けられたライセンスです。セントラル ライセンスの利点は次のとおりです。

最新問題: 90

あなたは大企業のセキュリティ管理者として働いています。あなたの会社の CSO はセキュリティ カンファレンスに出席し、ハッカーが戦略や手法を絶えず変更して検出を回避し、企業リソースに到達する方法を学びました。彼は、自分の会社が適切な保護を実施していることを確認したいと考えています。セキュリティベンダーにチェックポイントが選ばれました。安全なコンテンツをユーザーに迅速に配信しながら、マルウェアやゼロデイ攻撃から BEST を保護するチェック・ポイント製品はどれですか?

A. IPS とアプリケーション制御

B. IPS、ウイルス対策、ボット対策

C. IPS、ウイルス対策、メール セキュリティ

D. サンドブラスト

Answer: **D** ([メッセージを残す](#))

SandBlast ゼロデイ保護

ハッカーは、検出を回避して企業のリソースに到達するために、常に戦略と手法を変更しています。Check Point のゼロデイ エクスプロイト保護は、より深いレベルの検査を提供するため、より多くのマルウェアやゼロデイ攻撃を防止しながら、安全なコンテンツをユーザーに迅速に配信できます。

最新問題: 91

Dave と Jon の 2 人の管理者が ABC Corp の管理者として R80 Management を管理しています。Jon は R80 Management にログインし、Dave が同じサーバーにログインした直後にログインしました。どちらも [セキュリティ ポリシー] ビューにあります。以下のスクリーンショットから、Jon の SmartConsole ビューに規則 6 があるにもかかわらず、Dave の SmartConsole ビューに規則 6 がないのはなぜですか？

- A. Jon は現在ルール 6 を編集していますが、変更の一部を公開しています。
- B. Dave は現在ルール 6 を編集しており、このルールを削除対象としてマークしています。
- C. Dave は現在、ルール No.6 を編集しており、ルール ベースから削除しました。
- D. Jon は現在、ルール No.6 を編集していますが、まだ変更を公開していません。

Answer: D (メッセージを残す)

説明

管理者が SmartConsole を介して Security Management Server にログインすると、新しい編集セッションが開始されます。セッション中に管理者が行った変更は、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールにロック アイコンが表示されます。すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルールのロックを解除するには、管理者はセッションを公開する必要があります。

参考文献:

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 92

会社のビジネス パートナーの 1 人とサイト間 VPN を構成しようとしているときに、フェーズ 2 ネゴシエーションが失敗していると思われます。疑わしいことを確認するには、どの SmartConsole アプリケーションを使用する必要がありますか？

- A. SmartView トラッカー
- B. スマートダッシュボード
- C. SmartView ステータス
- D. SmartUpdate

Answer: A (メッセージを残す)

最新問題: 93

次の図では、ポリシーのレイヤーが示されています。

定義されたポリシーのトラフィック インспекションの優先順位は？

- A. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされます。その後、暗黙的なドロップルールによってパケットがドロップされた場合、パケットは IPS レイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。.

B. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合され、パケットを受け入れるルールがあれば、IPS レイヤーの次の場所に到着し、パケットを受け入れた後、Threat に渡されます。防止層

C. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合されます。パケットを受け入れるルールがあれば、次に脅威防御レイヤーに到達し、パケットを受け入れた後、次のレイヤーに渡されます。IPS レイヤー。

D. パケットはゲートウェイに到着し、IPS ポリシー レイヤーのルールに対してチェックされ、次にネットワーク ポリシー レイヤーに到着し、パケットを受け入れた後、脅威防御レイヤーに渡されます。

Answer: B (メッセージを残す)

ポリシー管理を簡素化するために、R80 はポリシーをポリシー レイヤーに編成します。レイヤーは一連のルール、つまりルール ベースです。

たとえば、以前のバージョンから R80 にアップグレードする場合:

ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

すべてのレイヤーが並行して評価されます

最新問題: 94

次の図では、管理者が Identity Awareness を構成しています。

[次へ] をクリックした後、上記の構成は以下でサポートされます。

A. Active Directory 統合のために機能する Kerberos SSO

B. Active Directory 統合に基づいており、Security Gateway は、ユーザーに対して完全に透過的な方法で、Active Directory ユーザーとマシンを IP アドレスに関連付けることができます。

C. キャプティブポータルの使用義務

D. ポート 443 または 80 は、ブラウザベースの構成済み認証で使用されます。

Answer: B (メッセージを残す)

説明

ID 認識を有効にするには:

Identity Awareness 設定ウィザードが開きます。

最新問題: 95

TCP/IP モデルのトランスポート層は何を担当していますか?

A. パケットをさまざまなルートに沿ってデータグラムとして転送し、宛先に到達させます。

B. 2 つのホスト間のデータの流れを管理して、パケットが正しく組み立てられ、ターゲット アプリケーションに配信されるようにします。

C. ネットワーク間でデータを交換するために使用されるプロトコルと、ホスト プログラムがアプリケーション層と対話する方法を定義します。

D. ネットワーク接続の物理コンポーネントのすべての側面を処理し、さまざまなネットワーク タイプに接続します。

Answer: B (メッセージを残す)

説明

最新問題: 96

次のうち、追跡オプションでないものはどれですか? (3つ選択)

A. 部分的なログ

B. ログ

C. ネットワークログ

D. フルログ

Answer: A,C,D ([メッセージを残す](#))

説明/参照:

https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide/131914

最新問題: 97

分散配置を使用している場合、Security Management Server で次のコマンドを実行すると、どのような影響がありますか？

A. インストールされているセキュリティ ポリシーを削除します。

B. ローカル ACL リストを削除します。

C. 効果なし。

D. すべてのゲートウェイで SIC をリセットします。

Answer: ([解答を表示する](#))

説明

このコマンドは、実際のセキュリティ ポリシーをアンインストールします (既にインストールされています)。

最新問題: 98

内部ルーターは、カプセル化されている UDP キープアライブ パケットを送信しています。

GRE に送信され、R77 Security Gateway を介してパートナー サイトに送信されます。ACCEPT/LOG には GRE トラフィックのルールが設定されています。キープアライブ パケットは毎分送信されていますが、GRE トラフィックの SmartView Tracker ログを検索すると、1 日 (ポリシー インストール後の早朝) の 1 つのエントリしか表示されません。

パートナー サイトは、GRE カプセル化キープアライブ パケットを 1 分間隔で正常に受信していることを示しています。

ルーターで GRE カプセル化がオフになっている場合、SmartView Tracker は UDP キープアライブ パケットのログ エントリを毎分表示します。

この動作の最も適切な説明は次のうちどれですか？

A. ログ統合プロセスは、破損した LUUID (ログ統合固有 ID) を使用しています。暗号化されているため、R77 Security Gateway は GRE セッションを区別できません。これは GRE の既知の問題です。カプセル化には、非標準の GRE プロトコルの代わりに IPSEC を使用します。

B. 設定ログは、GRE のこのレベルの詳細をキャプチャしません。特定のタイプのトラフィックはこの方法でしか追跡できないため、ルール追跡アクションを監査に設定します。

C. VPN トラフィックであるため、Log Server は GRE トラフィックを正しくログに記録できません。すべて無効にする適切なログ記録を有効にするためのパートナー サイトへの VPN 構成。

D. Log Server ログ統合プロセスは、特定の接続上の Security Gateway からのすべてのログ エントリを、SmartView Tracker 内の 1 つのログ エントリに統合します。GRE トラフィックには

10 分間のセッション タイムアウト。したがって、各キープアライブ パケットは、1 日の初めにログに記録された元の接続の一部と見なされます。

Answer: D ([メッセージを残す](#))

最新問題: 99

チェック ポイントのコンポーネント間で信頼関係が確立された後、名前と IP アドレスの変更について正しいのはどれですか？

- A. Security Gateway の IP アドレスは、信頼を再確立しないと変更できません
- B. 信頼を再確立しないと、コマンドラインで Security Gateway 名を変更できません。
- C. 信頼を再確立しないと、SmartConsole で Security Management Server 名を変更できません。
- D. Security Management Server の IP アドレスは、信頼を再確立しないと変更できません

Answer: A ([メッセージを残す](#))

解説 参考 :

最新問題: 100

Gaia Platform で役割を編集するとき、機能に与えられるオプションはどれですか？

- A. 読み取り/書き込み、読み取り専用
- B. 読み取り/書き込み、読み取り専用、なし
- C. 読み取り/書き込み、なし
- D. 読み取り専用、なし

Answer: B ([メッセージを残す](#))

役割

役割ベースの管理 (RBA) を使用すると、ユーザーの管理役割を作成できます。RBA を使用すると、管理者は、役割にそれらの機能を含め、その役割をユーザーに割り当てることにより、Gaia ユーザーが指定された機能にアクセスできるようにすることができます。各役割には、一部の機能への管理 (読み取り/書き込み) アクセス、他の機能への監視 (読み取り専用) アクセス、および他の機能へのアクセスなしの組み合わせを含めることができます。

また、ユーザーが使用できるアクセス メカニズム (WebUI または CLI) を指定することもできます。

注 - ユーザーが WebUI にログインすると、読み取り専用または読み取り/書き込みアクセス権を持つ機能のみが表示されます。機能への読み取り専用アクセス権を持つユーザーは、設定ページを表示できますが、設定を変更することはできません。

Gaia には、次の事前定義された役割が含まれています。

定義済みロールを削除または変更することはできません。

注 - 外部ユーザー用に新しいユーザーを定義しないでください。外部ユーザーとは、ローカルの Gaia システムではなく、認証サーバー (RADIUS や TACACS など) で定義されているユーザーです。

最新問題: 101

ドロップ テンプレートがアクティブになっているかどうかを確認するのに適したコマンドはどれですか？

- A. fwaccel 統計
- B. fw ctl テンプレート -d
- C. fw ctl get int activate_drop_templates
- D. fwaccel 統計

Answer: A ([メッセージを残す](#))

最新問題: 102

ユーザー、グループ、およびマシンの可視性を提供すると同時に、ID ベースのポリシーによるアクセス制御も提供するチェック ポイントのソフトウェア ブレードはどれですか？

- A. ファイアウォール
- B. アイデンティティの認識
- C. アプリケーション制御
- D. URL フィルタリング

Answer: B ([メッセージを残す](#))

説明

Check Point Identity Awareness Software Blade は、ユーザー、グループ、およびマシンをきめ細かく可視化し、正確な ID ベースのポリシーを作成することで、比類のないアプリケーションとアクセス制御を提供します。集中管理と監視により、単一の統合コンソールからポリシーを管理できます。

参考文献:

最新問題: 103

次のうち、Threat Extraction がどのように機能するかを説明しているのはどれですか？

- A. プロアクティブに脅威を検出
- B. オリジナルコンテンツのファイルを配信
- C. アクティブ コンテンツが削除された元のファイルの PDF バージョンを配信します。
- D. 脅威を検出し、検出された脅威の詳細なレポートを提供します

Answer: A ([メッセージを残す](#))

最新問題: 104

いつ新しいライセンスを生成する必要がありますか？

- A. アプライアンスの MAC アドレスまたはシリアル番号が変更されたときの RMA 手続きの後。
- B. 契約ファイルをインストールする前。
- C. ライセンスをアップグレードした場合のみ。
- D. 既存のライセンスの有効期限が切れた場合、ライセンスがアップグレードされるか、ライセンスが関連付けられている IP アドレス変化します。

Answer: A ([メッセージを残す](#))

最新問題: 105

Security Management Server で次のコマンドを実行すると、どのような影響がありますか？

- A. インストールされているセキュリティ ポリシーを削除します。
- B. ローカル ACL リストを削除します。
- C. 効果なし。
- D. すべてのゲートウェイで SIC をリセットします。

Answer: A ([メッセージを残す](#))

説明

このコマンドは、実際のセキュリティ ポリシーをアンインストールします (既にインストールされています)。

参考文献:

最新問題: 106

すべての製品とプロトコルを非常に幅広くカバーし、パフォーマンスに顕著な影響を与えます。

適切なレベルのセキュリティを維持しながら CPU 負荷を下げるために、プロファイルをどのように調整できますか？ ベストアンサーを選択してください。

- A. パフォーマンスへの影響を中以下に設定します。
- B. 高信頼度を低に、低信頼度を非アクティブに設定します。
- C. 脅威対策プロファイルに問題はありません。アプライアンスにメモリを追加することを検討してください。
- D. 回避するには、パフォーマンスへの影響を非常に低い信頼度に設定します。

Answer: A (メッセージを残す)

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 107

空欄を埋めてください: _____ は、VPN ゲートウェイが物理インターフェイスであるかのようにトラフィックを送信するために使用されます。

- A. VPN トンネル インターフェイス
- B. VPN コミュニティ
- C. VPN ルーター
- D. VPN インターフェース

Answer: A (メッセージを残す)

解説 参考 :

説明: ルートベースの VPN

VPN トラフィックは、Security Gateway オペレーティング システムのルーティング設定 (静的または動的) に従ってルーティングされます。Security Gateway は、VTI (VPN トンネル インターフェース) を使用して、物理インターフェースであるかのように VPN トラフィックを送信します。VPN コミュニティ内の Security Gateway の VTI は接続し、ダイナミック ルーティング プロトコルをサポートできます。

参照: http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

最新問題: 108

NAT エントリのトラブルシューティングに SmartView Tracker を使用しています。Source NAT を使用している場合、NAT された送信元ポートを確認するためにどの列をチェックしますか？

- A. XlateDPort
- B. XlateSrc
- C. XlateDst
- D. XlateSPort

Answer: D ([メッセージを残す](#))

最新問題: 109

次のうち、SecureXL トラフィック フローでないものはどれですか？

- A. ミディアム パス
- B. 加速パス
- C. ファスト パス
- D. スローパス

Answer: ([解答を表示する](#))

説明

SecureXL は、ファイアウォールのパフォーマンスを最大化し、セキュリティを損なうことのないアクセラレーション ソリューションです。Security Gateway で SecureXL が有効になっている場合、一部の CPU を集中的に使用する操作は、ファイアウォール カーネルではなく、仮想化されたソフトウェアによって処理されます。ファイアウォールは、接続をより効率的に検査および処理し、スループットと接続速度を加速できます。これらは SecureXL トラフィック フローです:

低速パス - ファイアウォールによって検査され、SecureXL によって処理されないパケットと接続。

加速パス - SecureXL にオフロードされ、ファイアウォールによって処理されないパケットと接続。

中程度のパス - より詳細な検査が必要なパケットは、高速化されたパスを使用できません。ファイアウォールがこれらのパケットを検査する必要はありません。これらのパケットはオフロードでき、低速パスを使用しません。たとえば、IPS によって検査されるパケットは高速パスを使用できず、IPS PSL (パッシブ ストリーミング ライブラリ) にオフロードできます。SecureXL は、これらのパケットを低速パスのパケットよりも高速に処理します。

最新問題: 110

空欄を埋めてください: ツール _____ は、R80 Security Gateway 構成レポートを生成します。

- A. 情報CP
- B. 情報ビュー
- C. cpinfo
- D. fw cpinfo

Answer: C ([メッセージを残す](#))

CPInfo は、実行時に顧客のマシンで診断データを収集し、チェック ポイント サーバーにアップロードする自動更新ユーティリティです (ファイルをチェック ポイント サーバーにアップロードするためのスタンドアロン cp_uploader ユーティリティを置き換えます)。

CPinfo 出力ファイルにより、離れた場所から顧客の設定を分析できます。小切手

ポイント サポート エンジニアは、実際の顧客のセキュリティ ポリシーとオブジェクトを表示しながら、CPinfo ファイルをデモ モードで開くことができます。これにより、お客様の構成と環境設定を詳細に分析できます。

チェック ポイントのサポートに連絡する際は、セキュリティ ページから cpinfo ファイルを収集してください。

ケースに関係する管理サーバーとセキュリティ ゲートウェイ。

最新問題: 111

空白を埋める: アプリケーション層ファイアウォールは、TCP/IP モデルの _____ 層を通過し、_____ 層までのトラフィックを検査します。

- A. 最初の 2 つ。輸送

- B. 下; 応用
C. 最初の 2 つ。インターネット
D. 上; 応用
Answer: B ([メッセージを残す](#))

最新問題: 112

空欄を埋めてください: _____ は、VPN ゲートウェイが物理インターフェイスであるかのようにトラフィックを送信するために使用されます。

- A. VPN トンネル インターフェイス
B. VPN コミュニティ
C. VPN ルーター
D. VPN インターフェース

Answer: A ([メッセージを残す](#))

説明

ルートベース VPN

VPN トラフィックは、Security Gateway オペレーティング システムのルーティング設定 (静的または動的) に従ってルーティングされます。Security Gateway は、VTI (VPN トンネル インターフェース) を使用して、物理インターフェースであるかのように VPN トラフィックを送信します。VPN コミュニティ内の Security Gateway の VTI は接続し、ダイナミック ルーティング プロトコルをサポートできます。

参考文献:

最新問題: 113

アクセス ロールにより、ファイアウォール管理者は次のようにネットワーク アクセスを構成できます。

- A. コンピュータグループとネットワークの組み合わせ
B. ユーザーとユーザー グループ
C. 上記すべて
D. リモート アクセス クライアント

Answer: ([解答を表示する](#))

説明

アクセス ロールを作成するには:

[アクセス ロール] ウィンドウが開きます。

選択内容は、[役割のプレビュー] ペインの [ネットワーク] ノードに表示されます。

ウィンドウが開きます。Active Directory エントリを検索するか、リストから選択できます。

AD エントリを検索するか、リストから選択できます。

アクセス ロールが [ユーザーと管理者] ツリーに追加されます。

最新問題: 114

ALPHA Corp ネットワークの管理者である Kofi は、デフォルトの HTTPS ポートに現在設定されているデフォルトの Gaia WebUI ポータルのポート番号を変更したいと考えています。この TCP ポートを変更するには、どの CLISH コマンドが必要ですか?

- A. set web ssl-port <新しいポート番号>
B. Gaia-portal ポートを設定 <新しいポート番号>

C. Gaia-portal https-port <新しいポート番号> を設定します

D. Web https-port <新しいポート番号> を設定します

Answer: A (メッセージを残す)

クリッシュで

A. Security Gateway / 各クラスタ メンバーのコマンド ラインに接続します。

B. Clish にログインします。

C. 目的のポートを設定します (例: ポート 4434):

HostName> web ssl-port <Port_Number> を設定します

D. 変更を保存します。

ホスト名 > 設定を保存

E. 構成が保存されたことを確認します。

[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial

参考 :[https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482)

最新問題: 115

Gaia Platform のユーザーを最もよく表しているものを選択してください。

A. 削除できないデフォルト ユーザーが 1 つあります。

B. 2 つのデフォルト ユーザーがあり、1 つは削除できません。

C. 削除できるデフォルト ユーザーは 1 人です。

D. 2 つのデフォルト ユーザーがあり、どちらも削除できません。

Answer: B (メッセージを残す)

説明

これらのユーザーはデフォルトで作成され、削除できません。

* admin - WebUI および CLI から、すべての Gaia 機能に対する完全な読み取り/書き込み機能を備えています。このユーザーのユーザー ID は 0 であるため、root ユーザーのすべての権限を持っています。

* モニター - WebUI および CLI のすべての機能に対して読み取り専用機能があり、独自のパスワードを変更できます。アカウントを使用する前に、このユーザーのパスワードを指定する必要があります。

最新問題: 116

このセキュリティ ポリシーを確認する際に、ルール 4 に対応するためにどのような変更を加えることができますか？

A. 何もない

B. ルール 4 の列のサービスからサービス HTTP を削除します。

C. ルール 2 の列 VPN を変更して、特定のトラフィックへのアクセスを制限します。

D. ルール 4 の送信元または宛先の列を変更します。

Answer: C (メッセージを残す)

最新問題: 117

サテライト ゲートウェイが処理するすべての接続に VPN ルーティングを使用する VPN ルーティング オプションはどれですか？

A. センターのみ経由でサテライトへ

- B. 中央のみへ
- C. センターへ、センター経由で他の衛星へ
- D. センターへ、またはセンターを経由して他の衛星へ、インターネットや他の VPN ターゲットへ

Answer: ([解答を表示する](#))

説明

[VPN ルーティング] ページで、次のいずれかのオプションを選択して、サテライト セクションの VPN ルーティングを有効にします。

最新問題: 118

SmartConsole のタブの [ポリシーのインストール] ボタンと特定のポリシー内の [ポリシーのインストール] ボタンの違いの最も完全な定義は何ですか？

- A. ローカル ポリシーは、マルウェア対策ポリシーをネットワーク ポリシーと共にインストールしません。
- B. グローバル 1 は、選択した複数のポリシーを同時にインストールできます。
- C. 2 つ目は、現在のポリシーと適用可能なゲートウェイのみのインストールを事前に選択します。
- D. Global も、インストール前にセッションを保存して公開します。

Answer: C ([メッセージを残す](#))

最新問題: 119

ユーザーがトークンを所有する必要がある認証スキームはどれですか？

- A. TACACS
- B. SecurID
- C. チェックポイントのパスワード
- D. 半径

Answer: ([解答を表示する](#))

解説 参考 :

説明: SecurID

SecurID では、ユーザーはトークン オーセンティケーターを所有し、PIN またはパスワードを提供する必要があります。

最新問題: 120

SmartEvent で、管理者が構成できるさまざまなタイプの自動応答は何ですか？

- A. メール、ブロック ソース、ブロック イベント アクティビティ、外部スクリプト、SNMP トラップ
- B. メール、ブロック元、ブロック先、ブロック サービス、SNMP トラップ
- C. メール、ブロック元、ブロック先、外部スクリプト、SNMP トラップ
- D. メール、ブロック ソース、ブロック イベント アクティビティ、パケット キャプチャ、SNMP トラップ

Answer: A ([メッセージを残す](#))

解説 参考 :

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_SmartEvent_AdminGuide/17401.htm

最新問題: 121

次の機能のうち、チェック ポイントの URL フィルタリングとアプリケーション制御に関連付けられていないものはどれですか？

- A. ユーザーが影響を受ける前に、複数の検出エンジンを関連付けることで、マルウェアを検出してブロックします。
- B. UserCheck を使用して、特定の Web サイトが会社のセキュリティ ポリシーに違反していることをユーザーが理解できるようにします。
- C. 指定したユーザーまたはグループの使用可能なネットワーク帯域幅を制限するルールを構成します。
- D. 個々のアプリケーション、カテゴリ、およびリスクレベル。

Answer: ([解答を表示する](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **122**

次のうち、Identity Awareness に使用される ID ソースでないものはどれですか？

- A. リモートアクセス
- B. ユーザーチェック
- C. AD クエリ
- D. 半径

Answer: B ([メッセージを残す](#))

解説 参考 <https://www.checkpoint.com/products/identity-awareness-software-blade/>

最新問題: **123**

すべての製品とプロトコルを非常に幅広くカバーし、パフォーマンスに顕著な影響を与えます。

適切なレベルのセキュリティを維持しながら CPU 負荷を下げるために、プロファイルをどのように調整できますか？ ベストアンサーを選択してください。

- A. 高信頼度を低に、低信頼度を非アクティブに設定します。
- B. パフォーマンスへの影響を中以下に設定します。
- C. 脅威対策プロファイルに問題はありません。アプライアンスにメモリを追加することを検討してください。
- D. 回避するには、パフォーマンスへの影響を非常に低い信頼度に設定します。

Answer: ([解答を表示する](#))

最新問題: **124**

Gaia で構成ロックを取得するために使用されるコマンドはどれですか？

- A. ロック データベース オーバーライド
- B. データベース オーバーライドのロック解除
- C. データベース ロックのロックを解除します。
- D. データベース ユーザーのロック

Answer: A (メッセージを残す)

構成ロックの取得

最新問題: 125

ALPHA Corp ネットワークの管理者である Kofi は、デフォルトの HTTPS ポートに現在設定されているデフォルトの Gaia WebUI ポータルのポート番号を変更したいと考えています。この TCP ポートを変更するには、どの CLISH コマンドが必要ですか？

- A. set web ssl-port <新しいポート番号>
- B. Gaia-portal <新しいポート番号> を設定します。
- C. Gaia-portal https-port <新しいポート番号> を設定します
- D. Web https-port <新しいポート番号> を設定します

Answer: A (メッセージを残す)

解説 参考 :

1. 説明:

クリッシュで

A. Security Gateway / 各クラスタ メンバーのコマンドラインに接続します。

B. Clish にログインします。

C. 目的のポートを設定します (例: ポート 4434):

HostName> web ssl-port <Port_Number> を設定します

D. 変更を保存します。

ホスト名 > 設定を保存

E. 構成が保存されたことを確認します。

[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial

参考 :[https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk83482)

最新問題: 126

パケット フィルタリングの利点ではないものは何ですか？

- A. セキュリティが低く、ネットワーク レイヤー上でのスクリーニングなし
- B. アプリケーション非依存
- C. ハイパフォーマンス
- D. スケーラビリティ

Answer: A (メッセージを残す)

解説 参考 :

解説 :パケットフィルターのメリットとデメリット

参考 :<https://www.checkpoint.com/smb/help/utm1/8.2/7078.htm>

最新問題: 127

どの構成要素が、どのトラフィックを VPN トンネルに暗号化する必要があるか、または VPN トンネルで送信する必要があるかを決定します。

クリア？

- A. ファイアウォール トポロジ
- B. VPN ドメイン
- C. ルールベース
- D. NAT ルール

Answer: ([解答を表示する](#))

最新問題: 128

セキュリティ ポリシーを正しく適用するには、Security Gateway に次のものがが必要です。

- A. ルーティング テーブル
- B. ネットワークトポロジーの認識
- C. 非武装地帯
- D. セキュリティ ポリシーのインストール

Answer: B ([メッセージを残す](#))

ネットワーク トポロジは、ゲートウェイによって保護される内部ネットワーク (LAN と DMZ の両方) を表します。ゲートウェイは、ネットワーク トポロジのレイアウトを認識して、次のことを行う必要があります。

- * セキュリティ ポリシーを正しく実施する。
- * インバウンドおよびアウトバウンド トラフィックの IP アドレスの有効性を確認します。
- * バーチャル プライベート ネットワーク用の特別なドメインを構成します。

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm?topic=documents/R76/CP_R76_SecMan_WebAdmin/118037

最新問題: 129

次のスクリーンショットを見て、最良の回答を選択してください。

- A. 内部クライアントは、FTP を使用してアーカイブ ファイルを FTP_Ext サーバーにアップロードおよびダウンロードできます。
- B. Security Gateway の外部にあるクライアントは、FTP を使用して FTP_Ext サーバーからアーカイブ ファイルをダウンロードできます。
- C. 内部クライアントは、FTP を使用して任意のファイルを FTP_Ext-server にアップロードおよびダウンロードできます。
- D. Security Gateway の外部にあるクライアントは、FTP を使用して任意のファイルを FTP_Ext-server にアップロードできます。

Answer: ([解答を表示する](#))

最新問題: 130

次のうち、SecureXL トラフィック フローでないものはどれですか？

- A. ミディアム パス
- B. 加速パス
- C. ファスト パス
- D. スローパス

Answer: C ([メッセージを残す](#))

SecureXL は、ファイアウォールのパフォーマンスを最大化し、セキュリティを損なうことのないアクセラレーション ソリューションです。Security Gateway で SecureXL が有効になっている場合、一部の CPU を集中的に使用する操作は、ファイアウォール カーネルではなく、仮想化されたソフトウェアによって処理されます。

ファイアウォールは、接続をより効率的に検査および処理し、スループットと接続速度を加速できます。これらは SecureXL トラフィックフローです:

低速パス - ファイアウォールによって検査され、SecureXL によって処理されないパケットと接続。

加速パス - SecureXL にオフロードされ、ファイアウォールによって処理されないパケットと接続。

中程度のパス - より詳細な検査が必要なパケットは、高速化されたパスを使用できません。ファイアウォールがこれらのパケットを検査する必要はありません。これらのパケットはオフロードでき、低速パスを使用しません。たとえば、IPS によって検査されるパケットは高速パスを使用できず、IPS PSL (パッシブ ストリーミング ライブラリ) にオフロードできます。

SecureXL は、これらのパケットを低速パスのパケットよりも高速に処理します。

最新問題: 131

R77 Windows CDからインストールできるSmartConsoleクライアントは次のうちどれですか? すべての回答を読み、最も完全で有効なリストを選択してください。

- A. セキュリティ ポリシー エディタ、ログ ビューア、リアルタイム モニタ GUI
- B. SmartView トラッカー、SmartDashboard、CPINFO、SmartUpdate、SmartView ステータス
- C. SmartView トラッカー、CPINFO、SmartUpdate
- D. SmartView トラッカー、SmartDashboard、SmartLSM、SmartView モニター

Answer: C ([メッセージを残す](#))

最新問題: 132

ウイルス シグネチャと ThreatCloud の異常ベースの保護を使用して、悪意のあるファイルがネットワークに侵入するのを防いでいるチェック ポイントのソフトウェア ブレードはどれですか?

- A. ファイアウォール
- B. アプリケーション制御
- C. スпам対策とメール セキュリティ
- D. ウイルス対策

Answer: D ([メッセージを残す](#))

説明

強化された Check Point Antivirus Software Blade は、リアルタイムのウイルス シグネチャと、サイバー犯罪と闘う最初の共同ネットワークである ThreatCloud の異常ベースの保護を使用して、ユーザーが影響を受ける前にゲートウェイでマルウェアを検出してブロックします。

参考文献:

最新問題: 133

AdminA と AdminB は両方とも SmartConsole にログインしています。AdminB がルールにロックされたアイコンを表示する場合、それはどういう意味ですか? 最良の答えを選択する。

- A. ルールのオブジェクトが編集されたため、ルールは AdminA によってロックされています。
- B. ルールは AdminA によってロックされており、セッションが公開された場合に使用可能になります。
- C. 保存ボタンが押されていないため、ルールは AdminA によってロックされています。
- D. ルールは AdminA によってロックされており、セッションが保存されるとルールが使用可能になります

Answer: B ([メッセージを残す](#))

最新問題: 134

帯域幅とトラフィック制御ルールを適用するために使用されるポリシーの種類はどれですか？

- A. 脅威のエミュレーション
- B. アクセス制御
- C. QoS
- D. 脅威対策

Answer: C (メッセージを残す)

解説 参考 :

Explanation:

チェック ポイントの QoS ソリューション

QoS は、Check Point Software Technologies Ltd. のポリシーベースの QoS 管理ソリューションであり、帯域幅管理ソリューションのニーズを満たします。QoS は、ネットワーク ハードウェアおよびソフトウェア全体に適用を分散することにより、ネットワーク全体のトラフィックをエンド ツー エンドで管理する、独自のソフトウェア専用ベースのアプリケーションです。

参考 https://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/index.html

最新問題: 135

2 人の管理者 Dave と Jon は両方とも、Alpha Corp の管理者として R80 Management を管理しています。Jon は R80 Management にログインし、Dave が同じサーバーにログインした直後にログインしました。どちらも [セキュリティ ポリシー] ビューにあります。以下のスクリーンショットから、Jon の SmartConsole ビューに規則 6 があるにもかかわらず、Dave の SmartConsole ビューに規則 6 がないのはなぜですか？

- A. Jon は現在ルール 6 を編集していますが、変更の一部を公開しています。
- B. Dave は現在ルール 6 を編集しており、このルールを削除対象としてマークしています。
- C. Dave は現在、ルール No.6 を編集しており、ルール ベースから削除しました。
- D. Jon は現在、ルール No.6 を編集していますが、まだ変更を公開していません。

Answer: D (メッセージを残す)

管理者が SmartConsole を介して Security Management Server にログインすると、新しい編集セッションが開始されます。セッション中に管理者が行った変更は、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールにロック アイコンが表示されます。すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルールのロックを解除するには、管理者はセッションを公開する必要があります。

最新問題: 136

SandBlast には、攻撃をリアルタイムで防止するために連携する機能コンポーネントがいくつかあります。次のうち、SandBlast コンポーネントの一部でないものはどれですか？

- A. 脅威のエミュレーション
- B. モバイル アクセス
- C. メール転送エージェント
- D. 脅威の雲

Answer: C (メッセージを残す)

解説 参考 :

参考 <https://www.checkpoint.com/products-solutions/zero-day-protection/>

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 137

チェック・ポイントのホスト・オブジェクトについて正しいものは次のうちどれですか？

- A. チェック ポイント ホストは、ファイアウォールとして機能できます。
- B. R77.30 以前のバージョンから R80 にアップグレードすると、チェック ポイント ホスト オブジェクトはゲートウェイ オブジェクトに変換されます。
- C. チェック・ポイント・ホストは、IP 転送メカニズムを持つことができます。
- D. チェック ポイント ホストには、複数のインターフェイスがインストールされていてもルーティング機能がありません。

Answer: D ([メッセージを残す](#))

最新問題: 138

LDAP が Check Point Security Management と統合されると、_____ と呼ばれます。

- A. ユーザーチェック
- B. ユーザー ディレクトリ
- C. ユーザー管理
- D. ユーザーセンター

Answer: ([解答を表示する](#))

Check Point User Directory は、LDAP およびその他の外部ユーザー管理テクノロジーを Check Point ソリューションと統合します。ユーザー数が多い場合は、Security Management Server のパフォーマンスを向上させるために、LDAP などの外部ユーザー管理データベースを使用することをお勧めします。

参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/118981

最新問題: 139

(n) _____ ルールは管理者によって作成され、ルール ベース内の最初と最後のルールの前に配置されます。

- A. ファイアウォール ドロップ
- B. 明示的
- C. 暗黙の受け入れ
- D. 暗黙のドロップ
- E. 暗示

Answer:

ルールが適用される順序は次のとおりです。

1. 最初の暗黙のルール: このルールを編集または削除することはできず、その前に明示的なルールを配置することはできません。
2. 明示的なルール: これらはユーザーが作成するルールです。
3. 最後の暗黙ルールの前: これらの暗黙ルールは、最後の明示ルールの前に適用されます。
4. 最後の明示的なルール: クリーンアップ ルールを最後の明示的なルールとして使用することをお勧めします。
5. Last Implied Rules: グローバル プロパティで Last として設定された暗黙のルール。
6. 暗黙のドロップ ルール: ログを記録せずにすべてのパケットをドロップします。

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

最新問題: 140

IKE によって実行される 2 フェーズ ネゴシエーション プロセスのフェーズ 1 は、_____ モードで動作します。

- A. メイン
- B. 認証
- C. クイック
- D. 高警報

Answer: ([解答を表示する](#))

フェーズ 1 モード

Security Gateway 間では、IKE フェーズ 1 に 2 つのモードがあります。

これらのモードは IKEv1 にのみ適用されます。

最新問題: 141

エンドポイント ID エージェントは、ユーザー認証に _____ を使用します。

- A. 共有シークレット
- B. トークン
- C. ユーザー名/パスワードまたは Kerberos チケット
- D. 証明書

Answer: ([解答を表示する](#))

解説 参考: <https://sc1.checkpoint.com/documents/R76/>

CP_R76_IdentityAwareness_AdminGuide/62050.htm

最新問題: 142

セキュリティ監査を実施しています。構成ファイルとログを確認しているときに、ログが受け入れていることに気付く POP3 トラフィックですが、Rule Base に POP3 トラフィックを許可するルールが表示されません。次のうちどれですか最も可能性の高い原因は？

- A. POP3 は、R77 の既定のメール オブジェクトで受け入れられる 3 つのサービス (POP3、IMAP、SMTP) の 1 つです。
- B. POP3 ルールは無効です。
- C. POP3 はグローバル プロパティで受け入れられます。
- D. POP3 ルールは非表示です。

Answer: D ([メッセージを残す](#))

最新問題: 143

完全ログ」追跡オプションには含まれるが、「ログ」追跡オプションには含まれない情報はどれですか？

- A. ファイル属性
- B. アプリケーション情報
- C. データ型情報
- D. 宛先ポート

Answer: ([解答を表示する](#))

最新問題: 144

SmartEvent がイベントの識別に使用しない手順は次のとおりです。

- A. ローカル除外に対するログの照合
- B. イベント候補を作成する
- C. グローバル除外に対するログの照合
- D. ログと各イベント定義の照合

Answer: ([解答を表示する](#))

最新問題: 145

R80.10 で、LEA (ログ エクスポート API) を使用してログを読み取るようにサードパーティ デバイスを構成する場合、デフォルト Log Server は次のポートを使用します:

- A. 18184
- B. 18191
- C. 18210
- D. 257

Answer: A ([メッセージを残す](#))

最新問題: 146

次のオブジェクトのうち、NAT を構成できないものはどれですか？

- A. アドレス範囲
- B. ホスト
- C. ゲートウェイ
- D. HTTP 論理サーバー

Answer: ([解答を表示する](#))

最新問題: 147

インターフェイスごとのマルチキューを有効または無効にするために使用できるコマンドはどれですか？

- A. cpmq セット
- B. Cpmqueue セット
- C. Cpmq 構成
- D. cpmq を有効に設定

Answer: A ([メッセージを残す](#))

解説 参考 https://sc1.checkpoint.com/documents/R76/CP_R76_PerformanceTuning_WebAdmin/93689.htm

最新問題: 148

ALPHA Corp ネットワークの管理者である Kofi は、デフォルトの Gaia WebUI ポータル ポートを変更したいと考えています。デフォルトの HTTPS ポートに現在設定されている番号。変更できるようにするために必要な CLISH コマンドはどれですかこのTCPポート？

- A. set web ssl-port <新しいポート番号>
- B. Gaia-portal <新しいポート番号> を設定します。
- C. Gaia-portal https-port <新しいポート番号> を設定します
- D. Web https-port <新しいポート番号> を設定します

Answer: ([解答を表示する](#))

説明

クリッシュで

HostName> web ssl-port <Port_Number> を設定します

ホスト名 > 設定を保存

[Expert@HostName]# grep 'httpd:ssl_port' /config/db/initial

最新問題: 149

サイト間 IPSEC セキュリティ アソシエーション (SA) を削除するために使用できるコマンドは次のうちどれですか？

- A. VPN tu
- B. vpn ipsec 削除 -l
- C. vpn デバッグ ipsec
- D. fw ipsec tu

Answer: ([解答を表示する](#))

解説 参考 :

説明: vpn tu

説明 VPN トンネルの制御に使用される TunnelUtil ツールを起動します。

使用法 vpn tu

vpn トンネルユーティリティ

例 vpn tu

出力

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_CLI_WebAdmin/12467.htm#o12627

最新問題: 150

SmartView Tracker を使用しているときに、Brady は非常に奇妙なネットワーク トラフィックに気付き、侵入の可能性があると考えています。彼は 60 分間トラフィックをブロックすることにしましたが、すべての手順を思い出せません。ブロックを設定するために必要な手順の正しい順序は？

- 1) SmartView Tracker で [アクティブ モード] タブを選択します。
- 2) [ツール] > [ブロック侵入者] を選択します。
- 3) SmartView Tracker で [ログ表示] タブを選択します。
- 4) ブロッキング タイムアウト値を 60 分に設定します。

5) ブロックする必要がある接続を強調表示します。

A. 1、2、5、4

B. 3、2、5、4

C. 1、5、2、4

D. 3、5、2、4

Answer: C ([メッセージを残す](#))

解説 参考 :

最新問題: 151

IT 管理チームは、Check Point R80 Management の新機能に関心があり、アップグレードを希望していますが、既存の R77.30 Gaia ゲートウェイは R80 とは大きく異なるため、R80 で管理できないことを懸念しています。ファイアウォールを担当する管理者として、これらの懸念にどのように答えたり確認したりできますか？

A. R80 Management には、R80 より前のバージョンの Check Point Gateway を管理するための互換性パッケージが含まれています。詳細については、R80 リリース ノートを参照してください。

B. R80 Management では、R80 より前のチェック ポイント ゲートウェイの以前のバージョンを管理するために、互換性修正プログラムパッケージを個別にインストールする必要があります。詳細については、R80 リリース ノートを参照してください。

C. R80 管理は、まったく異なる管理システムとして設計されているため、R80 より前のチェック ポイント ゲートウェイのみを監視できます。

D. R80 Management は、R80 より前の Check Point Gateway の以前のバージョンを管理できません。R80 以降のゲートウェイのみを管理できます。詳細については、R80 リリース ノートを参照してください。

Answer: A ([メッセージを残す](#))

説明

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 152

Gaia Platform のユーザーを最もよく表しているものを選択してください。

A. 削除できないデフォルト ユーザーが 1 つあります。

B. 2 つのデフォルト ユーザーがあり、1 つは削除できません。

C. 削除できるデフォルト ユーザーは 1 人です。

D. 削除できないデフォルト ユーザーが 2 人、SmartConsole Administrator が 1 人います。

Answer: B ([メッセージを残す](#))

解説 参考 :

Exlantion: これらのユーザーはデフォルトで作成され、削除できません:

admin - WebUI および CLI から、すべての Gaia 機能に対する完全な読み取り/書き込み機能を備えています。このユーザー

ユーザー ID が 0 であるため、root ユーザーのすべての権限を持っています。
モニター - WebUI および CLI のすべての機能に対して読み取り専用機能があり、その機能を変更できます。
自分のパスワード。アカウントを使用する前に、このユーザーのパスワードを指定する必要があります。
参考 https://sc1.checkpoint.com/documents/R76/CP_R76_Gaia_WebAdmin/73101.htm

最新問題: 153

あなたは Alpha Corp の管理者です。R80 管理サーバーにログインしています。あなたは
ルール ベースにいくつかの変更を加えると、ルール No.6 の横に鉛筆アイコンがあることに注意してください。
これは何を意味するのでしょうか？

- A. ルール No.6 は、管理セッションで削除対象としてマークされています。
- B. ルール No.6 は、別の管理セッションで削除対象としてマークされています。
- C. ルール No.6 は、別の管理セッションで編集するためにマークされています。
- D. ルール No.6 は、管理セッションで編集するようにマークされています。

Answer: D ([メッセージを残す](#))

最新問題: 154

クライアントは、リモート ロケーションで管理される新しいゲートウェイ オブジェクトを作成しました。クライアントがセキュリティ ポリシーを新しいゲートウェイ オブジェクトにインストールしようとする、オブジェクトが [インストール先] チェック ボックスに表示されません。
何を探すべきですか？

- A. セキュアな内部通信 (SIC) がオブジェクトに構成されていません。
- B. [ネットワーク オブジェクト] ダイアログ ボックスの [チェック ポイント] > [外部管理 VPN ゲートウェイ] オプションを使用して作成されたゲートウェイ オブジェクト。
- C. ゲートウェイ オブジェクトのインターフェイスでスプーフィング対策が構成されていません。
- D. [ネットワーク オブジェクト] ダイアログ ボックスの [Check Point] > [Secure Gateway] オプションを使用して作成された Gateway オブジェクトですが、Security Gateway オブジェクトのインターフェイスを設定する必要があります。

Answer: B ([メッセージを残す](#))

説明

最新問題: 155

TCP/IP モデルのトランスポート層は何を担当していますか？

- A. 2 つのホスト間のデータの流れを管理して、パケットが正しく組み立てられ、ターゲット アプリケーションに配信されるようにします。
- B. ネットワーク間でデータを交換するために使用されるプロトコルと、ホスト プログラムがアプリケーション層と対話する方法を定義します。
- C. パケットをデータグラムとしてさまざまなルートに沿って転送し、宛先に到達させます。
- D. ネットワーク接続の物理コンポーネントのすべての側面を処理し、さまざまなネットワーク タイプに接続します。

Answer: A ([メッセージを残す](#))

最新問題: 156

SmartConsole で 「ヒット カウント」機能を有効または無効にする場所はどこですか？

- A. ポリシー パッケージについて
- B. 各 Security Gateway で
- C. ポリシー層
- D. Security Management Server のグローバル プロパティ

Answer: B ([メッセージを残す](#))

解説 参考 https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

最新問題: 157

SmartConsole で 「ヒット カウント」機能を有効または無効にする場所はどこですか？

- A. Security Management Server のグローバル プロパティ
- B. ポリシー層
- C. ポリシーパッケージについて
- D. 各 Security Gateway で

Answer: D ([メッセージを残す](#))

最新問題: 158

サイト間 VPN 展開の最も重要な部分は _____ です。

- A. インターネット
- B. リモート ユーザー
- C. 暗号化された VPN トンネル
- D. VPN ゲートウェイ

Answer: ([解答を表示する](#)**)**

説明

サイト間 VPN

Site to Site VPN の基礎は、暗号化された VPN トンネルです。2 つの Security Gateway がリンクをネゴシエートし、VPN トンネルであり、各トンネルには複数の VPN 接続を含めることができます。1 つの Security Gateway で同時に複数の VPN トンネルを維持します。

最新問題: 159

_____ の場合を除き、次のすべての状況で新しいライセンスを生成してインストールする必要があります。

- A. ライセンスが間違った Security Gateway に添付されています
- B. 既存のライセンスの有効期限が切れます
- C. ライセンスがアップグレードされます
- D. Security Management または Security Gateway の IP アドレスが変更されました

Answer: A ([メッセージを残す](#))

この状況では、新しいライセンスを生成する必要はありません。ライセンスを間違った Security Gateway から切り離して、正しいゲートウェイに接続するだけで済みます。

最新問題: 160

次の図は、次のことを示しています。

- A. ソース アドレス 10.1.1.202 から開始されたログの SmartLog からの表示
- B. 宛先アドレス 10.1.1.202 のログの SmartView Tracker からの表示
- C. ソース アドレス 10.1.1.202 から開始されたログの SmartView Monitor からの表示
- D. ソース アドレス 10.1.1.202 から開始されたログの SmartView Tracker からの表示

Answer: D ([メッセージを残す](#))

最新問題: 161

SmartConsole に表示される 不明な SIC ステータスは何を意味しますか？

- A. SMS は Security Gateway に接続できますが、安全な内部通信を確立できません。
- B. SIC アクティベーション キーはリセットが必要です。
- C. SIC アクティベーション キーは、どの管理者にも知られていません。
- D. Security Gateway と SMS の間に接続がありません。

Answer: D ([メッセージを残す](#))

説明

最も一般的なステータスは通信中です。その他のステータスは、SIC 通信に問題があることを示しています。たとえば、SIC ステータスが不明の場合、ゲートウェイとセキュリティ管理サーバーの間に接続がありません。SIC ステータスが Not Communicating の場合、Security Management Server はゲートウェイに接続できますが、SIC 通信を確立できません。

最新問題: 162

各ゲートウェイのポリシーのインストール履歴を表示するには、管理者はどのツールを使用しますか？

- A. リビジョン
- B. ゲートウェイのインストール
- C. インストール履歴
- D. ゲートウェイ履歴

Answer: C ([メッセージを残す](#))

解説 参考 https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/119225

最新問題: 163

SmartDashboard にログインできません。管理サーバーにログインして #cpwd_admin list を実行すると、次の出力が表示されます。

SmartDashboard に接続できない理由を最もよく説明できる理由は何ですか？

- A. CDP がダウンしています
- B. SVR がダウンしています
- C. FWM がダウンしています
- D. CPSM がダウンしています

Answer: (解答を表示する)

解説 参考 :

正解は FWM (SmartConsole アプリケーションと Security Management Server 間の通信を可能にするプロセスです) です。STATE は T (Terminate = Down) です。

症状

SmartDashboard が Security Management サーバーに接続できません。

1. FWM プロセスが実行されているかどうかを確認します。これを行うには、次のコマンドを実行します。

[Expert@HostName:0]# ps -aux | grep fwm

2. FWM プロセスが実行されていない場合は、次のコマンドを使用してプロセスを強制的に開始してみてください。

[Expert@HostName:0]# cpwd_admin start -name FWM -path "\$FWDIR/bin/fwm" -command "fwm" 参照:

[https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638)

[https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk12120)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk12120](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk12120)

最新問題: 164

提示されたルールで、ExternalZone は何を表していますか？

- A. インターネットです。
- B. 管理者が外部セキュリティ ゾーンの一部として定義したインターフェイス。
- C. すべてのセキュリティ ゲートウェイの外部インターフェイス。
- D. 特定のゲートウェイの外部インターフェース。

Answer: ([解答を表示する](#))

解説 参考 :

Explanation:

インターフェイスの設定

「Security Gateway」ウィンドウの「Interfaces」タブで、Security Gateway 80 インターフェースを構成します。

インターフェイスを設定するには:

1. [デバイス] ウィンドウで、Security Gateway 80 をダブルクリックします。

[セキュリティ ゲートウェイ] ウィンドウが開きます。

2. [インターフェース] タブを選択します。

3. [次の設定を使用する] を選択します。インターフェイス設定が開きます。

4. インターフェイスを選択し、[編集] をクリックします。

編集ウィンドウが開きます。

5. [IP 割り当て] セクションで、インターフェイスの IP アドレスを構成します。

1. 静的 IP を選択します。

2. インターフェイスの IP アドレスとサブネット マスクを入力します。

6. [セキュリティ ゾーン] で、[ワイヤレス]、[DMS]、[外部]、または [内部] を選択します。セキュリティ ゾーンはゾーンの種類であり、IP アドレスとルーター構成を維持しながら、セグメントを簡単に作成するためにブリッジによって作成されます。セキュリティ ゾーンでは、セグメント間のファイアウォールを有効にするかどうかを選択できます。

参考 <https://sc1.checkpoint.com/documents/R76/>

CP_R76_SmartProvisioning_WebAdmin/16741.htm

最新問題: 165

MegaCorp のセキュリティ インフラストラクチャは、Security Gateway を地理的に分離しています。1 つのリモート Security Gateway の集中ライセンスを要求する必要があります。

どのようにライセンスを適用しますか？

- A. Gateway の各 IP アドレスを使用し、コマンド `cprlic put` を使用して Security Management Server にライセンスを適用します。
- B. Security Management Server の IP アドレスを使用し、ライセンスを SmartUpdate 経由でリモート ゲートウェイに接続します。
- C. リモート Gateway の IP アドレスを使用し、コマンド `cplic put` を使用してライセンスをローカルに適用します。
- D. リモート Gateway の IP アドレスを使用し、SmartUpdate を介してライセンスをリモート Gateway にアタッチします。

Answer: ([解答を表示する](#))

最新問題: 166

SandBlast には、攻撃をリアルタイムで防止するために連携する機能コンポーネントがいくつかあります。次のうち、SandBlast コンポーネントの一部でないものはどれですか？

- A. 脅威のエミュレーション
- B. モバイル アクセス
- C. メール転送エージェント
- D. 脅威の雲

Answer: ([解答を表示する](#))

解説 参考 <https://www.checkpoint.com/products-solutions/zero-day-protection/>

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 167

管理者 Kofi は、管理サーバーにいくつかの変更を加え、SmartConsole の [公開] ボタンをクリックしましたが、下のスクリーンショットに示すエラー メッセージが表示されました。

これらのエラーの詳細について、管理者はどこで確認できますか？

- A. SmartConsole の Log and Monitor セクション
- B. SmartConsole の検証セクション
- C. SmartConsole のオブジェクトセクション
- D. SmartConsole のポリシー セクション

Answer: ([解答を表示する](#))

説明

検証エラー

SmartConsole の検証ペインには、構成エラー メッセージが表示されます。エラーの例としては、固有でないオブジェクト名、およびルール ベースで無効なオブジェクトの使用があります。

発行するには、エラーを修正する必要があります。

参考文献:

最新問題: 168

Gateway をインストールしたばかりで、SmartView Monitor を使用してトラフィックのパケット サイズ分布を分析したいと考えています。

残念ながら、次のメッセージが表示されます。

Firewall Blade と SmartView Monitor を含むマシンはありません」。

トラフィックのパケット サイズ分布を分析するにはどうすればよいですか? 最高の答えを出してください。

A. Security Management Server の SmartView Monitor ライセンスを購入します。

B. Security Gateway の SmartView Monitor ライセンスを購入します。

C. Security Management Server で監視を有効にします。

D. Security Gateway でモニタリングを有効にします。

Answer: D (メッセージを残す)

最新問題: 169

空欄を埋めてください: ツール _____ は、R80 Security Gateway 構成レポートを生成します。

A. 情報CP

B. 情報ビュー

C. cpinfo

D. fw cpinfo

Answer: C (メッセージを残す)

CPInfo は、実行時に顧客のマシンで診断データを収集し、それをチェック ポイント サーバーにアップロードする自動更新可能なユーティリティです (ファイルをチェック ポイント サーバーにアップロードするためのスタンドアロンの cp_uploader ユーティリティを置き換えます)。

CPinfo 出力ファイルを使用すると、離れた場所から顧客のセットアップを分析できます。チェック ポイントのサポート エンジニアは、実際の顧客のセキュリティ ポリシーとオブジェクトを表示しながら、CPinfo ファイルをデモ モードで開くことができます。これにより、お客様の構成と環境設定を詳細に分析できます。

チェック ポイントのサポートに連絡する際は、ケースに関連する Security Management Server および Security Gateway から cpinfo ファイルを収集してください。

参照: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92739

最新問題: 170

契約ファイルをインストールするには、どのアプリケーションを使用する必要がありますか?

A. SmartView モニター

B. WebUI

C. SmartUpdate

D. SmartProvisioning

Answer: C ([メッセージを残す](#))

説明

SmartUpdate の使用: NGX R65 (またはそれ以降) の Security Management / Provider-1 / Multi-Domain Management Server を既に使用している場合、SmartUpdate を使用すると、手順 3 でダウンロードしたサービス契約ファイルをインポートできます。

SmartUpdate を開き、[Launch Menu] から [Licenses & Contracts] -> [Update Contracts] -> [From File...] を選択し、手順 3 でダウンロードしたファイルへのパスを指定します。

注: SmartUpdate がインターネットに接続されている場合は、ダウンロードおよびインポートの手順を実行しなくても、UserCenter からサービス契約ファイルを直接ダウンロードできます。

参考文献:

最新問題: 171

NAT エントリのトラブルシューティングに SmartView Tracker を使用しています。Source NAT を使用している場合、NAT された送信元ポートを確認するためにどの列をチェックしますか?

- A. XlateDst
- B. XlateDPort
- C. XlateSPort
- D. XlateSrc

Answer: C ([メッセージを残す](#))

最新問題: 172

パッケージとライセンスは、これらのソースを除くすべてからロードされます

- A. ダウンロード センター Web サイト
- B. ユーザーアップデート
- C. ユーザーセンター
- D. チェックポイント DVD

Answer: B ([メッセージを残す](#))

解説 参考 :

Explanation:

パッケージとライセンスは、いくつかのソースからこれらのリポジトリにロードされます。

- * ダウンロード センター Web サイト (パッケージ)
- * チェックポイント DVD (パッケージ)
- * ユーザー センター (ライセンス)
- * ファイル (パッケージとライセンス) をインポートすることによって
- * cplic コマンド ラインを実行する

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide-webAdmin/13128.htm

最新問題: 173

メッシュとスターは、2 種類の VPN トポロジです。これらのタイプのコミュニティについて正しいのは次のうちどれですか?

- A. メッシュ コミュニティでは、メンバー ゲートウェイは互いに直接通信できません。

- B. スター コミュニティには、チェック ポイント独自のテクノロジーであるため、チェック ポイントのゲートウェイが必要です。
- C. スター コミュニティでは、サテライト ゲートウェイは相互に通信できません。
- D. メッシュ コミュニティでは、すべてのメンバーが他のメンバーとの間でトンネルを作成できます。

Answer: D ([メッセージを残す](#))

最新問題: 174

以下のルールをご覧ください。左の列のロック記号は何を意味していますか？

- A. 現在の管理者には、脅威対策ポリシーへの読み取り専用権限があります。
- B. 別のユーザーがルールを編集のためにロックしています。
- C. 構成ロックが存在します。ロック記号をクリックして、読み取り/書き込みアクセスを取得します。
- D. 他の誰かがポリシーを編集しているため、現在の管理者は読み取り専用としてログインしています。

Answer: B ([メッセージを残す](#))

管理者のコラボレーション

複数の管理者が同時に Security Management Server に接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。

管理者が SmartConsole を介して Security Management Server にログインすると、新しい編集セッションが開始されます。セッション中に管理者が行った変更は、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールにロック アイコンが表示されます。

すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルールのロックを解除するには、管理者はセッションを公開する必要があります。

参照: [https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?](https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265)

[topic=documents/R80/CP_R80_SecMGMT/124265](https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/124265)

最新問題: 175

空白を埋める: トンネル テスト パケットが応答を呼び出さなくなった場合、SmartView Monitor は次のように表示します。

指定された VPN トンネルの _____。

- A. 下
- B. 失敗
- C. 無反応
- D. 非アクティブ

Answer: A ([メッセージを残す](#))

最新問題: 176

RADIUS プロトコルは、_____ を使用してゲートウェイと通信します。

- A. UDP
- B. TDP
- C. CCP
- D. HTTP

Answer: (解答を表示する)

説明

パラメーター：

最新問題: 177

レイヤーを編集するために、選択した管理者の権限を定義したいと考えています。ただし、このレイヤーを編集できる追加のプロファイルを選択してください」の + 記号をクリックすると、何も表示されません。この問題の最も可能性の高い原因は何ですか？ ベストアンサーを選択してください。

- A. 使用できるアクセス許可プロファイルはありません。最初に作成する必要があります。
- B. 権限プロファイルで Software Blade ごとにレイヤーを編集する」が選択されていない
- C. すべての権限プロファイルが使用中です。
- D. [レイヤー エディターで選択したプロファイルでレイヤーを編集する] が、アクセス許可プロファイルで選択されていません。

Answer: A ([メッセージを残す](#))

最新問題: 178

Gateway をインストールしたばかりで、SmartView Monitor を使用してトラフィックのパケット サイズ分布を分析したいと考えています。

残念ながら、次のメッセージが表示されます。

Firewall Blade と SmartView Monitor を含むマシンはありません」。

トラフィックのパケット サイズ分布を分析するにはどうすればよいですか？ 最高の答えを出してください。

- A. Security Gateway の SmartView Monitor ライセンスを購入します。
- B. Security Management Server の SmartView Monitor ライセンスを購入します。
- C. Security Management Server で監視を有効にします。
- D. Security Gateway でモニタリングを有効にします。

Answer: D ([メッセージを残す](#))

最新問題: 179

オフィス モードとは、次のことを意味します。

- A. SecureID クライアントはルーティング可能な MAC アドレスを割り当てます。ユーザーがトンネルに対して認証されると、VPN ゲートウェイはルーティング可能な IP アドレスをリモート クライアントに割り当てます。
- B. ユーザーはインターネット ブラウザで認証し、安全な HTTPS 接続を使用します。
- C. ローカル ISP (インターネット サービス プロバイダー) は、ルーティング不可能な IP アドレスをリモート ユーザーに割り当てます。
- D. セキュリティ ゲートウェイがリモート クライアントに IP アドレスを割り当ててることを許可します。ユーザーがトンネルに対して認証されると、VPN ゲートウェイはルーティング可能な IP アドレスをリモート クライアントに割り当てます。

Answer: D ([メッセージを残す](#))

オフィス モードでは、Security Gateway が内部 IP アドレスを SecureClient ユーザーに割り当てることができます。この IP アドレスはパブリック ネットワークには公開されませんが、クライアントとゲートウェイの間の VPN トンネル内にカプセル化されます。外部で使用する IP は、インターネット接続に使用されるインターネット サービス プロバイダーによって、通常の方法でクライアントに割り当てられる必要があります。このモードでは、セキュリティ管理者は、ローカル ネットワーク内のリモート クライアントが使用するアドレスを制御し、それらをローカル ネットワークの一部にすることができます。このメカニズムは、Security Gateway が内部 IP アドレスをクライアントに送信できる IKE プロトコル拡張に基づいています。

参考 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk30545

最新問題: 180

あるコミュニティの VPN ゲートウェイへのトラフィックのみに一致して許可するファイアウォール ルールのオプションはどれですか？
一般？

- A. すべての暗号化されたトラフィックを受け入れる
- B. すべてのサイト間 VPN コミュニティ
- C. すべての接続 (クリアまたは暗号化)
- D. 特定の VPN コミュニティ

Answer: D ([メッセージを残す](#))

最新問題: 181

GAiA を使用する場合、インターフェース eth0 の MAC アドレスを一時的に 00:0C:29:12:34:56 に変更する必要がある場合があります。ネットワークを再起動すると、古い MAC アドレスがアクティブになります。この変更をどのように構成しますか？

- A. WebUI を開き、[ネットワーク] > [接続] > [eth0] を選択します。[物理アドレス] フィールドに新しい MAC アドレスを入力し、[適用] を押して設定を保存します。
- B. ファイル /etc/sysconfig/netconf.C を編集し、フィールド (conf:(conns:(conn:hwaddr ("00:0C:2 :12:34:56"))) に新しい MAC アドレスを入力します。
- C. エキスパート ユーザーとして、次のコマンドを発行します。# IP link set eth0 down# IP link set eth0 addr 00:0C:29:12:34:56# IP link set eth0 up
- D. エキスパート ユーザーとして、次のコマンドを発行します: # IP link set eth0 addr 00:0C:29:12:34:56

Answer: D ([メッセージを残す](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 182

このセキュリティ ポリシーを確認する際に、ルール 4 に対応するためにどのような変更を加えることができますか？

- A. 何もない
- B. ルール 4 の列のサービスからサービス HTTP を削除します。
- C. ルール 4 の送信元または宛先の列を変更します。
- D. ルール 2 の列 VPN を変更して、特定のトラフィックへのアクセスを制限します。

Answer: D ([メッセージを残す](#))

最新問題: 183

空欄を埋めてください: R80 機能 _____ は、指定された期間、特定の IP アドレスをブロックすることを許可します。

- A. ブロック ポート オーバーフロー
- B. ローカル インターフェイス スプーフィング
- C. 不審なアクティビティの監視
- D. 適応型脅威対策

Answer: ([解答を表示する](#))

疑わしいアクティビティ ルール ソリューション疑わしいアクティビティ ルールは、SmartView Monitor は、疑わしいネットワーク アクティビティ (複数回の不正アクセスの試行など) が検出されたときにアクセス権限を変更するために使用されます。

疑わしいアクティビティの検出は、疑わしいアクティビティ ルールの作成に基づいています。

疑わしいアクティビティ ルールは、システム管理者が、現在適用されているセキュリティ ポリシーによって制限されていない疑わしい接続を即座にブロックできるようにするファイアウォール ルールです。これらのルールは、一度設定すると (通常は有効期限付き)、ポリシーのインストール操作を実行する必要なく、すぐに適用できます。

最新問題: 184

オペレーティング システム情報やリソース使用状況などのセキュリティ ゲートウェイの一般的なシステム情報の統計情報と、VPN、ID 認識、DLP の個々のソフトウェア ブレードの統計情報を表示するユーティリティはどれですか？

- A. cpconfig
- B. fw ctl pstat
- C. cpview
- D. fw ctl multik stat

Answer: C ([メッセージを残す](#))

CPView ユーティリティは、Security Gateway / Security Management Server / Multi-Domain Security Management Server で実行できる (「cpview」コマンド) テキスト ベースの組み込みユーティリティです。CPView ユーティリティは、一般的なシステム情報 (CPU、メモリ、ディスク容量) とさまざまなソフトウェア ブレードの情報 (Security Gateway のみ) の両方を含む統計データを表示します。データは、アクセスしやすいビューで継続的に更新されます。

最新問題: 185

R80.10 コードの一部として現在利用可能な Check Point API のタイプは何ですか？

- A. Security Gateway API、Management API、Threat Prevention API、Identity Awareness Web Services API
- B. Management API、Threat Prevention API、Identity Awareness Web Services API、OPSEC SDK API
- C. OSE API、OPSEC SDK API、脅威対策 API、ポリシー エディター API
- D. CPMI API、管理 API、脅威対策 API、ID 認識 Web サービス API

Answer: B ([メッセージを残す](#))

参照 :

<http://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/>

CP_R80_CheckPoint_API_ReferenceGuide.pdf?

HashKey=1517088487_4c0acda205460a92f44c83d399826a7b&xtn=.pdf

最新問題: 186

サイト間 VPN 展開の最も重要な部分は _____ です。

- A. インターネット
- B. リモート ユーザー
- C. 暗号化された VPN トンネル
- D. VPN ゲートウェイ

Answer: C ([メッセージを残す](#))

説明

サイト間 VPN

Site to Site VPN の基礎は、暗号化された VPN トンネルです。2 つの Security Gateway がリンクをネゴシエートして VPN トンネルを作成します。各トンネルには複数の VPN 接続を含めることができます。1 つの Security Gateway で同時に複数の VPN トンネルを維持できます。

最新問題: 187

機密性の高いサーバーに対してより高いレベルのセキュリティが必要な場合、Identity Awareness でどの ID ソースを選択する必要がありますか？

- A. AD クエリ
- B. ターミナル サーバー エンドポイント アイデンティティ エージェント
- C. Endpoint Identity Agent とブラウザベースの認証
- D. RADIUS とアカウント ログオン

Answer: C ([メッセージを残す](#))

Endpoint Identity Agents とブラウザベースの認証 - 高レベルのセキュリティが必要な場合。キャプティブ ポータルは、Endpoint Identity Agent の配布に使用されます。IP スプーフィング保護を設定して、パケットが IP スプーフィングされるのを防ぐことができます。

参照：

[https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/](https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/101858)

[CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?](https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/101858)

[topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/101858](https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm?topic=documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/101858)

最新問題: 188

次の図は、次のことを示しています。

- A. ソース アドレス 10.1.1.202 から開始されたログの SmartView Monitor からの表示
- B. 宛先アドレス 10.1.1.202 のログの SmartView Tracker からの表示
- C. ソース アドレス 10.1.1.202 から開始されたログの SmartLog からの表示
- D. ソース アドレス 10.1.1.202 から開始されたログの SmartView Tracker からの表示

Answer: ([解答を表示する](#))

最新問題: 189

Gaia オペレーティング システムは、どのルーティング プロトコルをサポートしていますか？

- A. BGP、OSPF、RIP
- B. BGP、OSPF、EIGRP、PIM、IGMP
- C. BGP、OSPF、RIP、PIM、IGMP

D. BGP、OSPF、RIP、EIGRP

Answer: A (メッセージを残す)

高度なルーティングスイート

Advanced Routing Suite CLI は、Advanced Networking Software Blade の一部として利用できます。

スケーラブルでフォールトトレラントな安全なネットワークの実装を検討している組織は、Advanced Networking ブレードを使用して、セキュリティゲートウェイで BGP、OSPF、RIPv1、RIPv2 などの業界標準の動的ルーティングプロトコルを実行できます。OSPF、RIPv1、および RIPv2 は、ネットワーク障害を回避するために、単一の部門、会社、またはサービスプロバイダーなどの単一の自律システムを介した動的ルーティングを有効にします。BGP は、企業が 2 つのサービスプロバイダーを使用する場合や、ネットワークを複数のエリアに分割し、異なる管理者がそれぞれのパフォーマンスを担当する場合など、複数の自律システムを含むより複雑なネットワーク全体でダイナミックルーティングサポートを提供します。

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_SecurePlatform_AdvancedRouting_WebAdmin/html_frameset.htm

最新問題: 190

ジャックはマネージドサービスプロバイダーで働いており、いくつかの新しいサービスに対して 17 の新しいポリシーを作成する任務を負っています。

顧客。彼にはあまり時間がありません。R80 セキュリティ管理でこれを行う最善の方法は何か？

- A. すべてのオブジェクトとポリシーを作成する mgmt_cli スクリプトを含むテキストファイルを作成します。でファイルを開きますそれを実行する SmartConsole コマンドライン。
- B. すべてのオブジェクトとポリシーを作成するために、Gaia CLI コマンドでテキストファイルを作成します。ファイルを実行しますコマンドロード構成を使用した CLISH。
- C. すべてのオブジェクトとポリシーを作成する DBEDIT スクリプトでテキストファイルを作成します。コマンドでファイルを実行します
コマンド dbedit -f を使用して、管理サーバーの行を編集します。
- D. SmartConsole でオブジェクトエクスプローラーを使用してオブジェクトを作成し、メニューからポリシーを管理して作成します。ポリシー。

Answer: A (メッセージを残す)

説明

ご存知でしたか: mgmt_cli は、--batch オプションを使用して csv ファイルを入力として受け入れることができます。

最初の行には引数名が含まれ、その下の行にはこれらの値が含まれている必要があります
パラメーター。

したがって、powershell スクリプトの同等のソリューションは次のようになります。

データ.csv:

```
mgmt_cli add host --batch data.csv -u <ユーザー名> -p <パスワード> -m <管理サーバー>
```

これは、「ホストの追加」だけでなく、任意のタイプのコマンドで機能します。列名を次のものに置き換えるだけです。

必要なコマンドに関連します。

最新問題: 191

アクセスコントロールポリシーレイヤーを構成する 2 つの順序付けられたレイヤーはどれですか？

- A. ネットワークと脅威対策

- B. ネットワークおよびアプリケーション制御
- C. アプリケーション制御と URL フィルタリング
- D. URL フィルタリングとネットワーク

Answer: C ([メッセージを残す](#))

最新問題: 192

空欄を埋めてください: _____ は、VPN ゲートウェイが物理インターフェイスであるかのようにトラフィックを送信するために使用されます。

- A. VPN トンネル インターフェイス
- B. VPN コミュニティ
- C. VPN ルーター
- D. VPN インターフェース

Answer: ([解答を表示する](#))

解説 参考 :

Explanation:

ルートベース VPN

VPN トラフィックは、Security Gateway オペレーティング システムのルーティング設定 (静的または動的) に従ってルーティングされます。Security Gateway は、VTI (VPN トンネル インターフェース) を使用して、物理インターフェースであるかのように VPN トラフィックを送信します。VPN コミュニティ内の Security Gateway の VTI は接続し、ダイナミック ルーティング プロトコルをサポートできます。

参照: http://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13868.htm

最新問題: 193

次のうち、SmartConsole で作成されたアカウントに使用される認証方式ではないものはどれですか？

- A. セキュリティの質問
- B. チェックポイントのパスワード
- C. SecurID
- D. 半径

Answer: A ([メッセージを残す](#))

認証方式 :- チェック ポイントのパスワード

- オペレーティング システムのパスワード

- ラディウス

- SecurID

- タカス

- 未定義 未定義の認証スキームを持つユーザーが、何らかの形式の認証を持つセキュリティ ルールに一致する場合、アクセスは常に拒否されます。

最新問題: 194

Tina は新しい管理者で、現在新しい Check Point R80 管理コンソール インターフェイスをレビューしています。ゲートウェイ ビューで、彼女は下のスクリーンショットのように [概要] 画面を確認しています。何として

「オープンサーバー」？

- A. チェック ポイント以外のアプライアンスに導入されたチェック ポイントのソフトウェア。
- B. Open Server Consortium が承認した、セキュリティと可用性の目的で使用するサーバー ハードウェア。
- C. Open Systems Interconnection (OSI) サーバーおよびセキュリティ展開モデルを使用して展開されたチェック ポイント管理サーバー。
- D. Open SSL を使用するチェック ポイント管理サーバー ソフトウェア。

Answer: ([解答を表示する](#))

説明

参考文献:

最新問題: 195

Tom は、Check Point R80 を分散展開にインストールする任務を負っています。トムがこの方法でシステムをインストールする前に、計算に SmartConsole マシンを含めない場合、何台のマシンが必要になるのでしょうか？

- A. 1 台のマシンですが、互換性のために SecurePlatform を使用してインストールする必要があります。
- B. 1台
- C. 2 台のマシン
- D. 3 台のマシン

Answer: C ([メッセージを残す](#))

解説 参考 :

説明: 1 つは Security Management Server 用で、もう 1 つは Security Gateway 用です。

最新問題: 196

複数の LDAP サーバーを使用する利点ではないのは、次のうちどれですか？

- A. ユーザーに関する情報は隠蔽されていますが、複数のサーバーに分散されています
- B. データベースを含む LDAP サーバーをリモート サイトに配置することで、アクセス時間を短縮できます。
- C. 多数のユーザーを複数のユーザーに分散できるようにすることで、区分化を実現します。
サーバー
- D. 同じ情報を複数のサーバーに複製することで、高可用性を実現します。

Answer: A ([メッセージを残す](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 197

空欄に記入してください: A(n) _____ ルールは管理者によって作成され、ルール ベース内の最初と最後のルールの前に配置されます。

- A. ファイアウォール ドロップ
- B. 明示的
- C. 暗黙の受け入れ

D. 暗黙のドロップ

E. 暗示

Answer:

ルールが適用される順序は次のとおりです。

最新問題: 198

アプリケーションとサーバーの脆弱性に焦点を当て、悪意のあるネットワーク トラフィックと不要なネットワーク トラフィックに対して包括的な機能を提供する Threat Prevention Software Blade はどれですか？

A. ウイルス対策

B. IPS

C. アンチスパム

D. アンチボット

Answer: B ([メッセージを残す](#))

IPS Software Blade は完全な侵入防御システム セキュリティ ソリューションを提供し、次のような悪意のあるネットワーク トラフィックや不要なネットワーク トラフィックに対する包括的なネットワーク保護を提供します。

最新問題: 199

VRRP におけるプライオリティ デルタの目的は何ですか？

A. ボックスが稼働中の場合、実効優先度 = 優先度 + 優先度デルタ

B. インターフェイスがアップしている場合、有効な優先度 = 優先度 + 優先度デルタ

C. インターフェイスに障害が発生した場合、実効優先度 = 優先度 - 優先度デルタ

D. ボックスが失敗した場合、実効優先度 = 優先度 - 優先度デルタ

Answer: ([解答を表示する](#))

説明

参考文献:

最新問題: 200

統合ポリシーとは何ですか？

A. SmartReporter データベースに保存されるログ データを構成するために SmartDashboard に記述された特定のポリシー。

B. セキュリティ ポリシー、アドレス変換、および IPS ポリシーの総称。

C. 複数のセキュリティに対して共通の施行ポリシーを共有するために使用されるグローバル ポリシー
ゲートウェイ。

D. SmartReporter によって生成されたログの総称。

Answer: A ([メッセージを残す](#))

最新問題: 201

ハッシュアルゴリズムは次のうちどれですか？

A. 3DES

B. アイデア

C. DES

D. MD5

Answer: D ([メッセージを残す](#))

最新問題: 202

すべての構成を変更せずに監査するための完全なアクセス権を必要とする管理者に割り当てる必要がある事前定義済みのアクセス許可プロファイルはどれですか？

A. 審査員

B. すべて読み取り専用

C. スーパーユーザー

D. フルアクセス

Answer: ([解答を表示する](#))

新しい権限プロファイルを作成するには:

[新しいプロファイル] ウィンドウが開きます。

最新問題: 203

ルール ベースとクライアント認証アクションのプロパティ画面を調べます。

Security Gateway によって認証された後、ユーザーは HTTP 接続を開始します。

Webサイト。ユーザーがコマンドラインを使用して別のサイトに FTP で接続しようとするとなりますか？ :

A. ユーザーが正常に認証された後、FTP データ接続が切断されます。

B. FTP 接続はルール 2 によってドロップされます。

C. ユーザーはその FTP サイトからのみ認証するように求められ、クライアント認証のためにユーザー名とパスワードを入力する必要はありません。

D. ユーザーは Security Gateway によって再度認証を求められます。

Answer: C ([メッセージを残す](#))

最新問題: 204

ユーザーの身元がわかっている場合はどうなりますか？

A. ユーザー資格情報がアクセス ロールと一致しない場合、システムはサンドボックスを表示します。

B. ユーザー資格情報がアクセス ロールと一致しない場合、トラフィックは自動的にドロップされます。

C. ユーザー資格情報がアクセス ロールと一致する場合、ルールが適用され、定義されたアクションに基づいてトラフィックが受け入れられるかドロップされます。

D. ユーザー資格情報がアクセス ロールと一致しない場合、システムはキャプティブを表示します。

ポータル。

Answer: ([解答を表示する](#))

最新問題: 205

ルール ベースとクライアント認証アクションのプロパティ画面を調べます。

Security Gateway によって認証された後、ユーザーは Web サイトへの HTTP 接続を開始します。ユーザーがコマンドラインを使用して別のサイトに FTP で接続しようとするとなりますか？ :

- A. ユーザーはその FTP サイトからのみ認証するように求められ、クライアント認証のためにユーザー名とパスワードを入力する必要はありません。
- B. ユーザーが正常に認証された後、FTP データ接続が切断されます。
- C. ユーザーは Security Gateway によって再度認証を求められます。
- D. FTP 接続はルール 2 によってドロップされます。

Answer: ([解答を表示する](#))

最新問題: 206

次のうち、追跡オプションでないものはどれですか? (3つ選択)

- A. 部分ログ
- B. ネットワークログ
- C. ログ
- D. フルログ

Answer: A,B,D ([メッセージを残す](#))

最新問題: 207

デフォルトで R80 管理に含まれていない脅威対策プロファイルはどれですか?

- A. 基本 - ネットワーク パフォーマンスへの影響を最小限に抑えながら、さまざまな非 HTTP プロトコルで信頼性の高い保護をサーバーに提供します。
- B. 最適化 - 最近または一般的な攻撃に対して、一般的なネットワーク製品およびプロトコルに優れた保護を提供します。
- C. Strict - すべての製品とプロトコルを幅広くカバーし、ネットワーク パフォーマンスに影響を与えます。
- D. 推奨 - すべての一般的なネットワーク製品とサーバーにすべての保護を提供し、ネットワーク パフォーマンスに影響を与えます。

Answer: D ([メッセージを残す](#))

解説 参考:

参照: https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486

最新問題: 208

差分同期について正しくない文はどれですか?

- A. ポート 8161 で UDP マルチキャストまたはブロードキャストを使用する
- B. クラスタ メンバー間でカーネル テーブルの変更を転送します。
- C. 完全同期より速い
- D. ポート 8116 で UDP マルチキャストまたはブロードキャストを使用する

Answer: A ([メッセージを残す](#))

最新問題: 209

Security Gateway の CPU 負荷が高いため、セキュリティ管理者は新しい

マルチコア CPU を使用して、既存のシングル コア CPU を置き換えます。インストール後、管理者は次のことを行う必要がありますか? 追加のタスクを実行しますか?

- A. clash-Run cpconfig に移動 | 追加のコアを利用するように CoreXL を構成します。cpconfig を終了します。

Security Gateway を再起動します

B. clash-Run cpconfig | 追加のコアを利用するように CoreXL を構成します。cpconfig を終了します。

Security Gateway | を再起動します。セキュリティ ポリシーをインストールする

C. 管理者がタスクを実行する必要はありません。Check Point は、新しく取り付けられた CPU を利用します。
とコア

D. clash-Run cpstop に移動 | cpstart を実行します

Answer: A ([メッセージを残す](#))

最新問題: 210

空欄に記入してください。Security Management Server によって証明書が Security Gateway から取り消されると、証明書情報は _____ になります。

A. 証明書失効リストに格納されます。

B. 内部認証局に送信されます。

C. Security Management Server に保存されます。

D. セキュリティ管理者に送信されます。

Answer: A ([メッセージを残す](#))

最新問題: 211

クラスター メンバーのフェイルオーバーはどこでトリガーできますか？

Security Gateway CLI にログインし、コマンド clusterXL_admin down を実行します。

SmartView Monitor で、Security Gateway メンバーを右クリックし、[Cluster member stop] を選択します。

Security Gateway CLI にログインし、コマンド cphaprob down を実行します。

A. 1、2、および 3

B. 2 と 3

C. 1 と 2

D. 1 と 3

Answer: C ([メッセージを残す](#))

FailoverMethod を開始する方法

ClusterXL を停止するには

ClusterXL を起動するには

走る :

と :

効果 :

効果 :

推奨される方法:

走る :

SmartView モニター:

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 212

次のうち、暗号化するのと同じ鍵を復号化に使用するのはいずれですか？

- A. 証明書ベースの暗号化
- B. 動的暗号化
- C. 対称暗号化
- D. 非対称暗号化

Answer: C ([メッセージを残す](#))

最新問題: 213

2 つの高可用性モードとは何ですか？

- A. 負荷分散とレガシー
- B. トラディショナルとニュー
- C. アクティブおよびスタンバイ
- D. 新規およびレガシー

Answer: ([解答を表示する](#)**)**

解説 参考：

説明: ClusterXL には 4 つの動作モードがあります。このセクションでは、各モードとその相対的な長所と短所について簡単に説明します。

負荷分散マルチキャスト モード

負荷分散ユニキャスト モード

新しい高可用性モード

高可用性レガシー モード

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm#o7363

最新問題: 214

John は、R77.30 Check Point Security Gateway を管理する R80 Security Management サーバーの管理者です。John は現在、SmartConsole を使用してネットワーク オブジェクトを更新し、ルールを修正しています。John の変更を他の管理者が利用できるようにし、ポリシーをインストールする前にデータベースを保存するには、John は何をする必要がありますか？

- A. セッションのログアウト
- B. ファイル > 保存
- C. データベースのインストール
- D. セッションを公開する

Answer: D ([メッセージを残す](#))

説明

インストールと発行

公開とインストールの違いを理解することが重要です。

これを行う必要があります：

これを行った後：

公開

SmartConsole でセッションを開き、変更を加えました。

発行操作は、SmartConsole のすべての変更を他の管理者に送信し、プライベート セッションで行った変更を公開します。

データベースをインストールする

サーバー、ユーザー、サービス、または IPS プロファイルなどの変更されたネットワーク オブジェクト。ただし、Rule Base は対象外です。

更新プログラムは、管理サーバーとログ サーバーにインストールされます。

ポリシーをインストールする

ルールベースを変更しました。

Security Management Server は、更新されたポリシーとデータベース全体を Security Gateway にインストールします (ネットワーク オブジェクトを変更していない場合でも)。

最新問題: 215

次のうち、アクセス ロール オブジェクトによって定義されていないものはどれですか？

- A. ソース ネットワーク
- B. ソース マシン
- C. ソース ユーザー
- D. ソース サーバー

Answer: ([解答を表示する](#))

解説 参考：

最新問題: 216

次のうち、Identity Awareness が ID を取得するために使用する方法でないものはどれですか？

- A. 半径
- B. 証明書
- C. Active Directory クエリ
- D. リモートアクセス

Answer: B ([メッセージを残す](#))

最新問題: 217

2 種類のアドレス変換規則とは？

- A. 翻訳済みパケットと未翻訳パケット
- B. 未翻訳のパケットと操作されたパケット
- C. 操作されたパケットと元のパケット
- D. 元のパケットと変換されたパケット

Answer: D ([メッセージを残す](#))

説明

NAT ルール ベース

NAT ルール ベースには、IP アドレスの変換方法を指定する 2 つのセクションがあります。

元のパケット

翻訳済みパケット

参考文献:

最新問題: 218

IKE によって実行される 2 フェーズ ネゴシエーション プロセスのフェーズ 1 は、_____ モードで動作します。

A. クイック

B. 高警報

C. 認証

D. メイン

Answer: D ([メッセージを残す](#))

最新問題: 219

Harriet は、ユーザーが特定の URL を参照したときに機密情報が意図的に失われないように保護したいと考えています。

https://personal.mymail.com、彼女は目標を達成するためにどのブレードを有効にしますか？

A. DLP

B. SSL インспекション

C. アプリケーション制御

D. URL フィルタリング

Answer: A ([メッセージを残す](#))

チェック・ポイントは、テクノロジーとプロセスを組み合わせることで DLP に革命をもたらし、ビジネスを受動的な検出から能動的なデータ損失防止に移行させます。革新的な MultiSpect データ分類は、ユーザー、コンテンツ、およびプロセス情報を組み合わせて正確な決定を行い、UserCheck テクノロジーにより、ユーザーはインシデントをリアルタイムで修復できます。チェック・ポイントのネットワークベースの自己教育型 DLP ソリューションは、IT/セキュリティ担当者をインシデント処理から解放し、適切なデータ処理ポリシーについてユーザーを教育し、企業の機密情報を意図的および意図的でない損失から保護します。

参考 <https://www.checkpoint.com/downloads/product-related/datasheets/DLP-software-blade-datasheet.pdf>

最新問題: 220

Joey は、R80 Security Management Server で NTP を構成したいと考えています。彼はこれを WebUI で行うことにしました。ブラウザ経由で Gaia プラットフォームの Web UI にアクセスするための正しいアドレスは？

A. https://<デバイス_IP_アドレス>

B. https://<デバイス_IP_アドレス>:443

C. https://<デバイス_IP_アドレス>:10000

D. https://<デバイス_IP_アドレス>:4434

Answer: ([解答を表示する](#))

説明

Web UI Gaia 管理インターフェースにアクセスし、ブラウザーからデフォルトの管理 IP アドレスへの接続を開始します。WebUI へのログイン ログイン WebUI にログインするには:
https://<ガイアIPアドレス>

最新問題: 221

空欄に記入してください。LDAP が Check Point Security Management と統合されている場合、LDAP は _____ と呼ばれます。

- A. ユーザーチェック
- B. ユーザー ディレクトリ
- C. ユーザー管理
- D. ユーザーセンター

Answer: ([解答を表示する](#))

Check Point User Directory は、LDAP およびその他の外部ユーザー管理テクノロジーを Check Point ソリューションと統合します。ユーザー数が多い場合は、Security Management Server のパフォーマンスを向上させるために、LDAP などの外部ユーザー管理データベースを使用することをお勧めします。

最新問題: 222

R77 の内部認証局として機能するコンポーネントはどれですか?

- A. 管理サーバー
- B. SmartLSM
- C. ポリシー サーバー
- D. セキュリティ ゲートウェイ

Answer: A ([メッセージを残す](#))

最新問題: 223

Gaia は _____ または _____ を使用して設定できます。

- A. GaiaUI; コマンド ライン インターフェイス
- B. WebUI; ガイアインターフェース
- C. コマンド ライン インターフェイス。WebUI
- D. ガイア インターフェイス; GaiaUI

Answer: C ([メッセージを残す](#))

説明

初めて Gaia を設定する

このセクションで :

WebUI での初回構成ウィザードの実行

CLI での初回構成ウィザードの実行

初めて Gaia をインストールした後、First Time Configuration Wizard を使用して、システムとそのシステム上の Check Point 製品を構成します。

最新問題: 224

Harriet は、ユーザーが特定の URL を参照したときに機密情報が意図的に失われないように保護したいと考えています。

https://personal.mymail.com、彼女は目標を達成するためにどのブレードを有効にしますか？

- A. DLP
- B. SSL インспекション
- C. アプリケーション制御
- D. URL フィルタリング

Answer: A ([メッセージを残す](#))

説明

チェック・ポイントは、テクノロジーとプロセスを組み合わせることで DLP に革命をもたらし、ビジネスを受動的な検出から能動的なデータ損失防止に移行させます。革新的な MultiSpect データ分類は、ユーザー、コンテンツ、およびプロセス情報を組み合わせて正確な決定を行い、UserCheck テクノロジーにより、ユーザーはインシデントをリアルタイムで修復できます。チェック・ポイントのネットワークベースの自己教育型 DLP ソリューションは、IT/セキュリティ担当者をインシデント処理から解放し、適切なデータ処理ポリシーについてユーザーを教育し、企業の機密情報を意図的および意図的でない損失から保護します。

参考文献:

最新問題: 225

空欄に記入してください: R80 ユーティリティ ファームウェア モニターは、トラブルシューティングに使用されます _____

- A. ユーザー データベースの破損
- B. LDAP の競合
- C. トラフィックの問題
- D. フェーズ 2 のキー ネゴシエーション

Answer: ([解答を表示する](#))

Check Point の FW Monitor は、ネットワーク トラフィックをパケット レベルでキャプチャするための強力な組み込みツールです。FW Monitor ユーティリティは、FireWall インспекション チェーンに沿った複数のキャプチャ ポイントでネットワーク パケットをキャプチャします。これらのキャプチャされたパケットは、後で WireShark を使用して検査できます。

最新問題: 226

次の図では、管理者が Identity Awareness を構成しています。

[次へ] をクリックした後、上記の構成は以下でサポートされます。

- A. Active Directory 統合のために機能する Kerberos SSO
- B. Active Directory 統合に基づいており、Security Gateway は、ユーザーに対して完全に透過的な方法で、Active Directory ユーザーとマシンを IP アドレスに関連付けることができます。
- C. キャプティブポータルの使用義務
- D. ポート 443 または 80 は、ブラウザーベースの構成済み認証で使用されます。

Answer: B ([メッセージを残す](#))

説明

ID 認識を有効にするには:

- * R80 SmartConsole にログインします。
- * Gateways & Servers ビューで、Identity Awareness を有効にする Security Gateway をダブルクリックします。
- * [ネットワーク セキュリティ] タブで、Identity Awareness 設定ウィザードが開きます。

- * 1 つまたは複数のオプションを選択します。これらのオプションは、管理対象アセットと管理対象外アセットの ID を取得する方法を設定します。
- * AD Query - Security Gateway が Active Directory ユーザーとコンピュータをシームレスに識別できるようにします。
- * ブラウザベースの認証 - ユーザーを Web ページに送り、未確認のユーザーから ID を取得します。透過的な Kerberos 認証が構成されている場合、AD ユーザーは透過的に識別されます。
- * ターミナル サーバー - ターミナル サーバー環境でユーザーを識別します (1 つの IP アドレスから発信されます)。

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **227**

セッションの一意の識別子は、どの http ヘッダー オプションを使用して Web API に渡されますか？

- A. X-chkp-sid
- B. Accept-Charset
- C. アプリケーション
- D. プロキシ承認

Answer: D (メッセージを残す)

最新問題: **228**

Gaia OS 用にチェック・ポイント製品を自動的に更新するために使用されるチェック・ポイントのツールはどれですか？

- A. Check Point INSPECT エンジン
- B. チェック ポイント アップグレード サービス エンジン
- C. チェック ポイント更新エンジン
- D. Check Point アップグレード インストール サービス

Answer: B (メッセージを残す)

解説 参考：

参照: https://sc1.checkpoint.com/documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/html_frameset.htm?topic=documents/R77/CP_R77_Gaia_Installation_and_Upgrade_Guide/129978

最新問題: **229**

オペレーティング システム情報やリソース使用状況などのセキュリティ ゲートウェイの一般的なシステム情報の統計情報と、VPN、ID 認識、DLP の個々のソフトウェア ブレードの統計情報を表示するユーティリティはどれですか？

- A. cpconfig
- B. fw ctl pstat
- C. cpview
- D. fw ctl multik stat

Answer: C ([メッセージを残す](#))

説明

CPView ユーティリティは、Security Gateway / Security Management Server / Multi-Domain Security Management Server で実行できる (cpview コマンド) テキスト ベースの組み込みユーティリティです。CPView ユーティリティは、一般的なシステム情報 (CPU、メモリ、ディスク容量) とさまざまなソフトウェア ブレードの情報 (Security Gateway のみ) の両方を含む統計データを表示します。データは、アクセスしやすいビューで継続的に更新されます。

最新問題: 230

SandBlast には、攻撃をリアルタイムで防止するために連携する機能コンポーネントがいくつかあります。次のうち、SandBlast コンポーネントの一部でないものはどれですか？

- A. 脅威の雲
- B. メール転送エージェント
- C. 脅威のエミュレーション
- D. モバイルアクセス

Answer: ([解答を表示する](#))

最新問題: 231

Identity Awareness が有効になっている場合、Application Control にはどの ID ソースが使用されますか？

- A. 半径
- B. リモート アクセスと RADIUS
- C. 上記すべて
- D. AD クエリとブラウザベースの認証

Answer: D ([メッセージを残す](#))

Identity Awareness は、次の取得ソースから ID を取得します。

- * AD クエリ
- * ブラウザベースの認証
- * エンドポイント アイデンティティ エージェント
- * ターミナル サーバー アイデンティティ エージェント
- * リモートアクセス

参照：

https://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62007.htm

最新問題: 232

契約ファイルをインストールするには、どのアプリケーションを使用する必要がありますか？

- A. SmartView モニター
- B. WebUI
- C. SmartUpdate
- D. SmartProvisioning

Answer: C ([メッセージを残す](#))

解説 参考：

説明: SmartUpdate の使用: NGX R65 (またはそれ以降) の Security Management / Provider-1 / Multi-Domain Management Server を既に使用している場合、SmartUpdate を使用すると、手順 3 でダウンロードしたサービス契約ファイルをインポートできます。

SmartUpdate を開き、[Launch Menu] から [Licenses & Contracts] -> [Update Contracts] -> [From File...] を選択し、手順 3 でダウンロードしたファイルへのパスを指定します。

注: SmartUpdate がインターネットに接続されている場合は、ダウンロードおよびインポートの手順を実行しなくても、UserCenter からサービス契約ファイルを直接ダウンロードできます。

参考 [https://supportcenter.checkpoint.com/supportcenter/portal?](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089)

[eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk33089)

最新問題: 233

空白を埋めてください: ブラウザベースの認証では、ユーザーを Web ページに送り、_____ を使用して ID を取得します。

- A. ユーザー ディレクトリ
- B. キャプティブ ポータルと透過的な Kerberos 認証
- C. キャプティブ ポータル
- D. ユーザーチェック

Answer: ([解答を表示する](#))

ID 認識を有効にするには:

Identity Awareness 設定ウィザードが開きます。

最新問題: 234

完全なログ] 追跡オプションに含まれるが、追跡オプションには含まれない情報はどれですか。

ログ] 追跡オプション?

- A. アプリケーション情報
- B. 宛先ポート
- C. データ型情報
- D. ファイル属性

Answer: C ([メッセージを残す](#))

最新問題: 235

R80 がサポートされているオペレーティング システムは次のうちどれですか。

- A. SecurePlatform のみ
- B. Gaia、SecurePlatform、および Windows
- C. Windows のみ
- D. ガイアのみ

Answer: D ([メッセージを残す](#))

最新問題: 236

Check Point Appliance で、backup_fw という名前の Security Management Server バックアップ ファイルを見つけるのに最適な場所を選択します。

- A. /var/log/Cpbackup/backups/backup/backup_fw.tgs

- B. /var/log/Cpbackup/backups/backup/backup_fw.tar
- C. /var/log/Cpbackup/backups/backups/backup_fw.tar
- D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: ([解答を表示する](#))

説明

Gaia のバックアップ機能を使用すると、Gaia OS および Security Management サーバー データベースの構成をバックアップしたり、以前に保存した構成を復元したりできます。

構成は、次のディレクトリの .tgz ファイルに保存されます。

Gaia OS バージョン

ハードウェア

ローカル ディレクトリ

R75.40 - R77.20

チェック ポイントのアプライアンス

/var/log/CPbackup/backups/

サーバーを開く

/var/CPbackup/バックアップ/

R77.30

チェック ポイントのアプライアンス

/var/log/CPbackup/backups/

サーバーを開く

参考文献:

最新問題: **237**

Check Point アプライアンスの最も推奨されるインストール方法は何ですか？

- A. SmartUpdate のインストール
- B. Check Point ISOMorphic で作成された DVD メディア
- C. Check Point ISOMorphic で作成された USB メディア
- D. クラウドベースのインストール

Answer: C ([メッセージを残す](#))

解説 参考 :

最新問題: **238**

完全ログ」追跡オプションには含まれるが、ログ」追跡オプションには含まれない情報はどれですか？

- A. ファイル属性
- B. アプリケーション情報
- C. 宛先ポート
- D. データ型情報

Answer: D ([メッセージを残す](#))

解説 参考 :

説明: 追跡オプション

ネットワーク ログ - 基本的なファイアウォール情報のみを含むログを生成します: ソース、宛先、ソース ポート、宛先ポート、およびプロトコル。

ログ - ネットワーク ログ オプションと同等ですが、アプリケーション名も含まれます (たとえば、Dropbox)、およびアプリケーション情報 (たとえば、Web サイトの URL)。これがデフォルトの追跡オプションです。

フル ログ - ログ オプションと同等ですが、行われた各 URL リクエストのデータも記録します。

- 抑制が選択されていない場合は、完全なログが生成されます (R80 より前の管理で定義されているように)。

- 抑制が選択されている場合、拡張ログが生成されます (R80 より前の管理で定義されているように)。

なし - ログを生成しません。

参照: [https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?](https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/131914)

[topic=documents/R80/CP_R80_LoggingAndMonitoring/131914](https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/CP_R80_LoggingAndMonitoring/131914)

最新問題: 239

RADIUS プロトコルは、_____ を使用してゲートウェイと通信します。

A. UDP

B. TDP

C. CCP

D. HTTP

Answer: ([解答を表示する](#))

パラメーター :

最新問題: 240

あなたの上司は、会社の秘密を秘密裏に転送した疑いのある従業員を注意深く監視するようにあなたに望んでいます。競争。IT 部門は、容疑者が暗号化を使用するために WinSCP クライアントをインストールしたことを発見しました。コミュニケーション。このタスクを達成するのに最適な方法は次のうちどれですか？

A. SmartDashboard を使用して、彼の IP アドレスと一致するファイアウォール ルール ベースにルールを追加します。潜在的なターゲットと疑わしいプロトコル。アラート アクションまたはカスタマイズされたメッセージを適用します。

B. キーロギング型トロイの木馬が添付された電子メールを容疑者に送信し、容疑者に関する直接的な情報を取得します。不正行為。

C. ルール ベースに一致するパケットにアラート アクションを設定して、SmartView Monitor で彼の IP を監視します。インバウンドおよびアウトバウンド トラフィック用の IP アドレス。

D. SmartView Tracker を使用して、WinSCP 宛先を特徴とするログ エントリをフィルタリングすることにより、彼のアクションを追跡します。

港。次に、対応するエントリをドキュメント用の別のログ ファイルにエクスポートします。

Answer: D ([メッセージを残す](#))

最新問題: 241

Threat Extraction の背後にあるメカニズムは何ですか？

A. これは、あらゆる種類のファイルから悪意のあるファイルを収集して、目的の受信者に送信する前に破壊できる新しいメカニズムです。

- B. これは、悪意のあるコードの送信者の IP アドレスを特定し、それを SAM データベース (Suspicious Activity Monitoring) に入れる新しいメカニズムです。
- C. JavaScript、マクロ、リンクなど、ドキュメントのアクティブなコンテンツはすべてドキュメントから削除され、目的の受信者に転送されます。これにより、このソリューションは非常に高速になります。
- D. これは、ドキュメントから悪意のあるファイルを抽出して、送信者に対する反撃として使用する新しいメカニズムです。

Answer: C ([メッセージを残す](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **242**

外部 (インターネット) インターフェイスを介してキャプティブ ポータルへのアクセスをユーザーに提供するには、セキュリティ ポリシーをどのように構成しますか？

- A. ゲートウェイの設定を変更して、外部インターフェイス経由でキャプティブ ポータルにアクセスできるようにします。
- B. グローバル プロパティの下で ID 認識設定を変更して、すべてのインターフェイスでキャプティブ ポリシー アクセスを許可します。
- C. [グローバル プロパティ] の [アイデンティティ認識] 設定を変更して、外部インターフェイスのキャプティブ ポリシー アクセスを許可します。
- D. 対処は必要ありません。このアクセスはデフォルトで利用可能です。

Answer: A ([メッセージを残す](#))

最新問題: **243**

MyCorp には、次の NAT ルールがあります。Alpha 内部ネットワークの場合、NAT 機能を無効にする必要があります。
Google DNS (8.8.8.8) サーバーへのアクセスを試みます。
この場合、何ができますか？

- A. 手動 NAT ルールを使用して例外を作成する
- B. グローバル プロパティの NAT 設定を使用します。
- C. VPN コミュニティ内の NAT を無効にする
- D. Alpha 内部ネットワーク オブジェクトでネットワーク例外を使用する

Answer: D ([メッセージを残す](#))

最新問題: **244**

空白を埋める: ネットワーク ポリシー レイヤーでは、暗黙の最後のルールの既定のアクションは次のとおりです。
_____ すべてのトラフィック。ただし、Application Control ポリシー層では、デフォルト アクションは
_____ すべてのトラフィック。

- A. ドロップ; 受け入れる
- B. 受け入れる; リダイレクト

- C. 受け入れる; 落とす
 - D. リダイレクトします。落とす
- Answer:** ([解答を表示する](#))

最新問題: 245

Security Gateway R75 以降では、SIC は暗号化に _____ を使用します。

- A. 3DES
- B. AES-256
- C. DES
- D. AES-128

Answer: D ([メッセージを残す](#))

最新問題: 246

管理者は、本社と支社の間に IPsec サイト間 VPN を作成しています。どちらのオフィスも、同じ Security Management Server によって管理される Check Point Security Gateway によって保護されています。事前共有シークレットを指定するように VPN コミュニティを構成しているときに、管理者は、事前共有シークレットを有効にするチェック ボックスが共有されており、有効にできないことに気付きました。事前共有シークレットを指定できないのはなぜですか？

- A. 事前共有は、サードパーティベンダーと Check Point Security Gateway の間で VPN を作成する場合にのみ使用できます。
- B. 両方の Security Gateway で IPsec VPN ブレードを有効にする必要があります。
- C. Security Gateway は R75.40 より前です。
- D. 証明書ベースの認証は、同じ SMS によって管理される 2 つの Security Gateway 間で使用できる唯一の認証方法です。

Answer: D ([メッセージを残す](#))

最新問題: 247

次のうち、情報セキュリティに関連する一連の規制要件ではないものはどれですか？

- A. ISO 37001
- B. Sarbanes Oxley (SOX)
- C. HIPAA
- D. PCI

Answer: A ([メッセージを残す](#))

説明

ISO 37001 - 贈収賄防止管理システム

参考文献:

最新問題: 248

ログのクエリが非常に高速になった理由について、最もよく説明するものを選択してください。

- A. 新しい Smart-1 アプライアンスは、物理メモリのインストールを 2 倍にします
- B. 検索結果を高速化するために、インデックスエンジンはログにインデックスを付けます。
- C. SmartConsole は、Security Gateway から直接結果を照会するようになりました
- D. 保存されているログの量は、古いバージョンでは通常よりも少なくなっています

Answer: B ([メッセージを残す](#))

解説 参考 :

最新問題: 249

コマンドライン インターフェイスのデフォルトのシェルは何ですか？

- A. エキスパート
- B. クリッシュ
- C. 管理者
- D. 通常

Answer: ([解答を表示する](#))

説明

CLI のデフォルト シェルは clish と呼ばれます

最新問題: 250

空欄を埋めてください: _____ はログを収集し、それらを _____ に送信します。

- A. ログサーバー。セキュリティ管理サーバー
- B. ログサーバー; セキュリティ ゲートウェイ
- C. セキュリティ ゲートウェイ。ログサーバー
- D. セキュリティ管理サーバー。セキュリティ ゲートウェイ

Answer: ([解答を表示する](#))

最新問題: 251

空欄を埋める: アプリケーション層ファイアウォールは、TCP/IP モデルの _____ 層を通過し、_____ 層までのトラフィックを検査します。

- A. 下; 応用
- B. 最初の 2 つ。インターネット
- C. 上; 応用
- D. 最初の 2 つ。輸送

Answer: ([解答を表示する](#))

最新問題: 252

正誤問題: R80 では、複数の管理者が同時に書き込み権限で Security Management Server にログインできます。

- A. いいえ、この機能はグローバル プロパティで有効にする必要があります。
- B. 確かに、すべての管理者は、他の管理者から独立したセッションで作業します。
- C. 確かに、すべての管理者は、他の管理者から独立した別のデータベースで作業しています。
- D. False、1 人の管理者のみが書き込み権限でログインできます。

Answer: ([解答を表示する](#))

複数の管理者が同時に Security Management Server に接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。

最新問題: 253

Security Gateway にインストールされているセキュリティ ポリシー名を確認するには、どの R80 SmartConsole ツールを使用しますか？

- A. SmartView ステータス
- B. なし。SmartConsole アプリケーションは Security Management Server とのみ通信します。
- C. SmartView モニター
- D. SmartUpdate

Answer: ([解答を表示する](#))

最新問題: 254

R77 から R80 にアップグレードしようとしています。アップグレードの前に、システムをバックアップして、問題が発生した場合に、すべての構成ファイルと管理ファイルをそのままにして古いバージョンに簡単に復元できるようにします。このシナリオで最適なバックアップ方法は何ですか？

- A. バックアップ
- B. データベースのリビジョン
- C. スナップショット
- D. エクスポートを移行

Answer: C ([メッセージを残す](#))

解説 参考：

解説: 2. スナップショット管理

スナップショットは、ルート (lv_current) ディスク パーティション全体のバイナリ イメージを作成します。これには、チェック ポイントの製品、構成、およびオペレーティング システムが含まれます。

R77.10 以降、あるマシンからのイメージのエクスポートと、同じタイプの別のマシンへのそのイメージのインポートがサポートされています。

ログ パーティションはスナップショットに含まれません。したがって、ローカルに保存された FireWall ログは保存されません。

参考 https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108902

最新問題: 255

IKE によって実行される 2 フェーズ ネゴシエーション プロセスのフェーズ 1 は、_____ モードで動作します。

- A. メイン
- B. 認証
- C. クイック
- D. 高警報

Answer: A ([メッセージを残す](#))

説明

フェーズ I モード

Security Gateway 間では、IKE フェーズ I に 2 つのモードがあります。

これらのモードは IKEv1 にのみ適用されます。

* メインモード

*アグレッシブモード

最新問題: 256

Security Gateway がサポートする 2 つのタイプの NAT は何ですか？

- A. 宛先と非表示
- B. 非表示にして静的
- C. 静的およびソース
- D. ソースと宛先

Answer: B ([メッセージを残す](#))

Security Gateway は、次の手順を使用して、ネットワーク内の IP アドレスを変換できます。

* 静的 NAT - 各内部 IP アドレスは、異なるパブリック IP アドレスに変換されます。ファイアウォールは、外部トラフィックが内部リソースにアクセスできるようにすることができます。

* Hide NAT - ファイアウォールはポート番号を使用して、指定されたすべての内部 IP アドレスを単一のパブリック IP アドレスに変換し、内部 IP 構造を隠します。接続は内部コンピューターからのみ開始でき、外部コンピューターは内部サーバーにアクセスできません。ファイアウォールは最大で変換できます

外部コンピューターおよびサーバーから同時に 50,000 接続。

* ポート変換で NAT を隠す - 1 つの IP アドレスを使用して、外部ユーザーが隠しネットワーク内の複数のアプリケーション サーバーにアクセスできるようにします。ファイアウォールは、要求されたサービス (または宛先ポート) を使用して、トラフィックを正しいサーバーに送信します。一般的な構成では、次のポートを使用できます: FTP サーバー (ポート 21)、SMTP サーバー (ポート 25)、および HTTP サーバー (ポート 80)。ポート変換を使用するには、手動で NAT ルールを作成する必要があります。

参照 :

https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/6724.htm

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w**特別割引コード: **Freepdfdumps**)

最新問題: 257

次のスクリーンショットを見て、最良の回答を選択してください。

- A. Security Gateway の外部にあるクライアントは、FTP を使用して任意のファイルを FTP_Ext-server にアップロードできます。
- B. 内部クライアントは、FTP を使用して任意のファイルを FTP_Ext-server にアップロードおよびダウンロードできます。
- C. Security Gateway の外部にあるクライアントは、FTP を使用して FTP_Ext サーバーからアーカイブ ファイルをダウンロードできます。
- D. 内部クライアントは、FTP を使用してアーカイブ ファイルを FTP_Ext サーバーにアップロードおよびダウンロードできます。

Answer: ([解答を表示する](#))

最新問題: 258

空欄に記入してください。永続的な VPN トンネルは、コミュニティ内のすべてのトンネル、特定のゲートウェイのすべてのトンネル、または _____ に設定できます。

- A. コミュニティ内の特定のトンネルについて
- B. 特定のゲートウェイの特定のトンネルについて
- C. 特定のサテライト ゲートウェイからセントラル ゲートウェイ トンネルへ
- D. サテライト ゲートウェイからサテライト ゲートウェイへのすべてのトンネル

Answer: A ([メッセージを残す](#))

説明

コミュニティ内の各 VPN トンネルは、永続的なトンネルとして設定できます。永続的なトンネルは常に監視されているため、VPN トンネルがダウンしている場合は、ログ、アラート、またはユーザー定義のアクションを発行できます。VPN トンネルは、「トンネル テスト」パケットを定期的に変信することによって監視されます。パケットへの応答が受信されている限り、VPN トンネルは「稼働中」と見なされます。所定の時間内に応答が受信されない場合、VPN トンネルは「ダウン」していると見なされます。パーマナント トンネルは、Check Point Security Gateway 間でのみ確立できます。常設トンネルの設定は、コミュニティ レベルで行われます。

最新問題: 259

アクセス ロールにより、ファイアウォール管理者は次のようにネットワーク アクセスを構成できます。

- A. 上記すべて
- B. コンピュータまたはコンピュータ グループとネットワークの組み合わせ
- C. リモート アクセス クライアント
- D. ユーザーとユーザー グループ

Answer: A ([メッセージを残す](#))

最新問題: 260

次の図を確認できます。

そこには何が提示されていますか？

- A. ユーザー John の期限切れの .p12 証明書プロパティ。
- B. John のパスワードの共有シークレット プロパティ。
- C. John のゲートウェイの VPN 証明書のプロパティ。
- D. ユーザー John に対して発行された個人用 .p12 証明書ファイルのプロパティ。

Answer: D ([メッセージを残す](#))

最新問題: 261

IKE によって実行される 2 フェーズ ネゴシエーション プロセスのフェーズ 1 は、_____ モードで動作します。

- A. メイン
- B. 認証
- C. クイック
- D. 高警報

Answer: A ([メッセージを残す](#))

解説 参考：

Explanation:

フェーズ I モード

Security Gateway 間では、IKE フェーズ I に 2 つのモードがあります。これらのモードは IKEv1 にのみ適用されます。

メインモード

アグレッシブモード

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13847.htm

最新問題: 262

Logging and Monitoring の追跡オプションは、ログ、詳細ログ、および拡張ログです。各ログ、詳細ログ、拡張ログに追加できるオプションは次のうちどれですか？

- A. アカウンティング/サプレッション
- B. アカウンティング/拡張
- C. 経理
- D. 抑制

Answer: A ([メッセージを残す](#))

最新問題: 263

あなたは Alpha Corp の管理者です。R80 管理サーバーにログインしています。ルール ベースにいくつかの変更を加えていると、ルール No.6 の横に鉛筆アイコンがあることがわかります。

これは何を意味するのでしょうか？

- A. ルール No.6 は、管理セッションで編集するようにマークされています。
- B. ルール No.6 は、別の管理セッションで削除対象としてマークされています。
- C. ルール No.6 は、別の管理セッションで編集するためにマークされています。
- D. ルール No.6 は、管理セッションで削除対象としてマークされています。

Answer: A ([メッセージを残す](#))

最新問題: 264

R80 では、異なるチェックポイントコンポーネント間の通信はどのように保護されていますか？すべての質問と同様に、最良の回答を選択してください。

- A. IPSEC を使用して
- B. SICを使用
- C. ICA を使用して
- D. 3DES を使用して

Answer: B ([メッセージを残す](#))

解説 参考：

参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/125443

最新問題: 265

次のうち、識別名の構成要素ではないものはどれですか？

- A. 組織単位

- B. 国
- C. 通称
- D. ユーザーコンテナ

Answer: D ([メッセージを残す](#))

識別名コンポーネント

CN=共通名、OU=組織単位、O=組織、L=地方、ST=州または県、C=国名
topic=documents/R76/CP_R76_SecMan_WebAdmin/71950

最新問題: 266

ボブがオブジェクト検索でこの結果を得た場合、それはどういう意味ですか？ 下の画像を参照してください。最良の答えを選択する。

- A. その名前またはその IP アドレスを持つオブジェクトはデータベースにありません。
- B. オブジェクトに NAT IP アドレスがありません。
- C. 検索の詳細にサブネット マスクがありません。
- D. その IP アドレスを持つオブジェクトはデータベースにありません。

Answer: ([解答を表示する](#)**)**

最新問題: 267

空欄に記入してください: ライセンスをインストールするには、最初に _____ に追加する必要があります。

- A. ユーザー センター
- B. パッケージリポジトリ
- C. ダウンロード センター Web サイト
- D. ライセンスと契約のリポジトリ

Answer: ([解答を表示する](#)**)**

解説 参考 <https://sc1.checkpoint.com/documents/R77/>

CP_R77_Non_Gaia_Installation_and_Upgrade_Guide/13128.htm

最新問題: 268

すべての構成を変更せずに監査するための完全なアクセス権を必要とする管理者に割り当てる必要がある事前定義済みのアクセス許可プロファイルはどれですか？

- A. 審査員
- B. すべて読み取り専用
- C. スーパーユーザー
- D. フルアクセス

Answer: B ([メッセージを残す](#))

説明

新しい権限プロファイルを作成するには:

[新しいプロファイル] ウィンドウが開きます。

最新問題: 269

次の自動生成ルールの NAT ルールのうち、実装の優先度が最も低いのはどれですか？

- A. マシン非表示 NAT
- B. アドレス範囲 Hide NAT
- C. ネットワーク非表示 NAT
- D. マシンの静的 NAT

Answer: ([解答を表示する](#))

解説 参考 :

Explanation:

SmartDashboard は、自動 NAT ルールを次の順序で編成します。

1. ファイアウォール、またはノード (コンピューターまたはサーバー) オブジェクトの静的 NAT ルール
2. ファイアウォールまたはノード オブジェクトの NAT ルールを非表示にする
3. ネットワークまたはアドレス範囲オブジェクトの静的 NAT ルール
4. ネットワークまたはアドレス範囲オブジェクトの NAT ルールを非表示にする

参照 :

https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm

最新問題: 270

分散環境では、Central ライセンスを CLI 経由で Security Gateway にインストールできます。

- A. 確かに、CLI はライセンス取得に推奨される方法です。
- B. はい。Central ライセンスは Security Gateway で CPLIC コマンドを使用してインストールできます。
- C. いいえ、セントラル ライセンスは Security Management Server 経由で処理されます
- D. いいえ、セントラル ライセンスは Gaia を介して Security Gateway にインストールされます。

Answer: B ([メッセージを残す](#))

最新問題: 271

管理者がこれらのファイルをスキャンまたは分析する必要があることを脅威対策ブレードに指定できるように、信頼できるファイルのリストを管理者に提供するツールはどれですか？

- A. ホワイトリスト ファイル
- B. アプリウィキ
- C. IPS 保護
- D. スレットウィキ

Answer: D ([メッセージを残す](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html>
(**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 272

ポリシー レイヤ トラフィック インスペクションについて説明する BEST を選択してください。

A. パケットがインライン層に一致する場合、次の層に一致し続けます。

B. パケットがどのインライン レイヤーとも一致しない場合、一致は次の層に続きます。
層。

C. パケットがどのインライン レイヤーとも一致しない場合、パケットは暗黙的クリーンアップ ルールと照合されます。

D. パケットがネットワーク ポリシー レイヤーと一致しない場合、一致はそのインライン レイヤーに続きます。

Answer: A ([メッセージを残す](#))

最新問題: 273

ヒット カウント データが保持されるデフォルトの期間は？

A. 3ヶ月

B. 4 週間

C. 12ヶ月

D. 6ヶ月

Answer: ([解答を表示する](#)**)**

説明

ヒット カウント データを最大に保つ - 時間範囲オプションのいずれかを選択します。デフォルトは 6 か月です。この期間、データは Security Management Server データベースに保持され、[ヒット数] 列に表示されます。

参考文献:

最新問題: 274

R80 より前のゲートウェイの IPS ポリシーは、_____ の間にインストールされます。

A. ファイアウォール ポリシーのインストール

B. 脅威対策ポリシーのインストール

C. アンチボット ポリシーのインストール

D. アクセス制御ポリシーのインストール

Answer: B ([メッセージを残す](#))

https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.htm?topic=documents/R80/CP_R80BC_ThreatPrevention/136486

最新問題: 275

_____ 種類のソフトウェア コンテナ _____ があります。

A. 3; セキュリティ管理、Security Gateway、およびエンドポイント セキュリティ

B. 3; セキュリティ ゲートウェイ、エンドポイント セキュリティ、およびゲートウェイ管理

C. 2; セキュリティ管理とエンドポイント セキュリティ

D. 2; エンドポイント セキュリティとセキュリティ ゲートウェイ

Answer: A ([メッセージを残す](#))

ソフトウェア コンテナには、Security Management、Security Gateway、Endpoint Security の 3 種類があります。

参照 :

<http://downloads.checkpoint.com/dc/download.htm?ID=11608>

最新問題: 276

次のうち、SecureXL トラフィック フローでないものはどれですか？

- A. ミディアム パス
- B. 加速パス
- C. 高優先パス
- D. スローパス

Answer: C ([メッセージを残す](#))

説明

SecureXL は、ファイアウォールのパフォーマンスを最大化し、セキュリティを損なうことのないアクセラレーション ソリューションです。Security Gateway で SecureXL が有効になっている場合、一部の CPU を集中的に使用する操作は、ファイアウォール カーネルではなく、仮想化されたソフトウェアによって処理されます。ファイアウォールは、接続をより効率的に検査および処理し、スループットと接続速度を加速できます。これらは SecureXL トラフィック フローです:

低速パス - ファイアウォールによって検査され、SecureXL によって処理されないパケットと接続。

加速パス - SecureXL にオフロードされ、ファイアウォールによって処理されないパケットと接続。

中程度のパス - より詳細な検査が必要なパケットは、高速化されたパスを使用できません。ファイアウォールがこれらのパケットを検査する必要はありません。これらのパケットはオフロードでき、低速パスを使用しません。たとえば、IPS によって検査されるパケットは高速パスを使用できず、IPS PSL (パッシブ ストリーミング ライブラリ) にオフロードできます。SecureXL は、これらのパケットを低速パスのパケットよりも高速に処理します。

最新問題: 277

ID共有をサポートするために使用される2つのIdentity Awarenessコマンドは？

- A. ポリシー決定ポイント (PDP) とポリシー施行ポイント (PEP)
- B. ポリシー実施ポイント (PEP) とポリシー操作ポイント (PMP)
- C. ポリシー操作ポイント (PMP) およびポリシー アクティベーション ポイント (PAP)
- D. ポリシー アクティベーション ポイント (PAP) とポリシー決定ポイント (PDP)

Answer: ([解答を表示する](#))

解説 参考 <https://sc1.checkpoint.com/documents/R76/>

CP_R76_IdentityAwareness_AdminGuide/66477.htm

最新問題: 278

ユーザーの身元がわかっている場合はどうなりますか？

- A. ユーザー資格情報がアクセス ロールと一致しない場合、トラフィックは自動的にドロップされます。
- B. ユーザー資格情報がアクセス ロールと一致しない場合、システムはサンドボックスを表示します。
- C. ユーザー資格情報がアクセス ロールと一致する場合、ルールが適用され、定義されたアクションに基づいてトラフィックが受け入れられるかドロップされます。
- D. ユーザー資格情報がアクセス ロールと一致しない場合、システムはキャプティブ ポータルを表示します。

Answer: C ([メッセージを残す](#))

最新問題: 279

空欄を埋めてください: 暗黙のルールは _____ ウィンドウで操作されます。

- A. NAT
- B. ファイアウォール
- C. グローバル プロパティ
- D. オブジェクト エクスプローラー

Answer: C ([メッセージを残す](#))

解説 参考 https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

最新問題: 280

次のうち、R77.X 以前では使用できなかった新しい R80.10 ゲートウェイ機能はどれですか？

- A. ルール ベースは、それぞれが一連のセキュリティ ルールを含むレイヤーで構築できます。レイヤーは定義された順序で検査されるため、ルール ベース フローを制御し、どのセキュリティ機能を優先するかを制御できます。
- B. 社内のストリーミング メディアのアップロードとダウンロードのスループットを 1 Gbps に制限します。
- C. ルールに対する時間オブジェクトで、指定された時間だけルールをアクティブにします。
- D. サブ ポリシーは、作成して特定のルールに関連付けることができる一連のルールです。ルールが一致した場合、インスペクションは次のルールではなく、それに関連付けられたサブ ポリシーで続行されます。

Answer: D ([メッセージを残す](#))

説明

参考文献:

最新問題: 281

ユーザーを既存のロールに追加する、または既存のロールからユーザーを追加するために使用するコマンドはどれですか？

- A. rba ユーザー <User Name> ロール <List> を追加します。
- B. rba ユーザーの追加 <ユーザー名>
- C. ユーザー <User Name> ロール <List> を追加します。
- D. ユーザーの追加 <ユーザー名>

Answer: ([解答を表示する](#))

説明

役割の構成 - CLI (rba)

最新問題: 282

ボブがオブジェクト検索でこの結果を得た場合、それはどういう意味ですか？ 下の画像を参照してください。

- A. その IP アドレスを持つオブジェクトはデータベースにありません。
- B. 検索の詳細にサブネット マスクがありません。
- C. その名前またはその IP アドレスを持つオブジェクトはデータベースにありません。
- D. オブジェクトに NAT IP アドレスがありません。

Answer: C ([メッセージを残す](#))

最新問題: 283

次のうち、Identity Awareness が ID を取得するために使用方法でないものはどれですか？

- A. 半径
- B. Active Directory クエリ
- C. リモートアクセス
- D. 証明書

Answer: D ([メッセージを残す](#))

解説 参考 <https://www.checkpoint.com/products/identity-awareness-software-blade/>

最新問題: 284

クラスター メンバーのフェイルオーバーはどこでトリガーできますか？

1. Security Gateway CLI にログインし、コマンド clusterXL_admin down を実行します。
2. SmartView Monitor で、Security Gateway メンバーを右クリックし、[Cluster member down] を選択します。
3. Security Gateway CLI にログインし、コマンド cphaprob down を実行します。

- A. 1、2、および 3
- B. 2 と 3
- C. 1 と 2
- D. 1 と 3

Answer: C ([メッセージを残す](#))

フェイルオーバーを開始する方法

最新問題: 285

チェック ポイントのホスト オブジェクトについて正しいものは次のうちどれですか？

- A. R77.30 以前のバージョンから R80 にアップグレードすると、チェック ポイントのホスト オブジェクトがゲートウェイ オブジェクトに変換されます。
- B. 複数のインターフェイスがインストールされている場合でも、Check Point Host にはルーティング機能がありません。
- C. Check Point Host は、IP 転送メカニズムを持つことができます。
- D. チェック ポイント ホストは、ファイアウォールとして機能できます。

Answer: B ([メッセージを残す](#))

最新問題: 286

SmartConsole にログインできません。管理サーバーにログインして #cpwd_admin list を実行すると、次の出力が表示されます。

SmartConsole に接続できない理由を最もよく説明できる理由は何ですか？

- A. CDP がダウンしています
- B. SVR がダウンしています
- C. CPM と FWM がダウン
- D. CPSM がダウンしています

Answer: C ([メッセージを残す](#))

説明

正解は FWM (SmartConsole アプリケーションと Security Management Server 間の通信を可能にするプロセスです) です。STATE は T (Terminate = Down) です。

* SmartDashboard が Security Management サーバーに接続できません。

* FWM プロセスが実行されているかどうかを確認します。これを行うには、次のコマンドを実行します。

```
[Expert@HostName:0]# ps -aux | grep fwm
```

* FWM プロセスが実行されていない場合は、次のコマンドでプロセスを強制的に開始してみてください。

```
[Expert@HostName:0]# cpwd_admin start -name FWM -path "$FWDIR/bin/fwm" -command "fwm"
```

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: **287**

暗号化されたパケットが復号化されると、これはどこで行われますか？

- A. 復号化はサポートされていません
- B. アウトバウンド チェーン
- C. セキュリティ ポリシー
- D. インバウンド チェーン

Answer: C (メッセージを残す)

最新問題: **288**

次のうち、SmartConsole で作成されたアカウントに使用される認証方式ではないものはどれですか？

- A. セキュリティの質問
- B. チェックポイントのパスワード
- C. SecurID
- D. 半径

Answer: A (メッセージを残す)

解説 参考 :

Explanation:

認証方式 :- チェック ポイントのパスワード

- オペレーティング システムのパスワード
- ラディウス
- SecurID
- タカス

- 未定義 未定義の認証スキームを持つユーザーが、何らかの形式の認証を持つセキュリティ ルールに一致する場合、アクセスは常に拒否されます。

参考 :http://dl3.checkpoint.com/paid/71/How_to_Configure_Client_Authentication.pdf?

HashKey=1479692369_23bc7cdfbeb67c147ec7bb882d557fd4&xtn=.pdf

最新問題: **289**

ルール ベースとクライアント認証アクションのプロパティ画面を調べます。

Security Gateway によって認証された後、ユーザーは Web サイトへの HTTP 接続を開始します。ユーザーがコマンド ラインを使用して別のサイトに FTP で接続しようとするとうなりますか？：

- A. ユーザーが正常に認証された後、FTP データ接続が切断されます。
- B. ユーザーは Security Gateway によって再度認証を求められます。
- C. ユーザーはその FTP サイトからのみ認証するように求められ、クライアント認証のためにユーザー名とパスワードを入力する必要はありません。
- D. FTP 接続はルール 2 によってドロップされます。

Answer: C ([メッセージを残す](#))

最新問題: 290

空欄を埋めてください: _____ 種類のソフトウェア コンテナ _____ があります。

- A. 3; セキュリティ管理、Security Gateway、およびエンドポイント セキュリティ
- B. 3; セキュリティ ゲートウェイ、エンドポイント セキュリティ、およびゲートウェイ管理
- C. 2; セキュリティ管理とエンドポイント セキュリティ
- D. 2; エンドポイント セキュリティとセキュリティ ゲートウェイ

Answer: A ([メッセージを残す](#))

解説 参考：

Explanation:

ソフトウェア コンテナには、Security Management、Security Gateway、Endpoint Security の 3 種類があります。

参照：

<http://downloads.checkpoint.com/dc/download.htm?ID=11608>

最新問題: 291

1 つを除いて、すべての R77 セキュリティ サーバーが認証を実行できます。認証を実行できないセキュリティ サーバーはどれですか？

- A. FTP
- B. HTTP
- C. SMTP
- D. RLOGIN

Answer: ([解答を表示する](#))

最新問題: 292

ネットワーク内のチェック ポイントのすべてのコンポーネントのうち、最も頻繁に変更され、最も頻繁にバックアップする必要があるのはどれですか？

- A. スマートコンソール
- B. スマートマネージャー
- C. セキュリティ ゲートウェイ
- D. セキュリティ管理サーバー

Answer: D ([メッセージを残す](#))

最新問題: 293

アクセス ロールにより、ファイアウォール管理者は次のようにネットワーク アクセスを構成できます。

- A. コンピュータグループとネットワークの組み合わせ
- B. ユーザーとユーザー グループ
- C. 上記すべて
- D. リモート アクセス クライアント

Answer: C (メッセージを残す)

アクセス ロールを作成するには:

[アクセス ロール] ウィンドウが開きます。

選択内容は、[役割のプレビュー] ペインの [ネットワーク] ノードに表示されます。

ウィンドウが開きます。Active Directory エントリを検索するか、リストから選択できます。

AD エントリを検索するか、リストから選択できます。

アクセス ロールが [ユーザーと管理者] ツリーに追加されます。

最新問題: 294

クリーンアップ規則の目的は何ですか？

- A. クリーンアップ ルールには何の目的もありません。
- B. 不要なルールを判断するためのメトリックを提供します。
- C. 明示的に許可されていないトラフィックをドロップします。
- D. ポリシーをより適切に最適化するために使用されます。

Answer: C (メッセージを残す)

これらは、すべてのルール ベースに推奨される基本的なアクセス コントロール ルールです。

* Security Gateway への直接アクセスを防止するステルス ルール。

* 以前のルールで許可されていないすべてのトラフィックをドロップするクリーンアップ ルール。

すべてのトラフィックをドロップする暗黙のルールもありますが、クリーンアップ ルールを使用してトラフィックをログに記録できます。

参照: https://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92703.htm

最新問題: 295

次の図では、管理者が Identity Awareness を構成しています。

[次へ] をクリックした後、上記の構成は以下でサポートされます。

- A. Active Directory 統合のために機能する Kerberos SSO
- B. Security Gateway が Active Directory を関連付けることができる Active Directory 統合に基づくユーザーに対して完全に透過的な方法で、ユーザーとマシンを IP アドレスに変換します。
- C. キャプティブポータルの使用義務
- D. ポート 443 または 80 は、ブラウザーベースの構成済み認証で使用されます。

Answer: B (メッセージを残す)

説明

ID 認識を有効にするには:

Identity Awareness 設定ウィザードが開きます。

最新問題: 296

空欄を埋める: R80 SmartConsole、SmartEvent GUI クライアント、および _____ は、数十億のログを統合し、それらを優先順位付けされたセキュリティ イベントとして表示します。

- A. スマートモニター
- B. SmartView Web アプリケーション
- C. SmartReporter
- D. スマートトラッカー

Answer: ([解答を表示する](#))

SmartEvent によるイベント分析 SmartEvent Software Blade は、統合されたセキュリティ イベント管理および分析ソリューションであり、リアルタイムのグラフィカルな脅威管理情報を提供します。SmartConsole、SmartView Web アプリケーション、および SmartEvent GUI クライアントは、数十億のログを統合し、優先順位付けされたセキュリティ イベントとして表示するため、セキュリティ インシデントに即座に対応し、必要なアクションを実行してさらなる攻撃を防ぐことができます。ビューをカスタマイズして、最も重要なイベントを監視できます。数回クリックするだけで、概要ビューから詳細なフォレンジック分析に移動できます。フリーテキスト検索と提案により、データ分析をすばやく実行し、重要なセキュリティ イベントを特定できます。

最新問題: 297

完全な読み取り/書き込みアクセス権を持つデフォルトの Gaia ユーザーは？

- A. 管理者
- B. スーパーユーザー
- C. モニター
- D. アルトユーザー

Answer: ([解答を表示する](#))

最新問題: 298

管理者 Kofi は、管理サーバーにいくつかの変更を加え、SmartConsole の [公開] ボタンをクリックしましたが、下のスクリーンショットに示すエラー メッセージが表示されました。

これらのエラーの詳細について、管理者はどこで確認できますか？

- A. SmartConsole の Log and Monitor セクション
- B. SmartConsole の検証セクション
- C. SmartConsole のオブジェクトセクション
- D. SmartConsole のポリシー セクション

Answer: B ([メッセージを残す](#))

検証エラー SmartConsole の検証ペインには、構成エラー メッセージが表示されます。エラーの例としては、固有でないオブジェクト名、およびルール ベースで無効なオブジェクトの使用があります。

発行するには、エラーを修正する必要があります。

最新問題: 299

SmartDashboard にアクセスできない管理者が、週末に新しい IPSO ベースの R80 セキュリティ ゲートウェイをインストールしました。彼は SIC アクティベーション キーと Security Gateway の IP アドレスを電子メールで送信しました。ポリシーをインストールして、Security Gateway と Management Server 間の通信を確認したい。ポリシーのインストールを妨げる原因は何ですか？

- A. 中間のローカル Security Gateway は、それを介してリモートの新しい Security Gateway アプライアンスにポリシーをインストールすることを許可しません。ローカル Security Gateway でコマンド fw unloadlocal を実行して解決します。
- B. 制限付きのデフォルト ポリシーを削除するには、最初に R77 Security Gateway アプライアンスでコマンド fw unloadlocal を実行する必要があります。
- C. Security Gateway と Management Server の間に Secure Internal Communications (SIC) が確立されていません。Security Management Server で SIC を初期化する必要があります。
- D. まず、SmartDashboard で新しいゲートウェイ オブジェクトを作成し、[通信] ボタンを使用して SIC を確立し、ゲートウェイのトポロジを定義する必要があります。

Answer: ([解答を表示する](#))

最新問題: 300

グローバル プロパティの次の設定を検討してください。

選択されたオプション UDP (クエリ) 経由でドメイン名を受け入れる」は、次のことを意味します。

- A. すべてのインターフェースを通過できるトラフィックでは、UDP クエリは受け入れられず、これが行われます。セキュリティ ポリシーで管理者によって記述された最初の明示的なルールの前。
- B. すべての UDP クエリは、すべてのインターフェースを通過できるトラフィックによって受け入れられ、これが行われます。セキュリティ ポリシーで管理者によって記述された最初の明示的なルールの前。
- C. すべての UDP クエリは、管理者によって記述された最初の明示的なルールによって許可されたトラフィックによって受け入れられます。セキュリティ ポリシー。
- D. UDP クエリは、外部のアンチ スプーフィングを備えたインターフェイスを介してのみ許可されるトラフィックによって受け入れられます。これは、セキュリティ ポリシーで管理者によって記述された最初の明示的なルールの前に行われます。

Answer: D ([メッセージを残す](#))

最新問題: 301

あなたは ABC Corp. の管理者です。R80 管理サーバーにログインしています。ルール ベースにいくつかの変更を加えていると、ルール No.6 の横に鉛筆アイコンがあることがわかります。

これは何を意味するのでしょうか？

- A. ルール No.6 は、別の管理セッションで編集するためにマークされています。
- B. ルール No.6 は、別の管理セッションで削除対象としてマークされています。
- C. ルール No.6 は、管理セッションで編集するようにマークされています。
- D. ルール No.6 は、管理セッションで削除対象としてマークされています。

Answer: ([解答を表示する](#))

有効な **156-215.80** 問題集は GoShiken.com が提供された合格しやすい 156-215.80 試験問題集！ GoShiken.com が最新の **156-215.80** 試験問題集を提供しています。GoShiken.com 156-215.80 試験問題は最新で、解答が正確でございます。最新の GoShiken.com 156-215.80 問題集をゲットする人はこちら: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (**52730%OFF**問題集溶と正解付きで **30%w** 特別割引コード: **Freepdfdumps**)

最新問題: 302

クライアントは、リモート ロケーションで管理される新しいゲートウェイ オブジェクトを作成しました。
クライアントがセキュリティ ポリシーを新しいゲートウェイ オブジェクトにインストールしようとする、オブジェクトが [インストール先] チェック ボックスに表示されません。何をすべきですか？

- A. セキュアな内部通信 (SIC) がオブジェクトに構成されていません。
- B. ゲートウェイ オブジェクトのインターフェイスでスプーフィング対策が構成されていません。
- C. [チェック ポイント] > [ネットワーク オブジェクト] ダイアログ ボックスの [セキュア ゲートウェイ] オプションを使用して作成されたゲートウェイ オブジェクトですが、セキュリティ用のインターフェイスを設定する必要があります。
ゲートウェイ オブジェクト。
- D. [ネットワーク オブジェクト] ダイアログ ボックスの [チェック ポイント] > [外部管理 VPN ゲートウェイ] オプションを使用して作成されたゲートウェイ オブジェクト。

Answer: D ([メッセージを残す](#))

最新問題: 303

次の図では、ポリシーのレイヤーが示されています。
定義されたポリシーのトラフィック インспекションの優先順位は？

- A. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールに対してチェックされます。その後、暗黙的なドロップルールによってパケットがドロップされた場合、パケットは IPS レイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。
- B. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合され、パケットを受け入れるルールがあれば、IPS レイヤーの次の場所に到着し、パケットを受け入れた後、Threat に渡されます。防止層
- C. パケットはゲートウェイに到着し、ネットワーク ポリシー レイヤーのルールと照合されます。パケットを受け入れるルールがあれば、次に脅威防御レイヤーに到達し、パケットを受け入れた後、次のレイヤーに渡されます。IPS レイヤー。
- D. パケットはゲートウェイに到着し、IPS ポリシー レイヤーのルールに対してチェックされ、次にネットワーク ポリシー レイヤーに到着し、パケットを受け入れた後、脅威防御レイヤーに渡されます。

Answer: ([解答を表示する](#)**)**

解説 参考：

説明: ポリシー管理を簡素化するために、R80 はポリシーをポリシー レイヤーに編成します。レイヤーは一連のルール、つまりルールベースです。

たとえば、以前のバージョンから R80 にアップグレードする場合:

ファイアウォールと Application Control Software Blade が有効になっているゲートウェイには、
アクセス コントロール ポリシーは、ネットワークとアプリケーションの 2 つの順序付けられた層に分割されます。
ゲートウェイがレイヤー内のルールと一致すると、次のレイヤー内のルールの評価を開始します。

IPS および脅威エミュレーション ソフトウェア ブレードが有効になっているゲートウェイには、その脅威があります。
防御ポリシーは、IPS と脅威対策の 2 つの並列レイヤーに分割されます。
すべてのレイヤーが並行して評価されます
参照: https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm?topic=documents/R80/CP_R80_SecMGMT/126197

最新問題: 304

再起動すると失われる、保存されていない変更が GAiA にあるかどうかを確認したいと考えています。どのようなコマンドを使用できますか？

- A. 構成状態を表示
- B. 保存状態を表示
- C. 未保存を表示
- D. 構成の差分を表示

Answer: A ([メッセージを残す](#))

最新問題: 305

キャプティブ ポータルへのアクセスを構成する際に有効なオプションではないのは、次のうちどれですか？

- A. すべてのインターフェイスを介して
- B. ファイアウォール ポリシーによる
- C. インターネットから
- D. 内部インターフェース経由

Answer: ([解答を表示する](#)**)**

最新問題: 306

SmartView Monitor でアラートを構成する方法を教えてください。

- A. ゲートウェイを右クリックし、[プロパティ] を選択します。
- B. ゲートウェイを右クリックし、[システム情報] を選択します。
- C. SmartView Monitor でアラートを構成できません。
- D. ゲートウェイを選択し、しきい値を構成します。

Answer: ([解答を表示する](#)**)**

最新問題: 307

セキュリティ ポリシーには、2 つのルール、10 人のユーザー、および 2 つのユーザー グループがあります。この構成のデータベース バージョン 1 を作成します。次に、2 人の既存のユーザーを削除し、新しいユーザー グループを追加します。1 つのルールを変更し、2 つの新しいルールをルール ベースに追加します。セキュリティ ポリシーを保存し、データベース バージョン 2 を作成します。しばらくして、ルール ベースを使用するためにバージョン 1 にロールバックすることにしましたが、ユーザー データベースは保持したいと考えています。どうすればこれを行うことができますか？

- A. ユーザー データベースを除くデータベース全体を復元します。
- B. ユーザー データベースを除くデータベース全体を復元し、新しいユーザーとユーザー グループを作成します。

C. fwm_dbexport を実行して、ユーザー データベースをエクスポートします。[データベース リビジョン] 画面で、[データベース全体を復元] を選択します。次に、fwm_dbimport を実行します。

D. fwm dbexport -1 filename を実行します。データベースを復元します。次に、fwm dbimport -1 filename を実行してユーザーをインポートします。

Answer: A ([メッセージを残す](#))

最新問題: 308

Dave と Jon の 2 人の管理者が ABC Corp の管理者として R80 Management を管理しています。Jon は R80 Management にログインし、Dave が同じサーバーにログインした直後にログインしました。どちらも [セキュリティ ポリシー] ビューにあります。以下のスクリーンショットから、Jon の SmartConsole ビューに規則 6 があるにもかかわらず、Dave の SmartConsole ビューに規則 6 がないのはなぜですか？

A. Jon は現在ルール 6 を編集していますが、変更の一部を公開しています。

B. Dave は現在ルール 6 を編集しており、このルールを削除対象としてマークしています。

C. Dave は現在、ルール No.6 を編集しており、ルール ベースから削除しました。

D. Jon は現在、ルール No.6 を編集していますが、まだ変更を公開していません。

Answer: D ([メッセージを残す](#))

説明

管理者が SmartConsole を介して Security Management Server にログインすると、新しい編集セッションが開始されます。セッション中に管理者が行った変更は、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールにロック アイコンが表示されます。すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルールのロックを解除するには、管理者はセッションを公開する必要があります。

Valid 156-215.80 Dumps shared by GoShiken.com for Helping Passing 156-215.80 Exam! GoShiken.com now offer the **newest 156-215.80 exam dumps**, the GoShiken.com 156-215.80 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 156-215.80 dumps with Test Engine here: <https://www.goshiken.com/CheckPoint/156-215.80-mondaishu.html> (527 Q&As Dumps, **30%OFF** Special Discount: **Freepdfdumps**)