CheckPoint.156-215.82.v2026-06-15.q106

試験コード:	156-215.82
試験名称:	Check Point Certified Security Administrator - R82
認定資格:	CheckPoint
無料問題数:	106
バージョン:	v2026-06-15
アクセス数:	104
ページビュー数:	1060
https://www.jpnpdf.com/CheckPoint.156-215.82.v2026-06-15.q106-mondaishu.html	

最新問題: **1**
Gaia Web インターフェースから、セキュリティ管理サーバー上で実行できない操作は次のどれですか?
A. セキュリティポリシーを検証する
B. ターミナルシェルを開く
C. 静的ルートを追加する
D. セキュリティ管理GUIクライアントの表示
Answer: (解答を表示する)
Gaiaウェブインターフェースからセキュリティ管理サーバー上で実行できない操作は、セキュリティポリシーの検証です。この操作はSmartConsole4からのみ実行できます。Check Point R81 SmartConsoleオンラインヘルプ

最新問題: **2**
R80 の 「共有ポリシー」の利点は何ですか?
A. 管理者がセキュリティゲートウェイによって識別されたすべてのユーザー間でポリシーを共有できるようにします。
B. 管理者がセキュリティ管理サーバーを管理するすべての管理者間でポリシーを共有できるようにします。
C. 管理者がポリシーを共有して、別のポリシー パッケージで使用できるようにします。
D. 管理者が 1 つのセキュリティ ゲートウェイにポリシーをインストールし、そのポリシーが別の管理対象セキュリティ ゲートウェイにもインストールされることを許可します。
Answer: C (メーッセージを残す)
共有ポリシーとは、複数のポリシーパッケージで使用できるルールセットです。管理者は、異なるゲートウェイやドメインに共通のセキュリティポリシーを作成し、重複や不整合を回避できます。共有ポリシーの他のオプションは、共有ポリシーの利点ではありません。
[共有ポリシーの概要]、[共有ポリシーのベストプラクティス]

最新問題: **3**
ゲートウェイとセキュリティ管理サーバー間の信頼関係を最初に構築するために使用されるのは次のどれですか?
A. 内部証明機関
B. トークン

C. ワンタイムパスワード
D. 証明書
Answer: C (メーッセージを残す**)**
ワンタイムパスワードは、ゲートウェイとセキュリティ管理サーバー間の信頼関係を最初に構築するために使用されます。管理者はSmartConsoleからワンタイムパスワードを生成し、cpconfigコマンドを使用してゲートウェイのコマンドラインインターフェースに入力します。これにより、ゲートウェイとサーバー間のセキュア内部通信（SIC）が確立されます。その他のオプションは、この目的では使用されません。[セキュア内部通信（SIC）の設定]、[Check Point CCSA - R81：模擬試験と解説]

最新問題**: 4**
主要なNATはどちらもHide NATとStatic NATをサポートしています。しかし、どちらか一方の方がより柔軟性が高いです。正しいのはどちらですか？
A. 手動 NAT は自動 NAT よりも柔軟性が高くなります。
B. 動的ネットワーク アドレス変換 (NAT) オーバーロードは、ポート アドレス変換よりも柔軟性が高くなります。
C. ポート アドレス変換を備えたダイナミック NAT は、ネットワーク アドレス変換 (NAT) オーバーロードよりも柔軟性が高くなります。
D. 自動 NAT は手動 NAT よりも柔軟性が高くなります。
Answer: A (メーッセージを残す**)**
手動NATは、管理者がNATルールを任意の順序と位置で定義できるため、自動NATよりも柔軟性が高くなります1。自動NATはNATルールを自動的に作成し、NATルールベースの最上位または最下位に配置します2。Check Point R81ファイアウォール管理ガイド、Check Point R81セキュリティ管理ガイド

最新問題**: 5**
空欄を埋めてください: _____ はサーバーをオフにする Gaia コマンドです。
A. システムダウン
B. 終了
C. 停止
D. シャットダウン
Answer: C (メーッセージを残す**)**
haltは、サーバーの電源を切るGaiaコマンドです。このコマンドはオペレーティングシステムをシャットダウンし、マシンの電源をオフにします。サーバーのシャットダウンに使用できる他のコマンドには、shutdownとpoweroffがあります。[Gaia管理ガイド R80.40]

最新問題**: 6**
SAM ルールはどのような機能や利点を提供するために実装されますか?
A. セキュリティ監査を許可します。
B. ポリシーで定義されたとおりにトラフィックを処理します。
C. シーケンスアクティビティを監視します。
D. 疑わしいアクティビティをブロックします。
Answer: (解答を表示する**)**
SAM（Suspicious Activity Monitoring：疑わしいアクティビティの監視）ルールは、疑わしいアクティビティをブロックする機能または利点を提供するために実装されます。SAMルールは、攻撃、スキャン、ポリシー違反などの疑わしいアクティビティをファイアウォール

が検出した際に実行するアクションを定義するルールです。アクションには、疑わしいアクティビティを引き起こしたトラフィックのブロック、ドロップ、拒否、またはログへの記録が含まれます。SAMルールは手動で作成することも、IPS、アンチボット、SmartEventなどの他のセキュリティ機能によって自動的に作成することもできます。[SAMルール]、[疑わしいアクティビティの監視ルール]

最新問題: **7**
コマンドラインインターフェースのデフォルトのシェルは何ですか?
A. クリッシュ
B. 管理者
C. 通常
D. エキスパート
Answer: A (メーッセージを残す**)**
Clishはコマンドラインインターフェースのデフォルトシェルです。メニューベースとコマンドラインモードを備えたユーザーフレンドリーなシェルです。Admin、Normal、Expertは有効なシェル名ではありません1。

最新問題: **8**
Check Pointアプライアンスへの初期インストール後、管理インターフェースとデフォルトゲートウェイが正しくないことに気づきました。IPアドレスを192.168.80.200/24、デフォルトゲートウェイを192.168.80.1に設定するには、どのコマンドを使用すればよいですか？
A. インターフェース管理ipv4アドレスを192.168.80.200、マスク長を24に設定、スタティックルートのデフォルトネクストホップゲートウェイアドレスを192.168.80.1に設定、onsave config
B. インターフェース管理ipv4アドレス192.168.80.200 255.255.255.0を追加し、スタティックルート0.0.0.0.0.0.0.0 gw 192.168.80.1を追加し、設定を保存します。
C. インターフェース管理ipv4アドレスを192.168.80.200 255.255.255.0に設定し、スタティックルートを0.0.0.0.0.0.0.0 gwを192.168.80.1に設定し、設定を保存します。
D. インターフェース管理ipv4アドレス192.168.80.200マスク長24スタティックルートのデフォルトネクストホップゲートウェイアドレス192.168.80.1を追加し、設定を保存します。
Answer: A (メーッセージを残す**)**
Check Point アプライアンスに最初にインストールした後、IP を 192.168.80.200/24 に、デフォルト ゲートウェイを 192.168.80.1 に設定するために使用できるコマンドは次のとおりです。
set interface Mgmt ipv4-address 192.168.80.200 mask-length 24。このコマンドは、管理インターフェイスの IPv4 アドレスとサブネット マスクを設定します。
set static-route default nexthop gateway address 192.168.80.1 on。このコマンドは、IPv4ルーティングのデフォルトゲートウェイを設定します。
save config。このコマンドは設定の変更を保存します。

最新問題: **9**
空欄を埋めてください: 各クラスターには、少なくとも _____ 個のインターフェースが必要です。
A. 5
B. 2
C. 3

D. 4
Answer: C (メーッセージを残す**)**
各クラスタには、少なくとも3つのインターフェースが必要です4。これらは次のとおりです。
クラスタ メンバー間の状態情報を同期するための非同期インターフェイス。
クラスタ制御パケットを送受信するためのクラスタ インターフェイス。
クラスタを通過する通常のトラフィックを処理するための本番環境インターフェース4. Check Point R80.20 - クラスタファイアウォールの設定方法 - 初回セットアップ

最新問題**: 10**
脅威抽出と脅威エミュレーションの主な違いは何ですか?
A. 脅威エミュレーションはファイルを配信せず、完了するまでに3分以上かかります
B. 脅威抽出は常にファイルを配信し、完了まで1秒もかかりません
C. 脅威エミュレーションは、完了に1秒もかからないファイルを配信することはありません。
D. 脅威の抽出はファイルを配信せず、完了するまでに3分以上かかります
Answer: B (メーッセージを残す**)**
正解はBです。脅威抽出は常にファイルを配信し、完了まで1秒もかかりません2。脅威抽出は、ファイルから悪用可能なコンテンツを削除し、クリーンで安全なファイルをユーザーに配信します2。脅威エミュレーションは、サンドボックス環境でファイルを分析し、悪意のあるファイルか無害なファイルかを判定します2。脅威エミュレーションは、ファイルのサイズと複雑さによっては、完了までに3分以上かかる場合があります2。Check Point R81 脅威対策管理ガイド

最新問題**: 11**
Check Point製アプライアンスではオンラインアクティベーションが利用可能です。管理者はオンラインアクティベーションをどのように利用しますか？
A. オンライン アクティベーション ツールを自動的に起動するには、SmartConsole から SmartLicensing GUI ツールを起動する必要があります。
B. ファイアウォールがインターネットにアクセスでき、ドメイン名を解決するための DNS サーバーがある場合は、アクションは必要ありません。
C. Gaia 初回構成ウィザードを使用して、アプライアンスは Check Point ユーザー センターに接続し、必要なライセンスと契約をすべてダウンロードします。
D. cpinfo コマンドは、スイッチ -online-license-activation を使用してファイアウォール上で実行する必要があります。
Answer: C (メーッセージを残す**)**
Check Point製アプライアンスでは、オンラインアクティベーションをご利用いただけます。管理者はGaia初回設定ウィザードを使用してオンラインアクティベーションを行います。アプライアンスはCheck Pointユーザーセンターに接続し、必要なライセンスと契約をすべてダウンロードします。この方法を使用するには、インターネットアクセスと有効なユーザーセンターアカウントが必要です。
[Check Pointライセンスおよび契約操作ユーザーガイド]、[Check Point R81 Gaiaインストールおよびアップグレードガイド]

最新問題**: 12**
ルール ベースに変更が加えられた場合、変更を適用するために _____ することが重要です。
A. データベースを公開する
B. ポリシーを有効にする

C. インストールポリシー
D. 変更を保存
Answer: A (メーッセージを残す**)**
ルールベースに変更を加えた場合は、変更を適用するためにデータベースを公開することが重要です。データベースを公開すると、変更内容がデータベースに保存され、他の管理者が利用できるようになります。ポリシーをインストールすると、セキュリティゲートウェイに変更が適用されます。Check Point R81 セキュリティ管理ガイド、[Check Point R81 SmartConsole R81 解決済みの問題]、[Check Point R81 ファイアウォール管理ガイド]

最新問題**: 13**
Identity Awareness を使用すると、どの 3 つの項目に基づいてネットワーク アクセスと監査を簡単に構成できますか?
A. クライアントマシンの IP アドレス。
B. ネットワークの場所、ユーザーの ID、およびマシンの ID。
C. ログ サーバーの IP アドレス。
D. ゲートウェイ プロキシ IP アドレス。
Answer: (解答を表示する**)**
Identity Awareness は、管理者が IP アドレスだけでなく、ユーザーやマシンの ID に基づいてアクセスルールを定義できるブレードです。Identity Awareness を使用すると、ネットワークの場所、ユーザーの ID、マシンの ID という 3 つの項目に基づいて、ネットワークアクセスと監査を簡単に設定できます。ネットワークの場所とは、トラフィックの送信元または送信先のネットワークセグメントを指します。ユーザーの ID とは、トラフィックを開始または受信するユーザーのユーザー名またはグループメンバーシップを指します。マシンの ID とは、トラフィックを開始または受信するマシンのホスト名または証明書を指します。[Check Point R81 Identity Awareness 管理ガイド]

最新問題**: 14**
ライセンスを検証し、ライセンスおよび契約リポジトリに追加された新しいライセンスをアクティブ化するために使用されるライセンス機能は何ですか?
A. 検証ツール
B. 検証ライセンス
C. 自動ライセンス
D. 自動ライセンスおよび検証ツール
Answer: D (メーッセージを残す**)**
ライセンスを検証し、ライセンスおよび契約リポジトリに追加された新しいライセンスをアクティブ化するために使用されるライセンス機能は、自動ライセンスおよび検証ツール1、p. 8です。自動ライセンスは、セキュリティ管理サーバーがセキュリティゲートウェイにライセンスを自動的にアタッチできるようにする機能です。検証ツールは、セキュリティ管理サーバーがライセンスと契約の有効性を検証できるようにする機能です2。Check Point CCSA - R81: 模擬試験と解説、Check Point ライセンスおよび契約管理ガイド R81

最新問題**: 15**
セキュリティ ゲートウェイが自身の IP アドレス以外の IP アドレスにログを送信する場合、どの展開オプションがインストールされますか?
A. 分散型
B. スタンドアロン

C. ブリッジ
Answer: A (メーッセージを残す**)**
セキュリティゲートウェイが自身のIPアドレス以外のIPアドレスにログを送信する場合、セキュリティゲートウェイとログサーバが異なるマシンにインストールされていることを意味します。これは分散型展開3の特徴です。したがって、正解はAです。

最新問題**: 16**
FW CLI コマンドを担当するファイアウォール デーモンはどれですか?
A. 転送
B. 大丈夫
C. cpm
D. cpd
Answer: A (メーッセージを残す**)**
正解はAです。fwdデーモンはFW CLIコマンド3を担当します。fwmデーモンは、セキュリティ管理サーバーとGUIクライアント間の通信を処理します。cpmデーモンは、セキュリティ管理サーバーとSmartConsole間の通信を処理します。cpdデーモンは、セキュリティゲートウェイ上の重要なプロセスの状態を監視します。Check Pointファイアウォールのプロセスとデーモン

最新問題**: 17**
UserCheckとは何ですか?
A. メッセージングツールのユーザーがユーザーの資格情報を確認する
B. ユーザーがアクセスしようとしているウェブサイトやアプリケーションについてユーザーに通知するために使用されるコミュニケーションツール
C. ネットワーク上のユーザーを監視するために使用される管理者ツール
D. 新しいユーザーが作成されたときに管理者に通知するために使用される通信ツール
Answer: (解答を表示する**)**
UserCheckは、ユーザーがアクセスしようとしているウェブサイトやアプリケーションに関する情報をユーザーに通知するためのコミュニケーションツールです。管理者はUserCheckを使用して、確認の要求、リスクの通知、アクセスのブロックなど、ユーザーの操作を必要とするアクションを定義できます3、38ページ。UserCheckはメッセージングツール、管理者ツール、通知ツールではありません。Check Point CCSA - R81: 模擬試験と解説、[Check Point UserCheck管理ガイドR81]

最新問題**: 18**
真偽: セキュリティ ゲートウェイ ログの送信先サーバーは、セキュリティ管理サーバーの構成によって異なります。
A. False、ログサーバーはログサーバーの一般プロパティで設定されます
B. Trueの場合、すべてのセキュリティゲートウェイはSmartCenterサーバー構成のログのみを転送します。

C. Trueの場合、すべてのセキュリティゲートウェイはログを自動的にセキュリティ管理サーバーに転送します。
D. False、ログサーバーはセキュリティゲートウェイの一般プロパティで有効になっています
Answer: (解答を表示する**)**
セキュリティ ･ゲートウェイのログの送信先サーバは、セキュリティ管理サーバの設定によって異なります。これは、セキュリティ管理サーバがセキュリティ ･ゲートウェイからログを受信するログサーバを定義するためです。ログサーバは、セキュリティ管理サーバ自体、または専用のログサーバのいずれかになります12。Check Point R81 ログおよびモニタリング管理ガイド、Check Point R81 Quantum セキュリティ ･ゲートウェイ ･ガイド

最新問題**: 19**
UserCheck メッセージの 3 つの種類とは何ですか?
A. 知らせる、尋ねる、そしてブロックする
B. ブロック、アクション、警告
C. 行動、情報提供、質問
D. 質問、ブロック、通知
Answer: A (メーッセージを残す**)**
UserCheckメッセージには、通知、確認、ブロックの3種類があります。通知メッセージはセキュリティイベントをユーザーに通知するもので、ユーザーによる操作は必要ありません。確認メッセージは、ユーザーにアクションを許可するかブロックするかの選択を促します。ブロックメッセージは、ユーザーによるアクションの実行を阻止し、その理由を表示します1。Check Point R81 ログおよびモニタリング管理ガイド

最新問題**: 20**
SICステータス 「不明」は
A. 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すが、信頼されていません。
B. 安全な通信が確立されました。
C. 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。
D. セキュリティ管理サーバーはゲートウェイに接続できますが、SIC を確立できません。
Answer: C (メーッセージを残す**)**
SICステータス 「不明」は、ゲートウェイとセキュリティ管理サーバ間の接続がないことを意味します。これは、ゲートウェイがダウンしているか、到達不能であるか、まだ初期化されていない場合に発生する可能性があります12。Check Point R81セキュリティ管理管理ガイド、無料のCheck Point CCSAサンプル問題と学習ガイド

最新問題**: 21**
空欄を埋めてください: Gaia は _____ の _____ を使用して構成できます。
A. コマンドラインインターフェース; WebUI
B. Gaia インターフェース; GaiaUI
C. WebUI; Gaiaインターフェース
D. GaiaUI; コマンドラインインターフェース
Answer: (解答を表示する**)**

Gaiaは、コマンドラインインターフェース（CLI）またはWebUIを使用して設定できます。CLIはテキストベースのインターフェースで、コマンドやスクリプトを使用してGaiaの設定を構成および管理できます。WebUIはグラフィカルインターフェースで、Webブラウザを使用してGaiaの設定を構成および管理できます。GaiaインターフェースおよびGaiaUIは、Gaia設定ツールを指す有効な用語ではありません。[Gaia管理ガイド]、[Gaia概要]

最新問題: **22**
コマンドラインを使用して OS のイメージを作成するバックアップ方法はどれですか?
A. システムバックアップ
B. 設定を保存
C. 移行
D. スナップショット
Answer: (解答を表示する**)**
Hewlett Packard Enterprise サポートセンター3によると、スナップショットコマンドはコマンドラインを使用してOSのイメージを作成します。スナップショットとは、ディスクパーティションの特定時点のコピーであり、障害や破損が発生した場合にシステムを復元するために使用できます。Hewlett Packard Enterprise サポートセンター

最新問題: **23**
ライセンスのインストールを確認するために使用されるコマンドはどれですか?
A. Cplic ライセンス検証
B. コピー印刷
C. クリック表示
D. Cplic ライセンス
Answer: B (メーッセージを残す**)**
cplic printコマンドは、ライセンスのインストールを確認するために使用されます。インストールされたライセンスとその有効期限を表示します。[Check Point R81 コマンドラインインターフェースリファレンスガイド],Check Point :: Pearson VUE

最新問題: **24**
SmartUpdate によってセキュリティ管理サーバーにインストールされるリポジトリは何ですか?
A. ライセンスとアップデート
B. パッケージリポジトリとライセンス
C. 更新とライセンスと契約
D. ライセンスと契約およびパッケージリポジトリ
Answer: D (メーッセージを残す**)**
SmartUpdate2によるライセンスの管理とインストールによると、SmartUpdateによってセキュリティ管理サーバにインストールされるリポジトリは、『ライセンス＆契約」と『パッケージリポジトリ」の2つです。『ライセンス＆契約」リポジトリには、利用可能なすべてのライセンスと割り当てられたすべてのライセンスが保存されます。『パッケージリポジトリ」には、Check Point Cloudからダウンロードされたパッケージ、またはローカルデバイスからアップロードされたすべてのパッケージが保存されます。SmartUpdateによるライセンスの管理とインストール

最新問題: **25**

セキュア内部通信 (SIC) はどのようなプロセスで処理されますか?
A. CPM
B. HTTPS
C. フォワード
D. CPD
Answer: D (メーッセージを残す)
セキュア内部通信 ‧SIC)は、CPDプロセス3によって処理されます。CPDは、すべてのCheck Pointモジュール上で実行されるCheck Pointデーモンであり、内部ライセンスとSIC操作を処理します。SICは、証明書と暗号化を使用してCheck Pointコンポーネント間の安全な通信を確保するメカニズムです。Check Point R81 セキュリティ管理管理ガイド

最新問題**: 26**
空欄を埋めてください: セキュリティ ゲートウェイ R75 以上では、SIC は暗号化に _____ を使用します。
A. AES-128
B. AES-256
C. DES
D. 3DES
Answer: (解答を表示する)
Security Gateway R75以降では、SICは暗号化にAES-128を使用します。SICはSecure Internal Communication ‧セキュア内部通信)の略で、Security Gateway、Security Management Server、Log ServerなどのCheck Pointコンポーネント間の信頼関係を確立するメカニズムです。SICは証明書を使用してコンポーネント間の通信を認証および暗号化します。AES-128は、128ビットの鍵を使用してデータの暗号化と復号を行う暗号化アルゴリズムです。その他の選択肢は正しくありません。AES-256は256ビットの鍵を使用する暗号化アルゴリズムですが、SICでは使用されません。DESと3DESはそれぞれ56ビットと168ビットの鍵を使用する古い暗号化アルゴリズムですが、SICでは使用されません。[Check Pointコンポーネント間のセキュア内部通信 ‧SIC)]、AES - Wikipedia、DES - Wikipedia、Triple DES - Wikipedia

最新問題**: 27**
脅威防止シグネチャが最後に更新された日時をすぐに確認するために、管理者はどの脅威ツールを使用すればよいですか?
A. 保護
B. IPS保護
C. プロファイル
D. 脅威ウィキ
Answer: B (メーッセージを残す)
脅威シグネチャの詳細4によると、脅威対策シグネチャの最終更新日を素早く確認するには、IPS保護ツールを使用できます。このツールでは、最終更新日時、シグネチャの数、カテゴリが表示されます。脅威シグネチャの詳細

最新問題**: 28**
セキュリティ ゲートウェイでサポートされている NAT の 2 つのタイプは何ですか?
A. 目的地と非表示
B. 非表示と静的
C. 静的およびソース

D. ソースと宛先
Answer: B (メーッセージを残す**)**
セキュリティゲートウェイがサポートするNATには、Hide NATとStatic NATの2種類があります。Hide NATは、複数の送信元IPアドレスを1つのIPアドレス（通常はゲートウェイの外部インターフェース）に変換します。Static NATは、1つの送信元IPアドレスを別のIPアドレス（通常はパブリックIPアドレス）に変換します34。その他のNATは有効なNATの種類ではありません。ネットワークアドレス変換（NAT）、Check Point CCSA - R81：模擬試験と解説

最新問題**: 29**
ログのクエリが非常に高速になった理由を最もよく表す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が2倍になります
B. インデックスエンジンはログをインデックス化し、より高速な検索結果を実現します。
C. SmartConsole は、セキュリティ ゲートウェイから直接結果を照会できるようになりました。
D. 保存されるログの量は、以前のバージョンで通常より少なくなっています
Answer: (解答を表示する**)**
答えはBです。インデックスエンジンがログをインデックス化し、より高速な検索結果を実現しているため、ログのクエリが非常に高速化されているからです。インデックスエンジンはSmart-1アプライアンスのコンポーネントであり、ログのフィールドと値（送信元、送信先、アクション、時刻など）にインデックスを作成します。このインデックスにより、大量のログデータを迅速かつ効率的に検索できます。[Check Point R81 Logging and Monitoring Administration Guide]、[Check Point R81 Indexing Engine]

最新問題**: 30**
Check Point コンポーネント間で信頼が確立された後、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. 信頼関係を再確立しないと、セキュリティゲートウェイのIPアドレスを変更することはできません。
B. 信頼関係を再確立しないと、コマンド ラインでセキュリティ ゲートウェイ名を変更することはできません。
C. セキュリティ管理サーバ名は、信頼関係を再確立しないと SmartConsole で変更できません。
D. セキュリティ管理サーバーのIPアドレスは、信頼関係を再確立しないと変更できません。
Answer: (解答を表示する**)**
答えはAです。セキュリティゲートウェイのIPアドレスを変更するには、セキュア内部通信（SIC）を初期化してセキュリティ管理サーバとの信頼関係を再確立する必要があるためです。コマンドラインでセキュリティゲートウェイ名を変更したり、SmartConsoleでセキュリティ管理サーバ名またはIPアドレスを変更したりする場合は、信頼関係の再確立は必要ありませんが、トポロジの更新とポリシーのプッシュが必要になる場合があります。[Check Point R81 セキュリティ管理管理ガイド]、[Check Point R81 セキュリティゲートウェイ管理ガイド]

最新問題**: 31**
API サーバーのステータスを表示するにはどのコマンドを実行する必要がありますか?
A. CPMステータス
B. APIの再起動
C. APIステータス
D. APIステータスを表示
Answer: D (メーッセージを残す**)**

コマンドapi statusは、APIサーバのステータス（有効かどうか、ポート番号、APIバージョン1など）を表示します。Check Point R81 API リファレンスガイド

最新問題: **32**
GAiAの設定を後で参照できるようにファイルに保存したいのですが、どのコマンドを使用すればよいですか？
A. メモリ <ファイル名> に書き込み
B. show config -f <ファイル名>
C. 設定を保存 -o <ファイル名>
D. 設定を保存 <ファイル名>
Answer: D (メーッセージを残す**)**
正解はDです。save onfiguration <filename>コマンドは、Gaiaの設定を後で参照できるようにファイルに保存します1。その他のコマンドはGaia Clishでは無効です1。Gaia R81.10 管理ガイド

最新問題: **33**
空欄を埋めてください: LDAP サーバーは 1 つ以上の _____ を保持します。
A. サーバーユニット
B. 管理者ユニット
C. アカウント単位
D. アカウントサーバー
Answer: (解答を表示する**)**
LDAPサーバは、1つ以上のアカウントユニットを保持します。アカウントユニットは、Check PointデータベースにおけるLDAPサーバの論理表現です。アカウントユニットは、接続パラメータ、認証方法、およびLDAPサーバから取得されるユーザとグループの情報を定義します。アカウントユニットにより、セキュリティゲートウェイはユーザ認証とID認識のためにLDAPサーバを使用できるようになります。その他のオプションは正しくありません。サーバユニットは、Check PointデータベースにおけるCheck Pointサーバの論理表現です。管理者ユニットは、Check Pointデータベースにおける管理者または管理者グループの論理表現です。アカウントサーバは、Check Pointの用語では有効な用語ではありません。[Check Point R81 Identity Awareness管理ガイド]、[Check Point R81 Security Management管理ガイド]、[Check Point R81 SmartConsole R81解決済みの問題]

最新問題: **34**
VMAC モードが有効になっていることを確認するには、すべてのクラスター メンバーでどの CLI コマンドを実行する必要がありますか? 最適な回答を選択してください。
A. fw ctl set int fwha vmac グローバルパラメータが有効
B. fw ctl get int fwha vmac global param enabled; コマンドの結果は値 1 を返す必要があります

C. cphaprob -a if
D. fw ctl get int fwha_vmac_global_param_enabled; コマンドの結果は値1を返す必要があります
Answer: B (メーッセージを残す)
VMACモードが有効になっていることを確認するには、すべてのクラスタメンバーでコマンドfw ctl get int fwha_vmac_global_param_enabledを実行し、コマンドの実行結果が値11を返すことを確認してください。このコマンドは、VMACモードの有効/無効を制御するグローバルカーネルパラメータfwha_vmac_global_param_enabledの現在の値を表示します。VMACモードは、クラスタの各仮想IPアドレスに仮想MACアドレスを関連付ける機能です。これにより、Gratuitous ARPパケットの必要性が軽減され、フェイルオーバーのパフォーマンスが向上します。1。その他のオプションは正しくありません。オプションAは有効なコマンドではありません。オプションCは、VMACモードではなく、クラスタインターフェースのステータスを表示するコマンドです。2。オプションDは、VMACモードをすべてのインターフェースで有効にするか、非VLANインターフェースのみで有効にするかを制御する、別のグローバルカーネルパラメータfwha_vmac_global_param_enabledの値を表示するコマンドです。1。ClusterXL仮想MAC（VMAC）モードを有効にする方法、cphaprob

最新問題: **35**
次のうち、各ポリシー パッケージで使用できないポリシー タイプはどれですか。
A. アクセス制御
B. 脅威エミュレーション
C. 脅威防止
D. デスクトップセキュリティ
Answer: (解答を表示する)

最新問題: **36**
空欄を埋めてください: 各ポリシー レイヤーの最後に _____ ルールを設定するのがベスト プラクティスです。
A. 明示的なドロップ
B. 暗黙のドロップ
C. 明示的なクリーンアップ
D. 暗黙的なドロップ
Answer: C (メーッセージを残す)
各ポリシーレイヤーの最後に明示的なクリーンアップルールを設定するのがベストプラクティスです。このルールは、レイヤー1の先行ルールのいずれにも一致しないトラフィックをログに記録してドロップします。23ページ。Check Point CCSA - R81: 模擬試験と解説

最新問題: **37**
ステートフル インスペクションの利点ではないものは何ですか?
A. 高性能
B. 優れたセキュリティ
C. ネットワーク層より上のスクリーニングなし
D. 透明性
Answer: C (メーッセージを残す)

ステートフル -インスペクションの利点ではないオプションは、 Rネットワーク層より上のスクリーニングなし」です。ステートフル -インスペクションは、OSI参照モデルの第3層 Rネットワーク）から第7層 Rアプリケーション）までのすべての層でパケットを検査するファイアウォール技術です。ステートフル -インスペクションは、TCPフラグ、シーケンス番号、ポート、アプリケーションプロトコルのチェックなど、ネットワーク層より上のスクリーニングを提供します。その他のオプションは、正当なトラフィックに対して高いパフォーマンス、優れたセキュリティ、そして透明性を提供するため、ステートフル -インスペクションの利点となります。

最新問題**: 38**
空欄を埋めてください: SmartConsole、SmartEvent GUI クライアント、および _____ を使用すると、数十億の統合ログを表示し、優先度付けされたセキュリティ イベントとして表示できます。
A. SmartView Web アプリケーション
B. スマートトラッカー
C. スマートモニター
D. スマートレポーター
Answer: (解答を表示する**)**
SmartConsole、SmartEvent GUIクライアント、SmartView Webアプリケーションは、数十億件の統合ログを表示し、優先度の高いセキュリティイベントとして表示します1。SmartView Webアプリケーションは、SmartEventレポートとダッシュボードにアクセスできるWebベースのインターフェースです2。Check Point R81セキュリティ管理ガイド、Check Point R81 SmartEvent管理ガイド

最新問題**: 39**
CPCA プロセスの目的は何ですか?
A. プロセスのステータスの監視
B. ログの送受信
C. GUIクライアントとSmartCenterサーバー間の通信
D. 証明書の生成と変更
Answer: D (メーッセージを残す**)**
CPCAプロセスの目的は、証明書の生成と変更です。CPCAはCheck Point Certificate Authority チェックポイント証明機関）の略で、セキュリティ管理サーバーまたはログサーバー上で実行されるプロセスです。SICなどのCheck Pointコンポーネント間の内部通信に使用する証明書の作成と管理を担います。[Check Point R81 Quantum Security Management 管理ガイド]、[Check Point R81 Quantum Security Gateway ガイド]

最新問題**: 40**
デフォルトで送信元ポート アドレス変換を有効にする NAT の種類は何ですか?
A. 自動静的NAT
B. 手動隠蔽NAT
C. 自動隠蔽NAT
D. 手動静的NAT
Answer: C (メーッセージを残す**)**
自動Hide NATは、デフォルトで送信元ポートアドレス変換 $IP）を有効にします1。つまり、送信元IPアドレスとポート番号は、別のIPアドレスとポート番号に変換されます。これにより、複数のホストが単一のIPアドレスをアウトバウンド接続で共有できるようになります。Check Point R81ファイアウォール管理ガイド

最新問題: **41**
スマート コンソールの最大帯域幅を監視できるツールはどれですか?
A. ログと監視
B. スマートイベント
C. ゲートウェイとサーバータブ
D. SmartView モニター
Answer: D (メーッセージを残す**)**
SmartView Monitorは、SmartConsole上で最も多くの帯域幅を監視できるツールです。SmartView Monitorは、トラフィック、スループット、接続、CPU使用率、メモリ使用率など、ネットワークとセキュリティのパフォーマンスデータをリアルタイムで表示するグラフィカルツールです。SmartView Monitorを使用することで、帯域幅を最も多く消費しているデバイスを特定し、ネットワークパフォーマンスを最適化できます。[SmartView Monitor]、[ネットワークトラフィックの監視]

最新問題: **42**
IPS-Blade について正しいことは何ですか?
A. R80では、IPSは脅威防止ポリシーによって管理されます。
B. R80のIPSレイヤーでは、可能なアクションは 基本」、 最適化」、 厳密」の3つだけです。
C. R80では、IPS例外を すべてのルール」に適用することはできません。
D. R80では、ジオポリシー例外と脅威防止例外は同じです
Answer: (解答を表示する)
R80では、IPSは脅威防止ポリシー567によって管理されます。脅威防止ポリシーは、IPS、アンチボット、アンチウイルス、および脅威エミュレーションソフトウェアブレード5を用いて、悪意のあるトラフィックからネットワークを保護する方法を定義します。脅威防止ポリシーのIPSレイヤーでは、異なるネットワークセグメントに対してIPSの保護とアクションを設定できます。5。その他のオプションはIPSブレードには当てはまりません。Check Point IPSデータシート、Check Point IPSソフトウェアブレード、Quantum侵入防止システム（IPS）

最新問題: **43**
新しいポリシー レイヤーを作成するときに含まれるデフォルトのレイヤーは何ですか?
A. アプリケーション制御、URLフィルタリング、脅威防止
B. アクセス制御、脅威防止、HTTPS検査
C. ファイアウォール、アプリケーション制御、IPSec VPN
D. ファイアウォール、アプリケーション制御、IPS
Answer: B (メーッセージを残す**)**
新しいポリシーレイヤーを作成する際に含まれるデフォルトのレイヤーは、アクセス制御、脅威防御、HTTPSインスペクションです。アクセス制御は、基本的なファイアウォールルールを定義するレイヤーです。脅威防御は、IPS、アンチウイルス、アンチボットなど、さまざまな種類の攻撃に対する保護を可能にするレイヤーです。HTTPSインスペクションは、暗号化されたトラフィックの検査を可能にするレイヤーです。その他のオプションは、新しいポリシーレイヤーを作成する際に含まれるデフォルトのレイヤーではありません。

最新問題: **44**
TCP/IP モデルはいくつの層で構成されていますか?

A. 2
B. 7
C. 6
D. 4
Answer: D (メーッセージを残す)
TCP/IPモデルは、アプリケーション層、トランスポート層、インターネット層、ネットワークインターフェース層の4層で構成されています1、p. 10。TCP/IPモデルは、アプリケーション層、プレゼンテーション層、セッション層、トランスポート層、ネットワーク層、データリンク層、物理層の7層からなるOSIモデルの簡略版です。Check Point CCSA - R81: 模擬試験と解説、[TCP/IPモデルの説明]

最新問題**: 45**
どの構成要素が、VPN トンネルに暗号化して送信するトラフィックと、クリアテキストで送信するトラフィックを決定しますか?
A. NATルール
B. ルールベース
C. VPNドメイン
D. ファイアウォールトポロジ
Answer: C (メーッセージを残す)
VPNドメイン構成要素は、VPNトンネルに暗号化して送信するトラフィックと、平文で送信するトラフィックを決定します。VPNドメインとは、ゲートウェイとの安全な通信が許可されているホストとネットワークのセットです12。ファイアウォールトポロジ、NATルール、ルールベースは、VPN暗号化の決定に直接影響を与えません。Check Point R81セキュリティゲートウェイ技術管理ガイド、CCSA/CCSE試験対策のヒントとコンテンツ - R80.XとR81.Xの比較 - Check Point CheckMates

最新問題**: 46**
新しいライセンスはいつ生成すればよいですか?
A. 契約ファイルをインストールする前。
B. デバイスのアップグレード後。
C. 既存のライセンスの有効期限が切れると、ライセンスがアップグレードされるか、ライセンスに関連付けられた IP アドレスが変更されます。
D. ライセンスがアップグレードされた場合のみ。
Answer: C (メーッセージを残す)
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た場合、またはライセンスに関連付けられているIPアドレスが変更された場合は、新しいライセンスを生成する必要があります。これらの状況が発生すると、現在のライセンスは無効になり、Check Pointユーザーセンターから新しいライセンスを取得し、Security Management ServerまたはSecurity Gatewayにインストールする必要があります。契約ファイルのインストールやデバイスのアップグレードは、ライセンスの有効性に影響を与えません
12Check Point R81、SmartUpdateによるライセンスの管理とインストール

最新問題: **47**
空欄を埋めてください: 特定の場所との間のトラフィックのポリシーを作成するには、_____ を使用します。
A. DLP共有ポリシー
B. 地理ポリシー共有ポリシー
C. モバイル アクセス ソフトウェア ブレード
D. HTTPS 検査
Answer: B (メーッセージを残す)
答えはBです。Geoポリシー共有ポリシーは、送信元国または送信先国に基づいて、特定の場所との間のトラフィックに関するポリシーを作成するために使用されます。DLP共有ポリシーは、ファイルやデータに機密情報がないか検査することで、データ損失を防止するために使用されます。Mobile Accessソフトウェアブレードは、さまざまなデバイスから企業リソースへの安全なリモートアクセスを提供するために使用されます。HTTPS検査は、暗号化されたWebトラフィックの脅威とコンプライアンスを検査するために使用されます。4Check Point R81 Geoポリシー管理ガイド、[Check Point R81 Data Loss Prevention管理ガイド]、[Check Point R81 Mobile Access管理ガイド]、[Check Point R81 HTTPS検査管理ガイド]

最新問題: **48**
スプーフィング対策に関して正しい記述はどれですか?
A. IPSソフトウェアブレードが有効になっている場合、スプーフィング対策は必要ありません。
B. スプーフィング対策グループを手動で作成する方が安全です
C. スプーフィング対策グループをルーティングテーブルと同期させることがベストプラクティスです。
D. 動的ルーティングを有効にすると、ルーティングが変更されるたびにアンチスプーフィンググループが自動的に更新されます。
Answer: C (メーッセージを残す)
スプーフィング対策に関して正しい記述は、スプーフィング対策グループをルーティングテーブルと同期させることがベストプラクティスであるということです。スプーフィング対策は、攻撃者が偽の送信元IPアドレスを持つパケットを送信することを防ぎます。スプーフィング対策グループは、セキュリティゲートウェイの各インターフェースで想定されるIPアドレスを定義します。ルーティングテーブルが変更された場合は、スプーフィング対策グループもそれに応じて更新する必要があります34。Check Point R81 ClusterXL管理ガイド、ルート定義ネットワーク :スプーフィング対策

最新問題: **49**
Identity Awareness を使用すると、セキュリティ管理者は次のどれに基づいてネットワーク アクセスを構成できますか?
A. アプリケーションの名前、ユーザーのID、マシンのID
B. マシンのID、ユーザー名、証明書
C. ネットワークの場所、ユーザーのID、マシンのID
D. ブラウザベースの認証、ユーザーのID、ネットワークの場所
Answer: C (メーッセージを残す)
Identity Awarenessを使用すると、セキュリティ管理者はネットワークの場所、ユーザーのID、マシンのIDに基づいてネットワークアクセスを構成できます1。これらは、Identity Awarenessがサポートする3つの主要なIDソースです1。Identity Awareness R80.40管理ガイド

最新問題: **50**
IKE フェーズ 2 が正常に完了したことを示すメッセージはどれですか。
A. クイックモード完了
B. アグレッシブモード完了
C. メインモード完了
D. IKEモード完了
Answer: A (メーッセージを残す**)**
クイックモード完了は、IKEフェーズ2が正常に完了したことを示すメッセージです2。IKEフェーズ2は、IKEv1ではクイックモード、IKEv2ではチャイルドSAとも呼ばれます。アグレッシブモードとメインモードは、IKE SAを確立するIKEフェーズ1の一部です。IKEモードはIKEネゴシエーションの有効な用語ではありません。IKEフェーズ2 VPNステータスメッセージの分析方法、IKEv2フェーズ1（IKE SA）とフェーズ2（チャイルドSA）のメッセージ交換、IPsec IKEv1プロトコルの理解

最新問題: **51**
どの構成要素が、VPN トンネルに暗号化して送信するトラフィックと、クリアテキストで送信するトラフィックを決定しますか?
A. ファイアウォールトポロジ
B. NATルール
C. ルールベース
D. VPNドメイン
Answer: (解答を表示する)
VPNドメイン構成要素は、VPNトンネルに暗号化して送信するトラフィックと、平文で送信するトラフィックを決定します。VPNドメインとは、ゲートウェイとの安全な通信が許可されているホストとネットワークのセットです12。ファイアウォールトポロジ、NATルール、ルールベースは、VPN暗号化の決定に直接影響を与えません。Check Point R81セキュリティゲートウェイ技術管理ガイド、CCSA/CCSE試験対策のヒントとコンテンツ - R80.XとR81.Xの比較 - Check Point CheckMates

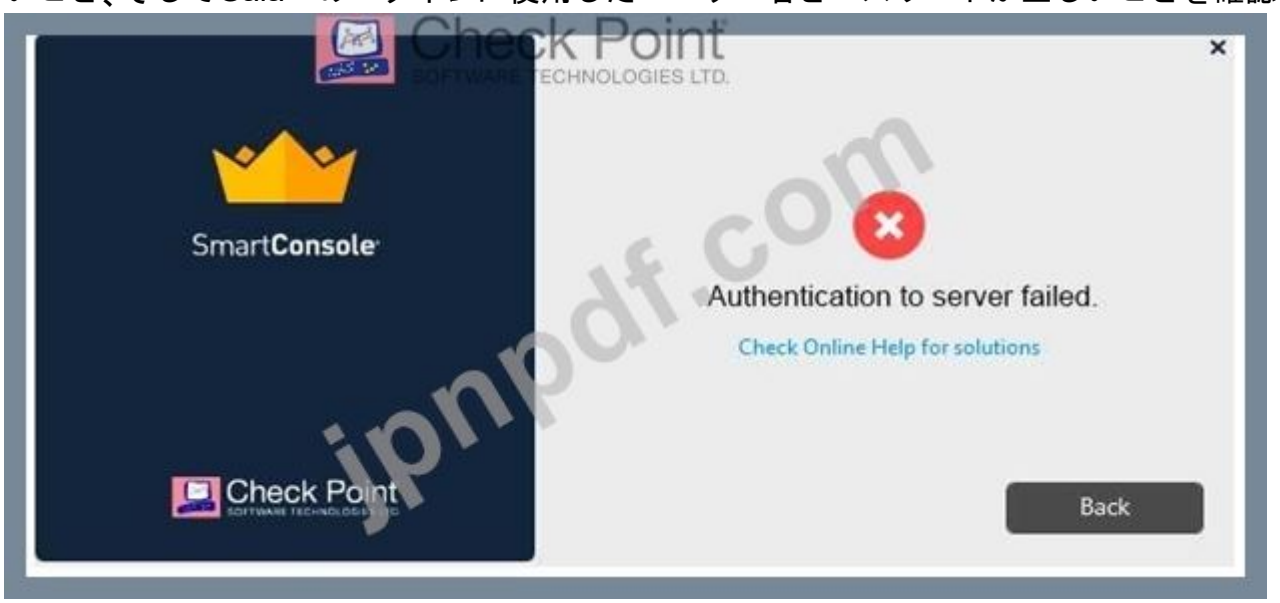
最新問題: **52**
Gaia には Check Point Upgrade Service Engine (CPUSE) が含まれていますが、どのコンポーネントの更新を直接受信できますか?
A. セキュリティ ゲートウェイ (SG) およびセキュリティ管理サーバー (SMS) ソフトウェアと CPUSE エンジン。
B. Gala オペレーティング システムおよび Gaia オペレーティング システム自体のライセンスされた Check Point 製品。
C. CPUSE エンジンと Gaia オペレーティング システム。
D. Gaia オペレーティング システムのみ。
Answer: B (メーッセージを残す**)**
GaiaにはCheck Point Upgrade Service Engine（CPUSE）が搭載されており、GaiaオペレーティングシステムおよびGaiaオペレーティングシステム自体のライセンス対象Check Point製品のアップデートを直接受信できます。CPUSEは、Gaiaプラットフォーム上のソフトウェアアップデートとアップグレードを自動化する高度なツールです。ホットフィックス、ジャンボホットフィックスアキュムレータ、マイナーバージョン、メジャーバージョン、OSアップデートなどのパッケージをダウンロードしてインストールできます。
[CPUSE - Gaiaソフトウェアアップデート（Gaiaソフトウェアアップデートエージェントを含む）]、[Check Point R81]

最新問題: **53**
次のブレードのうち、サブスクリプションベースではないため、定期的に更新する必要がないのはどれですか?

A. アプリケーション制御
B. 脅威エミュレーション
C. アンチウイルス
D. 高度なネットワークブレード
Answer: D (メーッセージを残す**)**
Advanced Networking Blade はサブスクリプション ベースではないため、定期的に更新する必要はありません1011。Advanced Networking Blade は、BGP、OSPF、VRRP、マルチキャスト ルーティングなどの高度なルーティング機能を提供します10。その他のブレードはサブスクリプション ベースであり、Check Point から更新とサポートを受けるには毎年更新する必要があります1012。

最新問題**: 54**
管理者が脅威防止ブレードに対してこれらのファイルをスキャンまたは分析する必要がないことを指定できるように、信頼できるファイルのリストを提供するツールはどれですか。
A. 脅威ウィキ
B. ホワイトリストファイル
C. アプリウィキ
D. IPS保護
Answer: (解答を表示する**)**
ThreatWikiは、管理者が信頼できるファイルのリストをThreat Preventionブレードで提供し、これらのファイルをスキャンまたは分析の対象から除外できるようにするツールです3。ThreatWikiは、Check Pointの顧客、パートナー、研究者など、さまざまなソースからファイルに関する情報を収集するWebベースのサービスです。管理者はThreatWikiを使用して、ファイルのレピュテーションを確認したり、分析用にファイルをアップロードしたり、侵害の兆候（IOC）をダウンロードしたりできます3。ホワイトリストファイル、AppWiki、IPS保護は、信頼できるファイルのリストを提供するツールではありません。Threat Prevention R80.40管理ガイド

最新問題**: 55**
ヴァネッサはGaiaウェブポータルにログインしようとしています。ログインは成功しました。次に、同じユーザー名とパスワードをSmartConsoleに入力しようとしましたが、下のスクリーンショットのようなメッセージが表示されます。サーバーのIPアドレスが正しいこと、そしてGaiaへのログインに使用したユーザー名とパスワードが正しいことを確認しました。



最も可能性の高い理由は何でしょうか?

A. Check Point R80 SmartConsole の認証は以前のバージョンよりもセキュリティが強化されており、Vanessa では R80 SmartConsole 用の特別な認証キーが必要です。正しいキーの詳細が使用されていることを確認してください。
B. Check Point管理ソフトウェアの認証情報は、オペレーティングシステムの認証情報と自動的には一致しません。正しい認証情報を使用していることを確認してください。
C. スーパー管理者が最初にログインし、他のすべての管理者セッションをクリアするまで、Vanessa の SmartConsole 認証は許可されません。
D. Gaia によるチェックは合格しましたが、新しい Threat Prevention コンソールの更新チェックでは Vanessa のユーザー名が許可されていないため、認証に失敗しました。
Answer: B (メーッセージを残す**)**
ヴァネッサの認証失敗の原因として最も可能性が高いのは、SmartConsoleに間違った情報を使用していることです。Check Point Managementソフトウェアの認証情報は、オペレーティングシステムの認証情報と自動的には一致しません。セキュリティ管理サーバーの初期構成時に定義された認証情報、または管理者によって割り当てられた認証情報を使用する必要があります12。その他の原因は、このエラーの原因として有効ではありません。SmartConsoleログイン、Check Point CCSA - R81：模擬試験と解説

最新問題: **56**
セキュリティ ゲートウェイ ソフトウェア ブレードは何に接続する必要がありますか?
A. セキュリティゲートウェイ
B. セキュリティゲートウェイコンテナ
C. 管理サーバー
D. 管理コンテナ
Answer: B (メーッセージを残す**)**
セキュリティゲートウェイソフトウェアブレードは、セキュリティゲートウェイコンテナに接続する必要があります。セキュリティゲートウェイコンテナは、セキュリティゲートウェイソフトウェアを実行する物理マシンまたは仮想マシンを表す論理オブジェクトです。ソフトウェアブレードは、コンテナ内で有効化または無効化できるモジュール式のセキュリティ機能です。ソフトウェアブレードは、ファイアウォール、VPN、IPS、アンチウイルス、アンチボット、アプリケーション制御、URLフィルタリングなどの機能を提供できます。[セキュリティゲートウェイコンテナ]、[ソフトウェアブレード]

最新問題: **57**
悪意のあるファイルのダウンロードをブロックし、マルウェアをホストしていることが知られている Web サイトをブロックするためにオンにできるセキュリティ ブレードはどれですか。
A. アンチボット
B. なし - これにはウイルス対策とボット対策の両方が必要です
C. アンチウイルス
D. なし - これには URL フィルタリングとウイルス対策の両方が必要です。
Answer: C (メーッセージを残す**)**
アンチウイルスは、悪意のあるファイルのダウンロードをブロックするだけでなく、マルウェアをホストしていることが知られているWebサイトをブロックするために有効化できる単一のセキュリティブレードです。アンチウイルスは、ファイルやメールの添付ファイルをスキャンし、ウイルス、ワーム、トロイの木馬、その他のマルウェアを検出します。また、リアルタイムの動的なセキュリティインテリジェンスを提供する協調型ネットワークであるThreatCloudを活用し、未知のマルウェアの挙動に基づいて検出します3。アンチボットは、ボットネット通信を検出してブロックするセキュリティブレードですが、ファイルのスキャンやWebサイトのブロックは行

いません。URLフィルタリングは、管理者がWebアプリケーションへのアクセスを制御できるようにするセキュリティブレードですが、ファイルのスキャンやマルウェアの検出は行いません。

最新問題: **58**
SmartConsole 経由でセキュリティ管理サーバーに初めてログインすると、指紋が次の場所に保存されます。
A. セキュリティ管理サーバーの /home/.fgpt ファイルであり、将来の SmartConsole 認証に使用できます。
B. Windows レジストリは、将来の Security Management Server 認証に使用できます。
C. とにかく、指紋を保存するためにメモリは使用されません。
D. SmartConsole キャッシュは、将来の Security Management Server 認証に使用できます。
Answer: D (メーッセージを残す)
SmartConsole経由でSecurity Management Serverに初めてログインすると、SmartConsoleのキャッシュにフィンガープリントが保存され、今後のSecurity Management Serverの認証に使用されます。フィンガープリントはSecurity Management Serverの一意の識別子であり、そのIDを検証し、中間者攻撃を防ぐために使用されます。SmartConsoleのキャッシュは、クライアントマシン上の一時ファイルと設定を保存するローカルフォルダです。

最新問題: **59**
バックアップは Check Point アプライアンスにどのように保存されますか?
A. /var/log/CPbackup/backups に *.tar として保存されました
B. /var/CPbackup に *tgz として保存されました
C. /var/CPbackup に *tar として保存されます
D. /var/log/CPbackup/backups に *tgz として保存されました
Answer: B (メーッセージを残す)
バックアップはCheck Pointアプライアンスの/var/CPbackup以下に*.tgzファイルとして保存されます。これは、backupコマンドによって作成されるバックアップファイルのデフォルトの保存場所です。したがって、正解はBです。/var/CPbackup以下に*.tgzファイルとして保存されます。

最新問題: **60**
ソフトウェア コンテナーにはどのような種類がありますか?
A. スマートコンソール、セキュリティ管理、セキュリティゲートウェイ
B. セキュリティ管理、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
C. セキュリティ管理、ログと監視、セキュリティポリシー
D. セキュリティ管理、スタンドアロン、セキュリティゲートウェイ
Answer: B (メーッセージを残す)
ソフトウェアコンテナの種類は、セキュリティ管理、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です。ソフトウェアコンテナは、Gaia OS上で実行される仮想環境であり、同じ物理マシン上で複数のCheck Point製品インスタンスを共存させることができます。その他のオプションは、ソフトウェアコンテナの有効な種類ではありません。

最新問題: **61**
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 ユーザーはどれですか?
A. 管理者

B. スーパーユーザー
C. モニター
D. 代替ユーザー
Answer: A (メーッセージを残す**)**
完全な読み取り/書き込み権限を持つデフォルトのGaiaユーザーはadmin3です。adminユーザーは、ネットワーク設定の構成、ソフトウェアアップデートのインストール、ライセンスの管理、スナップショットの作成など、Gaiaシステム上のあらゆる管理タスクを実行できるスーパーユーザーです。adminユーザーは、Gaiaの設定と機能を管理するためのWebベースのインターフェースであるGaiaポータルにもアクセスできます。Check Point R81 Gaia管理ガイド

最新問題**: 62**
HTTPS 検査ポリシーを構成する手順は何ですか?
A. 「管理と設定」> 「ブレード」> 「HTTPS検査」> 「SmartDashboardで構成」に移動します。
B. アプリケーションとURLフィルタリングブレード > 詳細 > HTTPS検査 > ポリシーに移動します。
C. 管理と設定 > ブレード > HTTPS 検査 > ポリシーに移動します
D. アプリケーションとURLフィルタリングブレード > HTTPS検査 > ポリシーに移動します。
Answer: (解答を表示する**)**
HTTPS 検査ポリシーを構成する手順は次のとおりです34。
[管理と設定] > [ブレード] > [HTTPS 検査] > [ポリシー] に移動します。
「新しい HTTPS 検査ルール」をクリックするか、既存のルールを選択して「ルールの編集」をクリックします。
ルールのソース、宛先、アクションを定義します。アクションは、検査、バイパス、または確認のいずれかになります。
「OK」をクリックし、「ポリシーのインストール」をクリックして変更を適用します。HTTPS検査R81管理ガイド、Check Point CCSA - R81：模擬試験と解説

最新問題**: 63**
ルールベースの最上位に、ゲストのワイヤレスインターネットアクセスを許可するルールを作成しました。しかし、ゲストユーザーがインターネットにアクセスしようとしても、利用規約に同意するためのスプラッシュページが表示されず、インターネットにアクセスできません。どうすれば解決できますか？
A. ルール内の「承認」を右クリックし、「詳細」を選択して、「アイデンティティキャプティブポータルを有効にする」をチェックします。
B. ファイアウォールオブジェクトのレガシー認証画面で、「アイデンティティキャプティブポータルを有効にする」をチェックします。
C. グローバルプロパティのキャプティブポータル画面で、「アイデンティティキャプティブポータルを有効にする」をチェックします。
D. セキュリティ管理サーバーオブジェクトで、「アイデンティティログ」ボックスをチェックします。
Answer: A (メーッセージを残す**)**

Identity Captive Portalは、Check Point Identity AwarenessのWebポータルです。ブラウザベースの認証を使用する場合、ユーザーはWebブラウザからログインして認証を行います。2.特定のルールに対してIdentity Captive Portalを有効にするには、ルールの 承認」を右クリックし、 詳細」を選択して 「dentity Captive Portalを有効にする」にチェックを入れます。3. Identity Awareness管理ガイドR80、Checkpoint R80のキャプティブポータルによるIdentity Awareness

最新問題: **64**
Capsule Connect と Capsule Workspace の違いは何ですか?
A. Capsule ConnectはLayer3 VPNを提供します。Capsule Workspaceは使用可能なアプリケーションを備えたデスクトップを提供します。
B. カプセルワークスペースは、あらゆるアプリケーションへのアクセスを提供します。
C. Capsule Connectはビジネスデータの分離を提供します
D. Capsule Connect はクライアントにアプリケーションをインストールする必要はありません。
Answer: (解答を表示する**)**
Capsule Connectは、ユーザーがモバイルデバイスから安全に企業リソースにアクセスできるようにするレイヤー3 VPNを提供します2。Capsule Workspaceは、モバイルデバイス上でビジネスデータとアプリケーションを個人データとアプリケーションから分離する安全なコンテナを提供します3。Capsule Workspaceは、電子メール、カレンダー、連絡先、ドキュメント、Webアプリケーションなどの使用可能なアプリケーションを備えたデスクトップも提供します3。Check Point Capsule Connect、Check Point Capsule Workspace

最新問題: **65**
IPSEC セキュリティ アソシエーション (フェーズ 2) で使用できる暗号化アルゴリズムではないものはどれですか。
A. AES-GCM-256
B. AES-CBC-256
C. AES-GCM-128
Answer: (解答を表示する**)**
答えはBです。AES-CBC-256は、R81のIPsecセキュリティアソシエーション（フェーズ2）でサポートされている暗号化アルゴリズムではないためです。サポートされている暗号化アルゴリズムは、AES-GCM-128、AES-GCM-256、AES-CBC-128、3DES、およびNULL3です。Check Point R81 VPN管理ガイド

最新問題: **66**
どの SmartConsole タブがログを表示し、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集中的に表示しますか?
A. ゲートウェイとサーバー
B. ログとモニター
C. 座席の管理
D. セキュリティポリシー
Answer: B (メーッセージを残す**)**
SmartConsoleのタブは 「ログと監視1」（24ページ）で、ログの表示とセキュリティ脅威の検出を行い、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します。 「ログと監視」タブでは、管理者はセキュリティゲートウェイ、SmartEventサーバー、SmartReporterサーバーなど、さまざまなソースからのログを表示できます。 「ゲートウェイとサーバー」、 設定の管理」、 セキュ

リティポリシー」は、SmartConsoleの他のタブで、それぞれ異なる機能を持っています。Check Point CCSA - R81: 模擬試験と解説、[Check Point SmartConsole R81 ヘルプ]

最新問題: **67**
ステートフル インスペクションはどこで接続をコンパイルして登録しますか?
A. 接続キャッシュ
B. 状態キャッシュ
C. 状態テーブル
D. ネットワークテーブル
Answer: C (メーッセージを残す**)**
ステートフル インスペクションは、接続をコンパイルしてステートテーブルに登録します。ステートテーブルは、セキュリティゲートウェイ上のアクティブな接続とセッションに関する情報を保存するデータベースです。その他のオプションは、接続情報を保存するデータベース名として有効ではありません。

最新問題: **68**
スプーフィング追跡を構成する際、スプーフィングされたパケットが検出された場合に管理者が実行する追跡アクションはどれですか?
A. ログ、SNMPトラップの送信、電子メール
B. パケットをドロップ、アラート、なし
C. ログ、アラート、なし
D. ログ、パケットの許可、電子メール
Answer: C (メーッセージを残す**)**
スプーフィングトラッキングの設定時に選択できるトラッキングアクションは、「ログ」、「アラート」、「なし」です。スプーフィングトラッキングは、偽装された送信元IPアドレスを持つパケットを検出し、SmartView Trackerに記録する機能です。管理者は、スプーフィングされたパケットが検出された場合、「ログのみ」、「ログとアラート」、「何もしない」のいずれかを選択できます。その他のオプションは、この機能では利用できないか、関連性がないため、スプーフィングトラッキングでは有効なトラッキングアクションではありません。

最新問題: **69**
Check Point セキュリティ管理アーキテクチャでは、どのコンポーネントがログを保存できますか?
A. スマートコンソール
B. セキュリティ管理サーバーとセキュリティゲートウェイ
C. セキュリティ管理サーバー
D. SmartConsoleおよびセキュリティ管理サーバー
Answer: B (メーッセージを残す**)**
セキュリティ管理サーバとセキュリティゲートウェイは、Check Pointセキュリティ管理アーキテクチャにおいてログを保存できるコンポーネントです。セキュリティ管理サーバはログをデータベースに保存し、外部のログサーバに転送することもできます。セキュリティゲートウェイは、ログをローカルのバッファまたはローカルログファイルに保存し、セキュリティ管理サーバまたはログサーバに送信することもできます。

最新問題: **70**
ログのクエリが非常に高速になった理由を最もよく表すものを選択してください。
A. 保存されるログの量は以前のバージョンよりも少なくなっています。
B. 新しい Smart-1 アプライアンスでは、物理メモリのインストールが 2 倍になります。
C. インデックス エンジンは、ログにインデックスを付けて、検索結果を高速化します。
D. SmartConsole は、Security Gateway から直接結果を照会するようになりました。
Answer: C (メーッセージを残す**)**
ログのクエリが非常に高速になった理由は、インデックスエンジンがログにインデックスを付けることで検索結果を高速化しているためです。インデックスエンジンは、R81 Management のコンポーネントであり、ログデータのインデックスを作成 維持することで、迅速かつ効率的なログ検索を可能にします4。その他のオプションは、ログのクエリ速度とは関係ありません。保存されるログの量は、ログ保存設定によって異なります。新しい Smart-1 アプライアンスはハードウェア仕様が向上していますが、ログのクエリ処理に直接影響を与えることはありません。SmartConsole は、Security Gateway ではなく、Security Management Server から結果をクエリします。

最新問題: **71**
ステルスルールの目的は何ですか?
A. サーバーの IP アドレスを外部から隠すために使用されるルール。
B. 管理者が任意のデバイスから SmartDashboard にアクセスできるようにするルール。
C. 明示的に許可されていない、ファイアウォール宛てのトラフィックをすべてドロップします。
D. 明示的に許可されていないトラフィックをドロップするためのポリシーの最後のルール。
Answer: (解答を表示する)
ステルスルールの目的は、ファイアウォール宛てのトラフィックのうち、明示的に許可されていないトラフィックをすべて破棄することです1、p. 32。ステルスルールは通常、ルールベースの最上位、つまりセキュリティゲートウェイへのトラフィックを許可する他のルールよりも前に配置されます2、p. 13。ステルスルールは、サーバーのIPアドレスを隠したり、管理者がSmartDashboardにアクセスできるようにしたり、明示的に許可されていないトラフィックを破棄したりするために使用されるものではありません。Check Point CCSA - R81: 模擬試験と解説、156-315.81 Checkpoint試験情報と無料模擬試験

最新問題: **72**
内部ネットワーク10.1.1.0/24、10.2.2.0/24、192.168.0.0/16はインターネットセキュリティゲートウェイの背後にあります。レイヤー2とレイヤー3の設定は正しいと仮定した場合、接続を確立するためにSmartConsoleでどのような手順を実行する必要がありますか？
A. 1. セキュリティ ポリシーで承認ルールを定義します。2. すべての内部ネットワークをゲートウェイの外部 IP の背後に隠すようにセキュリティ ゲートウェイを定義します。3. ポリシーを公開してインストールします。
B. 1. セキュリティ ポリシーで承認ルールを定義します。2. パブリック IP の背後にあるネットワークを NAT するために、各ネットワークに自動 NAT を定義します。3. ポリシーを公開します。
C. 1. セキュリティ ポリシーで承認ルールを定義します。2. パブリック IP の背後にあるネットワークを NAT するために、各ネットワークに自動 NAT を定義します。3. ポリシーを公開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. すべての内部ネットワークをゲートウェイの外部 IP の背後に隠すようにセキュリティゲートウェイを定義します。3. ポリシーを公開します。
Answer: C (メーッセージを残す**)**

インターネット セキュリティ ゲートウェイの背後で接続を機能させるために SmartConsole で実行する必要がある手順は次のとおりです。
セキュリティポリシーで許可ルールを定義します。このルールにより、内部ネットワークからのトラフィックがセキュリティゲートウェイを通過できるようになります。
各ネットワークに自動NATを定義して、パブリックIPアドレスの背後にあるネットワークをNAT変換します。このオプションは、内部ネットワークのプライベートIPアドレスを、ISPルーターによって割り当てられたパブリックIPアドレスに変換します。これにより、内部ネットワークは有効なIPアドレスを使用してインターネットと通信できるようになります。
ポリシーを公開してインストールします。この手順により、セキュリティゲートウェイに加えた変更が適用され、セキュリティルールとNATルールが有効化されます。

最新問題: **73**
SmartEvent は、イベントを識別するために以下のどの手順を使用しませんか?
A. 各イベント定義とログを照合する
B. イベント候補を作成する
C. ログをローカル除外と照合する
D. ログをグローバル除外と照合する
Answer: (解答を表示する**)**
SmartEventがイベントを識別するために使用しない手順は、ログをローカル除外と照合することです。ローカル除外は、SmartLogに関連しないログを除外するために使用され、SmartEventには関連しません12。SmartEventは、イベント定義、イベント候補、およびグローバル除外に基づいてイベントを識別するために、他の手順を使用します3。SmartLog R81管理ガイド、Check Point CCSA - R81：模擬試験と解説、SmartEvent R81管理ガイド、[無料のCheck Point CCSAサンプル問題と学習ガイド]

最新問題: **74**
現在の CPView ページを cpview_"cpview プロセス ID". cap"キャプチャ数" というファイル名形式で保存するために使用されるキーは何ですか?
A. S
B. W
C. C
D. スペースバー
Answer: C (メーッセージを残す**)**
キーCは、現在のCPViewページをcpview_"cpviewプロセスID".cap"キャプチャ数"2というファイル名形式で保存するために使用されます。無料のCheck Point CCSAサンプル問題と学習ガイド

最新問題: **75**
アクセス ロール オブジェクトで構成できないのは次のどれですか。
A. ネットワーク
B. ユーザー
C. 時間
D. マシン
Answer: C (メーッセージを残す**)**

アクセスロールオブジェクトでは、以下の項目は設定できません:時間4. アクセスロールオブジェクトは、ネットワーク、ユーザー、マシン、ロケーション5の4つの基準に基づいてユーザーグループを定義する方法です。ネットワークとは、トラフィックの送信元または送信先を表すIPアドレスまたはネットワークオブジェクトです。ユーザーは、LDAPやRADIUSなどのアイデンティティソースから取得されるユーザーアカウントまたはユーザーグループです。マシンとは、MACアドレスまたは証明書によって識別されるエンドポイントです。ロケーションとは、IPアドレスに基づく地理的な領域です。Check Point R81ファイアウォール管理ガイド、Check Point R81 Identity Awareness管理ガイド

最新問題: **76**
トラフィック ルールで 「アカウンティング」追跡オプションを有効にすると、ログはどのように変化しますか?
A. 関連するトラフィック ログはログ サーバーに転送されます。
B. ログの詳細表示を管理者にメールで送信します。
C. 関連するトラフィック ログは 10 分ごとに更新され、接続で渡されたデータの量が表示されます。
D. 接続しているユーザーに追加情報を提供します。
Answer: (解答を表示する)
アカウンティングトラッキングオプションは、接続を通過するデータ量を監視するために使用されます。トラフィックルールでこのオプションを有効にすると、関連するトラフィックログが10分ごとに更新され、接続で通過したデータ量が表示されます。この情報は、課金や監査の目的で使用できます3。Check Point R81 ログおよびモニタリング管理ガイド

最新問題: **77**
HTTPS 検査ポリシーでは、ルールの 「アクション」列でどのようなアクションを実行できますか?
A. 検査」、「バイパス」
B. 検査」、「バイパス」、「分類」
C. 検査」、「バイパス」、「ブロック」
D. 検出」、「バイパス」
Answer: A (メーッセージを残す)
HTTPSインスペクションポリシーのルールの 「アクション」列で選択できるアクションは、「インスペクション」と 「バイパス」です。「インスペクション」は、HTTPSトラフィックが復号され、アクセス制御ポリシーに従ってインスペクションされることを意味します。「バイパス」は、HTTPSトラフィックが復号されず、インスペクションなしで許可されることを意味します。その他のオプションは、HTTPSインスペクションポリシーでは有効なアクションではありません。

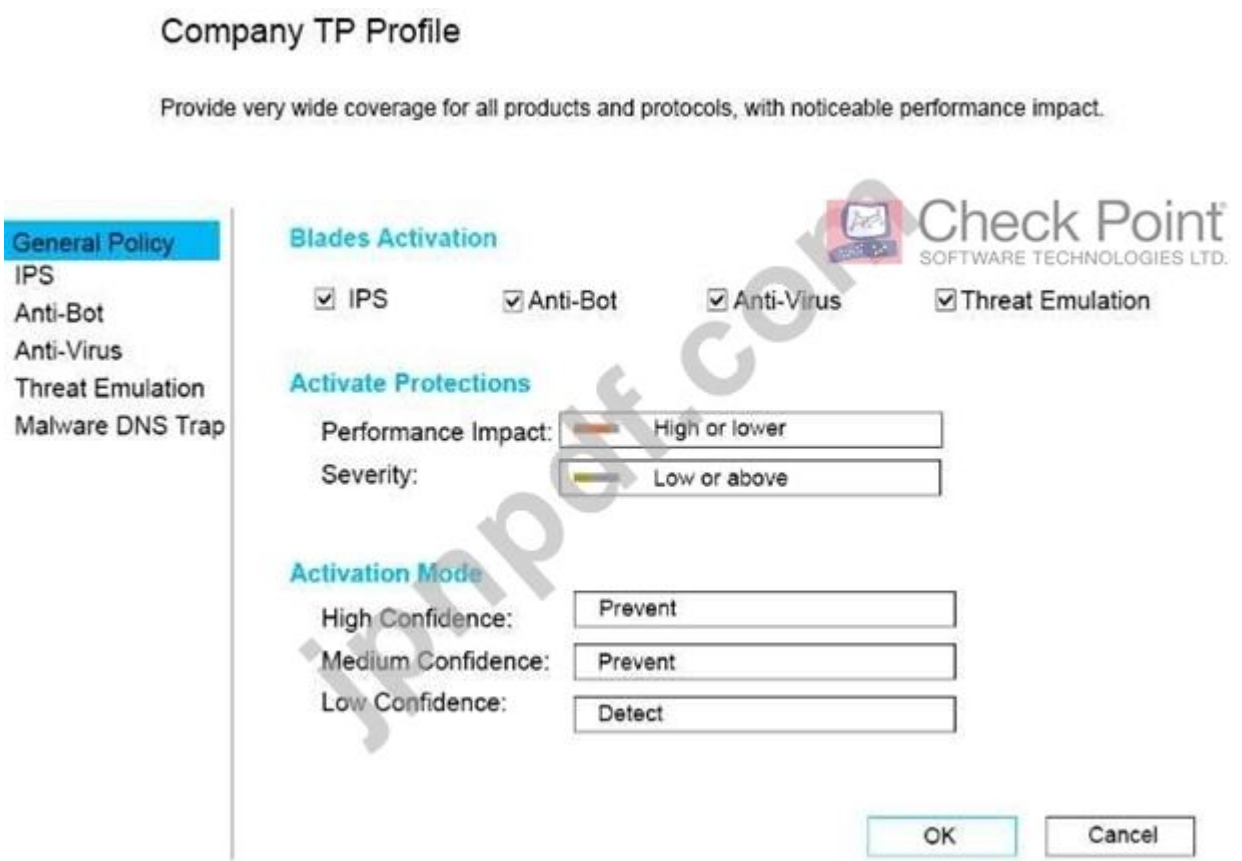
最新問題: **78**
現在のライセンスを表示するには、CLI のどのコマンドを使用すればよいですか?

A. ライセンスビュー
B. fw ctl tab -t ライセンス -s
C. ライセンスを表示 -s
D. コピー印刷
Answer: D (メーッセージを残す)
コマンドcplic printは、インストールされているライセンスとその有効期限をCLI1に表示します。Check Point CLIリファレンスカード

最新問題**: 79**
各ホストが一意のアドレスに変換される 1 対 1 の関係である NAT のタイプは何ですか?
A. ソース
B. 静的
C. 非表示
D. 宛先
Answer: (解答を表示する)
各ホストが一意のアドレスに変換される1対1の関係であるNATのタイプは静的NATです。静的NATは、未登録のIPアドレスを登録済みのIPアドレスに1対1でマッピングします3。つまり、各内部ホストには、それを表す対応する外部アドレスが存在します3。したがって、正解はBです。

最新問題**: 80**
専用の R80 SmartEvent サーバーをインストールする場合、ルート パーティションの推奨サイズはどれくらいですか?
A. 任意のサイズ
B. 20GB未満
C. 10GB以上20GB未満
D. 少なくとも20GB
Answer: D (メーッセージを残す)
正解はDです。専用R80 SmartEventサーバのルートパーティションの推奨サイズは20GB2以上です。20GB未満、または10GB以上20GB未満のサイズは、SmartEventサーバには不十分です。Check Point R80.40 インストールおよびアップグレードガイド

最新問題**: 81**
セキュリティゲートウェイのCPU使用率が100%に達し、トラフィックに問題が発生しています。脅威対策の設定に問題があると思われます。
次の脅威防止プロファイルが作成されました。



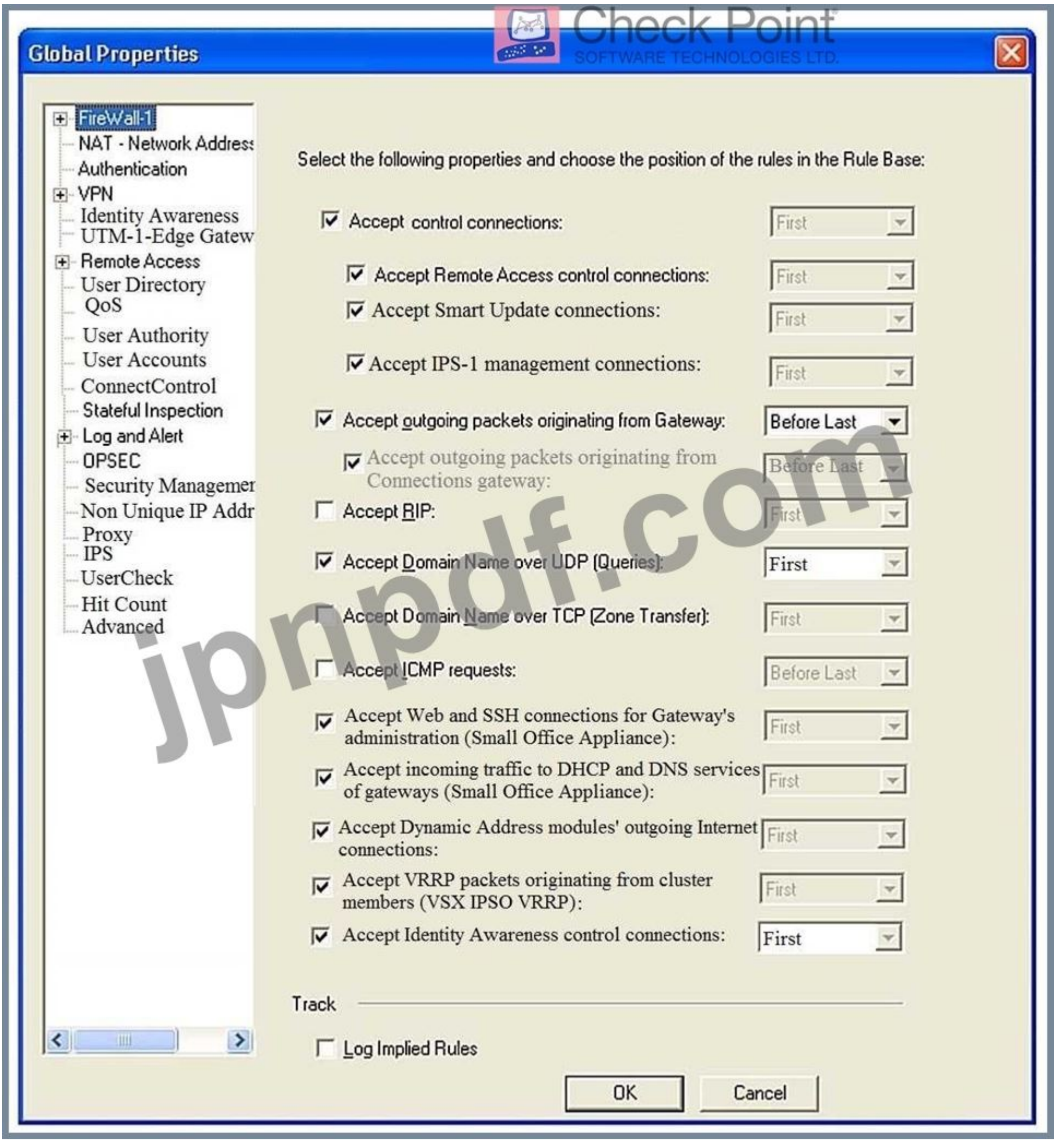
セキュリティを適切なレベルに維持しながら CPU 負荷を下げるには、プロファイルをどのように調整すればよいでしょうか。最適な回答を選択してください。

A. 高い信頼性を低い信頼性に、低い信頼性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. 問題は脅威対策プロファイルにはありません。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. パフォーマンスへの影響を 防止」の信頼度 非常に低い」に設定します。
Answer: B (メーッセージを残す**)**
セキュリティを良好なレベルに維持しながら CPU 負荷を下げるためにプロファイルを調整する最良の方法は、パフォーマンスへの影響を中以下に設定することです。これにより、脅威防止ブレードによって検査されるパケット数が減り、高いレベルの保護が提供されます。高信頼性を低に、低信頼性を非アクティブに設定すると、悪意のある可能性のあるトラフィックが多く許可されるため、セキュリティ レベルが低下します。この問題は、セキュリティ ゲートウェイの CPU 使用率に大きな影響を与える可能性があるため、脅威防止プロファイルに関係している可能性があります。アプライアンスにメモリを追加しても問題は解決しません。この場合、メモリがボトルネックではないからです。パフォーマンスへの影響を非常に低い信頼性に設定して防止すると、検査されるパケットが増え、誤検知の可能性のあるトラフィックがさらにブロックされるため、CPU 負荷が増加します。

最新問題**: 82**
空欄を埋めてください: 認証ルールは _____ に対して定義されています。
A. ユーザーグループ
B. UserCheckを使用しているユーザー
C. 個々のユーザー
D. データベース内のすべてのユーザー
Answer: A (メーッセージを残す**)**

認証ルールは、個々のユーザーではなくユーザーグループに対して定義されます1。認証ルールを定義するには、まずユーザーとグループを定義する必要があります。ユーザーは、Check Pointユーザーデータベース、またはLDAP1などの外部サーバーを使用して定義できます。UserCheckは、ユーザーがセキュリティイベントと対話できるようにする機能です2。個々のユーザーやデータベース内のすべてのユーザーは、認証ルールの定義に有効なオプションではありません。クライアント認証の設定方法、UserCheck

最新問題: **83**
次のグローバル プロパティの設定を検討してください。


Global Properties
Check Point
SOFTWARE TECHNOLOGIES LTD.
FireWall-1
NAT - Network Address
Authentication
VPN
Identity Awareness
UTM-1-Edge Gatew
Remote Access
User Directory
QoS
User Authority
User Accounts
ConnectControl
Stateful Inspection
Log and Alert
OPSEC
Security Managemer
Non Unique IP Addr
Proxy
IPS
UserCheck
Hit Count
Advanced
Select the following properties and choose the position of the rules in the Rule Base:
Accept control connections: First
Accept Remote Access control connections: First
Accept Smart Update connections: First
Accept IPS-1 management connections: First
Accept outgoing packets originating from Gateway: Before Last
Accept outgoing packets originating from Connections gateway: Before Last
Accept RIP: First
Accept Domain Name over UDP (Queries): First
Accept Domain Name over TCP (Zone Transfer): First
Accept ICMP requests: Before Last
Accept Web and SSH connections for Gateway's administration (Small Office Appliance): First
Accept incoming traffic to DHCP and DNS services of gateways (Small Office Appliance): First
Accept Dynamic Address modules' outgoing Internet connections: First
Accept VRRP packets originating from cluster members (VSX IPSO VRRP): First
Accept Identity Awareness control connections: First
Track
Log Implied Rules
OK
Cancel

選択されたオプション「UDP 経由でドメイン名を受け入れる (クエリ)」は、次のことを意味します。
A. UDP クエリは、外部のスプーフィング防止トポロジを持つインターフェースを通じてのみ許可されたトラフィックによって受け入れられ、これは、管理者がセキュリティ ポリシーに記述した最初の明示的なルールの前に実行されます。
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するトラフィックによって受け入れられます。これは、管理者がセキュリティ ポリシーに記述した最初の明示的なルールの前に実行されます。
C. すべてのインターフェースで許可されたトラフィックでは UDP クエリは受け入れられません。これは、管理者がセキュリティ ポリシーに記述した最初の明示的なルールの前に実行されます。
D. すべての UDP クエリは、セキュリティ ポリシーで管理者が記述し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。
Answer: (解答を表示する**)**
「UDP経由のドメイン名（クエリ）を受け入れる」オプションを選択すると、UDPクエリは、外部スプーフィング対策トポロジを持つインターフェースを介してのみ許可されたトラフィックによって受け入れられ、これは管理者がセキュリティポリシーに最初に明示的に記述したルールよりも先に実行されます。このオプションにより、セキュリティゲートウェイは外部ホストからのDNSクエリを受け入れ、内部DNSサーバーに転送できるようになります。クエリは、セキュリティポリシーに明示的に記述されたルールよりも先に適用される暗黙のルールによって受け入れられます。この暗黙のルールは、外部スプーフィング対策グループが定義されているインターフェースからのクエリのみを許可します。Check Point R81 Quantum Security Gatewayガイド、暗黙のルール

最新問題**: 84**
Check Pointソフトウェアライセンスは、ソフトウェアブレードとソフトウェアコンテナの2つのコンポーネントで構成されています。ソフトウェアコンテナには_____種類あります: _____。
A. 2; セキュリティ管理とエンドポイントセキュリティ
B. 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
C. 3つ; セキュリティ管理、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
D. 3つ; 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、ゲートウェイ管理
Answer: C (メーッセージを残す**)**
Check Pointソフトウェアライセンスは、ソフトウェアブレードとソフトウェアコンテナの2つのコンポーネントで構成されています。ソフトウェアコンテナには、セキュリティ管理、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の3種類があります。ソフトウェアブレードは、ソフトウェアコンテナ上で有効化または無効化できる特定のセキュリティ機能です。ソフトウェアコンテナは、1つ以上のソフトウェアブレードを実行するプラットフォームです。セキュリティ管理は、セキュリティゲートウェイのセキュリティポリシーと設定を管理するコンテナです。セキュリティゲートウェイは、ネットワークトラフィックにセキュリティポリシーを適用するコンテナです。エンドポイントセキュリティは、エンドポイントを脅威やデータ損失から保護するコンテナです。Check Pointライセンスおよび契約運用ユーザーガイド

最新問題**: 85**
疑わしいと思われるアクティビティをブロックするために使用されるユーティリティの名前を挙げてください。
A. ペナルティボックス
B. ルールベース内のルールを削除する
C. 不審な活動の監視 (SAM)
D. ステルスルール

Answer: C (メーッセージを残す)
疑わしいアクティビティの監視 $AM)は、疑わしいと思われるアクティビティをブロックするためのユーティリティです。SAMを使用すると、管理者は特定のIPアドレスまたはネットワークオブジェクトからの接続を一定期間ブロックできます3。ペナルティボックスは、ログエントリを過剰に生成するソースからの接続を自動的にブロックするSAMの機能です。ルールベースのドロップルールは、特定の条件に一致するパケットを破棄するファイアウォールアクションです。ステルスルールは、外部ソースからのセキュリティゲートウェイへの直接アクセスをブロックするファイアウォールルールです。

最新問題: **86**
アクセス制御ポリシー レイヤーはどのような 2 つのレイヤーで構成されていますか?
A. URLフィルタリングとネットワーク
B. ネットワークと脅威の防止
C. アプリケーション制御とURLフィルタリング
D. ネットワークとアプリケーションの制御
Answer: B (メーッセージを残す)
アクセス制御ポリシー層を構成する2つの階層は、ネットワーク層と脅威防御層です。ネットワーク層には、セキュリティゲートウェイによるトラフィックの検査と処理方法を定義するルールが含まれています。脅威防御層には、脅威防御ソフトウェアブレードによるトラフィックの検査方法を定義するルールが含まれています。Check Point R81 セキュリティ管理ガイド

最新問題: **87**
Check Point のどのテクノロジーがネットワーク トラフィックを拒否または許可しますか?
A. アプリケーション制御、DLP
B. パケット フィルタリング、ステートフル インスペクション、アプリケーション層ファイアウォール。
C. ACL、サンドブラスト、MPT
D. IPS、モバイル脅威保護
Answer: B (メーッセージを残す)
ネットワークトラフィックを拒否または許可するチェック・ポイントの技術には、パケットフィルタリング、ステートフル・インスペクション、アプリケーション層ファイアウォールがあります 1、15〜16ページ)。パケットフィルタリングは、パケットの送信元アドレスと宛先アドレス、およびポートに基づいて検査する基本的なファイアウォール技術です 2、13ページ)。ステートフル・インスペクションは、ネットワーク接続の状態とコンテキストを追跡し、パケットの内容とシーケンスに基づいて検査する高度なファイアウォール技術です 2、13ページ)。アプリケーション層ファイアウォールは、OSI参照モデルのアプリケーション層で動作し、パケットのアプリケーションプロトコルとデータに基づいて検査するファイアウォール技術です 2、14ページ)。Check Point CCSA - R81：模擬試験と解説、156-315.81 Checkpoint試験情報と無料模擬試験

最新問題: **88**
ルールに適用すると、特定の VPN コミュニティ内の VPN ゲートウェイへのトラフィックを許可するオプションはどれですか。
A. すべての接続 クリアまたは暗号化)
B. すべての暗号化されたトラフィックを受け入れる
C. 特定のVPNコミュニティ
D. すべてのサイト間VPNコミュニティ
Answer: C (メーッセージを残す)

特定のVPNコミュニティ内のVPNゲートウェイへのトラフィックを許可するオプションは、「特定のVPNコミュニティ」です。このオプションを使用すると、ルールで許可するVPNコミュニティを定義できます。「すべての接続（クリアまたは暗号化）」を選択すると、暗号化の有無にかかわらず、すべての宛先へのトラフィックが許可されます。「すべての暗号化トラフィックを受け入れる」を選択すると、VPNコミュニティに関係なく、すべての暗号化された宛先へのトラフィックが許可されます。「すべてのサイト間VPNコミュニティ」を選択すると、VPNコミュニティに関係なく、すべてのサイト間VPNゲートウェイへのトラフィックが許可されます。したがって、正解はC.「特定のVPNコミュニティ」です。

最新問題: **89**
SSL VPN と IPSec VPN の違いは何ですか?
A. IPSec VPNでは、常駐VPNクライアントのインストールは不要です。
B. SSL VPN には常駐 VPN クライアントのインストールが必要です
C. SSL VPNとIPSec VPNは同じです
D. IPSec VPNでは常駐VPNクライアントのインストールが必要で、SSL VPNではブラウザのインストールのみが必要です。
Answer: D (メーッセージを残す**)**
SSL VPNとIPSec VPNの違いは、IPSec VPNではVPNクライアントのインストールが必須であるのに対し、SSL VPNではブラウザのインストールのみで済むことです5。IPSec VPNは、事前共有鍵または証明書を使用してエンドポイントを認証し、ネットワーク層でデータを暗号化します。SSL VPNは、SSL/TLSプロトコルを使用してエンドポイントを認証し、アプリケーション層でデータを暗号化します。Check PointリモートアクセスVPN管理ガイドR81、[無料のCheck Point CCSAサンプル問題と学習ガイド]

最新問題: **90**
次のうち、より安全で推奨される VPN 認証方法はどれですか?
A. MD5
B. 事前共有秘密
C. パスワード
D. 証明書
Answer: D (メーッセージを残す**)**

最新問題: **91**
セキュリティゲートウェイのCPUコアが通常100%使用されており、多くのパケットがドロップされていることに気づきました。現時点ではハードウェアをアップグレードする予算がありません。ドロップを最適化するために、Priority Queuesを使用し、Dynamic Dispatcherを完全に有効化することにしました。どのように有効化すればよいでしょうか？
A. fw ctl multik dynamic_dispatching オン
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. FW CTRL 複数 PQ 有効
Answer: C (メーッセージを残す**)**
ドロップを最適化するには、セキュリティゲートウェイ23でPriority Queuesを使用し、Dynamic Dispatcherを完全に有効化します。Priority Queuesは、セキュリティゲートウェイに負荷がかかり、パケットをドロップする必要がある場合に、トラフィックの一部を優先するメカニズムです。Dynamic Dispatcherは、CPUコアの使用率に基づいて、新しい接続をCoreXL FWインスタンスに動的に割り

当てる機能です。両方の機能を有効にするには、セキュリティゲートウェイ4でコマンドfw ctl multik set_mode 9を実行する必要があります。したがって、正解はC.fw ctl multik set_mode 9です。CoreXL Dynamic Dispatcher - Check Point Software、R80.x / R81.xのファイアウォールPriority Queues - Check Point Software、Dynamic DispatcherとPriority Queuesの個別設定

最新問題: **92**
アイデンティティ認識におけるアイデンティティ共有について説明している記述はどれですか?
A. 管理サーバーはセキュリティゲートウェイとIDを取得し共有できる
B. ユーザーは他のユーザーとIDを共有できます
C. セキュリティゲートウェイは、他のセキュリティゲートウェイとIDを取得し共有することができます。
D. 管理者は他の管理者とIDを共有できます
Answer: (解答を表示する**)**
ID共有は、セキュリティゲートウェイが他のセキュリティゲートウェイとIDを取得 共有し、異なるネットワークセグメントまたはドメイン13にまたがるIDベースのアクセス制御を可能にする機能です。管理サーバー、ユーザー、および管理者は、セキュリティゲートウェイとIDを共有しません。

最新問題: **93**
CLI でクラスタ メンバーを監視するために使用されるコマンドはどれですか。
A. クラスターの状態を表示
B. アクティブなクラスターを表示
C. クラスターを表示
D. 実行中のクラスターを表示
Answer: A (メーッセージを残す**)**
show cluster stateコマンドは、CLIでクラスタメンバーを監視するために使用されます。このコマンドは、クラスタモード、クラスタメンバー、そのステータス、優先度、インターフェースなどの情報を表示します。[ClusterXL管理ガイド]、[Check Point CLIリファレンスカード]

最新問題: **94**
特定のセキュリティ ゲートウェイの IP アドレスに関連付けられており、異なる IP アドレスを持つゲートウェイに転送できない Check Point ライセンスの種類はどれですか。
A. フォーマル
B. 中央
C. 企業
D. ローカル

Answer: D (メーッセージを残す)
Check Pointのライセンスは、セントラルライセンスとローカルライセンスの2種類に分かれています。セントラルライセンスはセキュリティ管理サーバによって管理され、そのサーバが管理する任意のセキュリティゲートウェイに接続できます。ローカルライセンスは特定のセキュリティゲートウェイのIPアドレスに関連付けられており、異なるIPアドレスを持つゲートウェイには移行できません。フォーマルライセンスとコーポレートライセンスは、Check Pointのライセンスの種類ではありません。[Check Point R81 ライセンスおよび契約管理ガイド]

最新問題: **95**
空欄を埋めてください: バックアップと復元は_____を通じて実行できます。
A. SmartConsole、WebUI、または CLI
B. WebUI、CLI、または SmartUpdate
C. CLI、SmartUpdate、または SmartBackup
D. SmartUpdate、SmartBackup、または SmartConsole
Answer: A (メーッセージを残す)
バックアップと復元は、SmartConsole、WebUI、または CLI を通じて実行できます12。これらは、Gaia OS 構成と Security Management Server データベースを保存および復元するシステムのバックアップと復元を実行する方法です1。WebUI、CLI、または SmartUpdate は有効な方法ではありません。SmartUpdate はソフトウェア パッケージとパッチのインストールに使用するものであり、システムのバックアップや復元には使用しないためです3。CLI、SmartUpdate、または SmartBackup は有効な方法ではありません。SmartBackup は、セキュリティ ゲートウェイと VSX クラスターの構成のバックアップと復元を可能にする SmartProvisioning の機能であるため4。SmartUpdate、SmartBackup、または SmartConsole は有効な方法ではありません。SmartConsole はセキュリティポリシーの構成と管理に使用するものであり、システムのバックアップや復元には使用しないためです5。

最新問題: **96**
アクセス ロール オブジェクトの有効な構成画面ではないものはどれですか。
A. ユーザー
B. ネットワーク
C. 時間
D. マシン
Answer: C (メーッセージを残す)
アクセスロールオブジェクトには、ユーザー、マシン、ネットワーク、アイデンティティタグの4つの設定画面があります1、p. 27。時間はアクセスロールオブジェクトの有効な設定画面ではありません。Check Point CCSA - R81: 模擬試験と解説

最新問題: **97**
どの脅威防止プロファイルがサニタイズ技術を使用していますか?
A. クラウド/データセンター
B. 周囲
C. サンドボックス
D. ゲストネットワーク
Answer: B (メーッセージを残す)

脅威対策は、アンチボット、アンチウイルス、IPS、脅威エミュレーション、脅威抽出といった複数のセキュリティブレードを用いて、悪意のある攻撃からネットワークを保護する包括的なソリューションです。脅威対策プロファイルは、各ブレードのアクションと設定を定義し、様々なネットワークセグメントやシナリオに適用できます。境界プロファイルは、サニタイズ技術を用いて悪意のあるファイルやリンクからユーザーを保護する定義済みプロファイルの一つです。サニタイズ技術には、ファイルやWebコンテンツからマルウェアを検出 除去できる脅威エミュレーションブレードと脅威抽出ブレードが含まれます。[Check Point R81 脅威対策管理ガイド]

最新問題: **98**
URLフィルタリングは、ユーザーにウェブ利用ポリシーをリアルタイムで通知する技術を採用しています。その技術の名前は何ですか？
A. ウェブチェック
B. ユーザーチェック
C. ハーモニーエンドポイント
D. URLの分類
Answer: B (メーッセージを残す**)**
URLフィルタリングは、UserCheckと呼ばれる技術を採用しており、ユーザーにWeb利用ポリシーをリアルタイムで通知します。UserCheckは、ファイアウォールがユーザーと対話し、Web利用ポリシーとその違反について通知する機能です。また、ブロックされたWebサイトへのアクセスをリクエストしたり、誤検知を報告したりすることも可能です。UserCheckは、ユーザーがWeb利用ポリシーを理解し遵守するのを支援し、管理者の作業負荷を軽減します。

最新問題: **99**
以下のどの方法が、Management API を使用して通信する方法ではありませんか?
A. 「mgmt_cli」コマンドを使用してAPIコマンドを入力する
B. SmartConsole GUIアプリケーション内のダイアログボックスからAPIコマンドを入力する
C. Gaia のセキュア シェルを使用して API コマンドを入力する (clash)19+
D. Webサービスを使用してHTTP接続経由でAPIコマンドを送信する
Answer: (解答を表示する**)**
正解はDです。Webサービスを使用してHTTP接続経由でAPIコマンドを送信することは、Management APIを使用した通信方法ではありません。3. Management APIはHTTPSプロトコルのみをサポートしており、HTTPはサポートしていません。3. その他の方法は、Management APIを使用した通信方法として有効です。3. Check Point Learning and Training FAQs

最新問題: **100**
Check Point ライセンスを表示および適用するために使用できる GUI ツールはどれですか?
A. cpconfig
B. 管理コマンドライン
C. スマートコンソール
D. スマートアップデート
Answer: D (メーッセージを残す**)**
Check Pointライセンスの表示と適用に使用できるGUIツールはSmartUpdateです。SmartUpdateは、複数のゲートウェイとクラスタのライセンス、ソフトウェアパッケージ、ホットフィックスを管理できる集中管理ツールです12。cpconfig、管理コマンドライ

ン、SmartConsoleはライセンス管理ツールではありません。Check Point R81 SmartUpdate管理ガイド、Check Point CCSA - R81: 模擬試験と解説 | Udemy

最新問題: **101**
Static NAT と Hide NAT の主な違いは何ですか?
A. 静的 NAT は、ネットワークを保護するために着信接続のみを許可します。
B. 静的NATは受信と送信の両方の接続を許可します。Hide NATは送信のみを許可します。
C. 静的NATは送信接続のみを許可します。Hide NATは受信接続と送信接続を許可します。
D. Hide NAT はネットワークを保護するために着信接続のみを許可します。
Answer: B (メーッセージを残す**)**
静的NATと隠蔽NATの主な違いは、静的NATは受信と送信の両方の接続を許可するのに対し、隠蔽NATは送信のみを許可する点です4。静的NATは単一のIPアドレスを別の単一のIPアドレスに変換しますが、隠蔽NATは複数のIPアドレスを単一のIPアドレスに変換します。静的NATは内部サーバーを外部ネットワークに公開するために使用され、隠蔽NATは内部ホストを外部ネットワークから隠蔽するために使用されます。Check Point R81ファイアウォール管理ガイド

最新問題: **102**
セキュア ネットワーク ディストリビュータ (SND) は、どのような点でセキュリティ ゲートウェイの関連機能ですか?
A. SNDは複数のSSL VPN接続を高速化する機能です。
B. SNDはIPSecメインモードの代替であり、3つのパケットのみを使用します。
C. SNDはファイアウォールインスタンス間でパケットを分散するために使用されます
D. SNDは、高速化されたパケットをキャプチャするためのFWモニターの機能です。
Answer: C (メーッセージを残す**)**
セキュアネットワークディストリビュータ（SND）は、セキュリティゲートウェイの機能であり、ファイアウォールインスタンス間でパケットを分散するために使用されます。複数のCPUコアを活用することで、ファイアウォールのパフォーマンスとスケーラビリティを向上させます。その他のオプションはSNDとは関係ありません。[Check Point セキュリティゲートウェイのアーキテクチャとパケットフロー]、[Check Point CCSA の無料サンプル問題と学習ガイド]

最新問題: **103**
脅威抽出の機能について説明しているのは次のうちどれですか?
A. 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
B. 脅威を積極的に検出する
C. 元のコンテンツを含むファイルを配信します
D. アクティブコンテンツを削除した元のファイルのPDFバージョンを配信します
Answer: D (メーッセージを残す**)**
Threat Extractionは、マクロ、埋め込みオブジェクト、スクリプトなどのアクティブコンテンツを削除した元のファイルのPDF版を提供します。これにより、ユーザーは数秒でクリーンで安全なファイルを受け取ることができます12。Check Point SandBlast Zero-Day Protection、Check Point Threat Extraction

最新問題: **104**
空欄を埋めてください: ブラウザベースの認証では、ユーザーを Web ページに送信し、_____ を使用して ID を取得します。

A. キャプティブポータルと透過的Kerberos認証
B. ユーザーチェック
C. ユーザーディレクトリ
D. キャプティブポータル
Answer: A (メーッセージを残す**)**
ブラウザベース認証では、キャプティブポータルと透過的Kerberos認証を使用してIDを取得するために、ユーザーをWebページに誘導します。キャプティブポータルは、ユーザーに認証情報の入力を求めるWebページです。透過的Kerberos認証は、Active Directoryドメインコントローラ2から有効なKerberosチケットを取得したユーザーを自動的に認証する方法です。UserCheckは、ユーザーがセキュリティポリシーを操作できるようにする機能であり、認証方法ではありません。ユーザーディレクトリは、外部ユーザーデータベースと統合するコンポーネントであり、認証用のWebページではありません。キャプティブポータルは、ブラウザベース認証で使用される方法の1つに過ぎないため、それだけでは不十分です。

最新問題**: 105**
空欄を埋めてください: _____ 機能を使用すると、管理者はポリシーを他のポリシー パッケージと共有できます。
A. 同時ポリシーパッケージ
B. 同時ポリシー
C. グローバルポリシー
D. 共有ポリシー
Answer: (解答を表示する**)**
共有ポリシー機能を使用すると、管理者はポリシーを他のポリシーパッケージと共有できます3。これにより、セキュリティ要件が類似する複数のゲートウェイを管理する際の時間と労力を節約できます4。共有ポリシーは、アクセス制御、脅威防御、HTTPS検査レイヤーに適用できます4。Check Point R81 セキュリティ管理管理ガイド、Check Point R81 SmartConsole R81 解決済みの問題

最新問題**: 106**
クリーンアップルールの目的は何ですか?
A. ルールベースで明示的に許可または拒否されていないすべてのトラフィックをログに記録します。
B. コンプライアンスブレードレポートと一致しないポリシーをクリーンアップします
C. データベース内の他のルールと競合する可能性のあるすべてのルールを削除します
D. セキュリティゲートウェイ内の重複したログエントリを排除する
Answer: A (メーッセージを残す**)**
クリーンアップルールの目的は、ルールベース78で明示的に許可または拒否されていないすべてのトラフィックをログに記録することです。クリーンアップルールはルールベースの最後のルールであり、明示的に一致しないトラフィックをドロップしてログに記録するために使用されます97。ルールベースのパフォーマンスを向上させるには、クリーンアップルールでログに記録されるノイズトラフィックをノイズルールに含める必要があります。これにより、ルールベースの上位で一致およびドロップされるようになります8。その他のオプションは、クリーンアップルールの有効な目的ではありません。

GoShiken.com 156-215.82 問題集をゲットする人はこちら: https://www.goshiken.com/CheckPoint/156-215.82-mondaishu.html (**183**30%OFF問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

Valid 156-215.82 Dumps shared by GoShiken.com for Helping Passing 156-215.82 Exam! GoShiken.com now offer the **newest 156-215.82 exam dumps**, the GoShiken.com 156-215.82 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 156-215.82 dumps with Test Engine here: https://www.goshiken.com/CheckPoint/156-215.82-mondaishu.html (**183** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)