CheckPoint.156-215.81.v2024-01-26.q322

試験コード:	156-215.81
試験名称:	Check Point Certified Security Administrator R81
認定資格:	CheckPoint
無料問題数:	322
バージョン:	v2024-01-26
アクセス数:	3261
ページビュー数:	3220
https://www.jpnpdf.com/CheckPoint.156-215.81.v2024-01-26.q322-mondaishu.html	

最新問題: **1**
アンチスプーフィングの内部ネットワーク定義のオプションではないものは次のうちどれですか?
A. インターフェース IP とネットマスクによって定義されたネットワーク
B. ルートベース - ゲートウェイ ルーティング テーブルから派生
C. 特定 - 選択したオブジェクトから派生
D. 未定義
Answer: B (メーッセージを残す**)**

最新問題: **2**
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の違いの最も完全な定義は何ですか?
A. グローバル バージョンでも、インストール前にセッションが保存および公開されます。
B. グローバル ポリシーは、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. ローカル ポリシーは、ネットワーク ポリシーと一緒にマルウェア対策ポリシーをインストールしません。
D. 2 番目のポリシーでは、現在のポリシーと該当するゲートウェイのみのインストールを事前に選択します。
Answer: D (メーッセージを残す**)**
説明
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の違いは、前者は [ポリシーのインストール] ウィンドウで選択されたすべてのポリシーをインストールするのに対し、後者は現在のポリシーのみのインストールを事前に選択することです。該当するゲートウェイの場合 5 。他のオプションは正確な違いではありません。参考資料: ポリシーのインストール、[Check Point CCSA - R81: 模擬テスト]
& 説明]

最新問題: **3**
GAiA を使用する場合、インターフェイス eth 0 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るはずです。この変更をどのように設定しますか?

A. ファイル /etc/sysconfig/netconf.C を編集し、新しい MAC アドレスをフィールド (conf:(conns:(conn:hwaddr ("00:0C:29:12:34:56") に入力します))
B. 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
C. WebUI を開き、[ネットワーク] > [接続] > [eth0] を選択します。新しい MAC アドレスを [物理アドレス] フィールドに入力し、[適用] を押して設定を保存します。
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 (メーッセージを残す)

最新問題**: 4**
Check Point セキュリティ管理アーキテクチャの 3 つの主要コンポーネントは何ですか?
A. GUI クライアント、セキュリティ管理、およびセキュリティ ゲートウェイ
B. SmartConsole、セキュリティ管理、およびセキュリティ ゲートウェイ
C. スマート コンソール、スタンドアロン、およびセキュリティ管理
D. SmartConsole、セキュリティ ポリシー、ログとモニタリング
Answer: B (メーッセージを残す)

最新問題**: 5**
セキュリティ管理者は、新しいユーザー接続が承認されるたびに、クライアント認証の承認タイムアウトを更新する必要があります。これどうやってやるの？更新可能なタイムアウト設定を有効にします。
A. [クライアント認証アクションのプロパティ] 画面の [制限] タブ内。
B. [グローバル プロパティ認証] 画面。
C. ユーザー オブジェクトの認証画面内。
D. ゲートウェイ オブジェクトの認証画面内。
Answer: A (メーッセージを残す)

最新問題**: 6**
Security Gateway が Active Directory ユーザーとコンピュータを識別できるようにする ID 取得方法は次のうちどれですか?
A. Active Directory クエリ
B. ユーザー ディレクトリ クエリ
C. アカウント単位のクエリ
D. ユーザーチェック
Answer: A (メーッセージを残す)
説明
Active Directory クエリは、Security Gateway が Active Directory ユーザーとコンピュータを識別できるようにする ID 取得方法です。Active Directory クエリを使用すると、Security Gateway は、IP アドレス、グループ メンバーシップ、ログイン イベントなどのユーザーおよびコンピュータの情報を Active Directory ドメイン コントローラにクエリできるようになります。
参考資料: Check Point R81 Identity Awareness 管理ガイド、14 ページ。

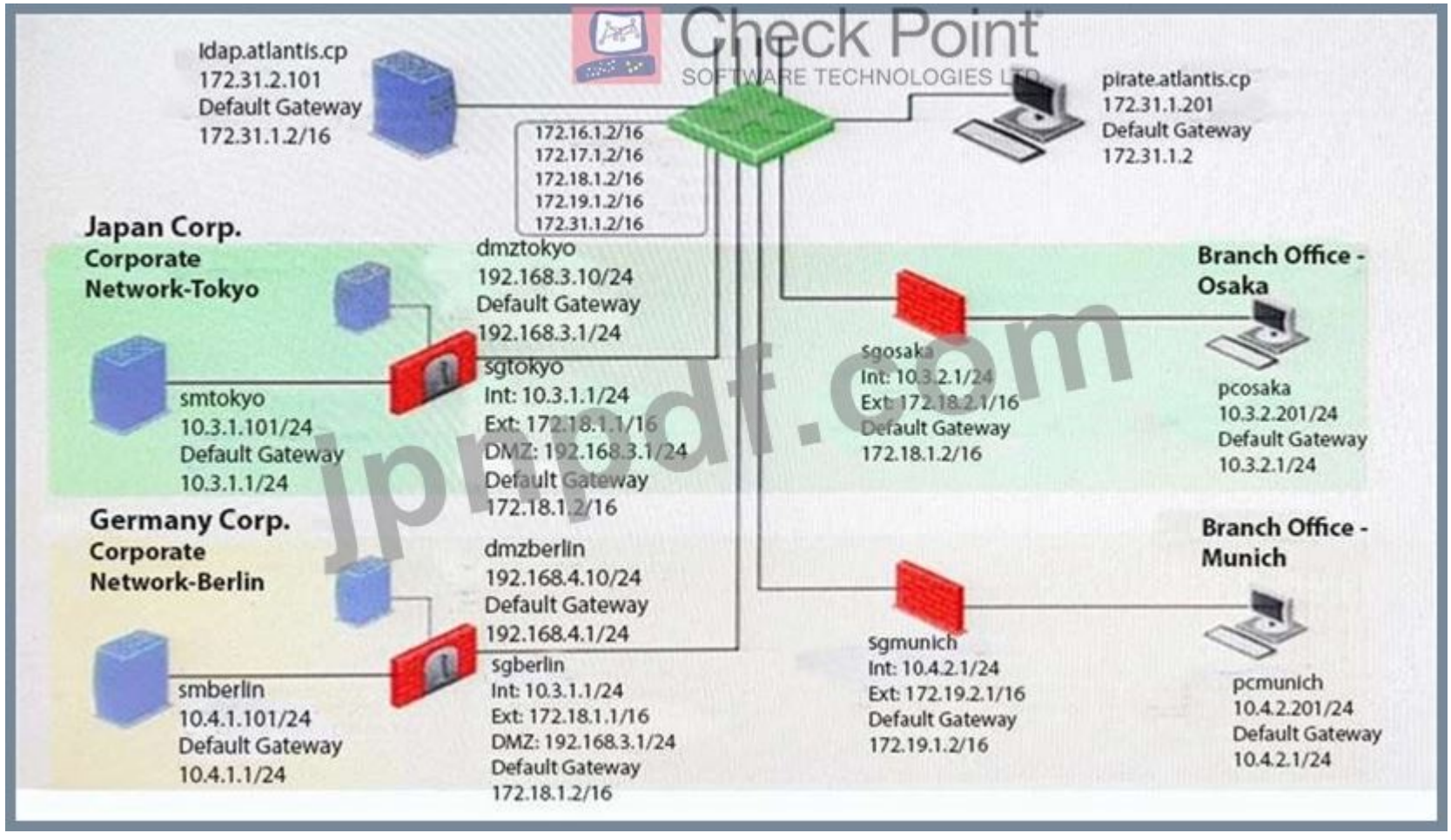
最新問題**: 7**

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. 状態テーブル
C. 状態キャッシュ
D. ネットワーク テーブル
Answer: (解答を表示する**)**

最新問題**: 8**
ID 認識を使用して LDAP 環境でグループベースのアクセスを定義する場合、セキュリティ ポリシーで LDAP グループを表すのに最適なオブジェクト タイプは何ですか?
A. アクセス役割
B. ユーザーグループ
C. SmartDirectory グループ
D. グループ テンプレート
Answer: (解答を表示する**)**
説明
セキュリティ ポリシーで LDAP グループを表す最適なオブジェクト タイプは、アクセス ロールです。アクセス ロール オブジェクトは、リソースまたはサービスにアクセスできるユーザー、マシン、またはネットワークのセットを定義します1、p. 27. アクセス ロール オブジェクトには、そのコンポーネントの 1 つとして LDAP グループを含めることができます2、p. 10. 参考文献: チェックポイント CCSA - R81:
実践テストと解説、Check Point Identity Awareness 管理ガイド R81

最新問題**: 9**
VPN 簡易モードと VPN コミュニティの要素ではないものは次のうちどれですか?
A. 設定チェックボックス 「すべての暗号化されたトラフィックを受け入れる」
B. ルールベースの 「VPN」列
C. 永続的なトンネル
D. ルールベースの 「暗号化」アクション
Answer: D (メーッセージを残す**)**

最新問題**: 10**
smberlin と sgosaka の間で SIC をリセットしたいと考えています。



SmartDashboard で、[sgosaka]、[Communication]、[Reset] を選択します。sgosaka で、cpconfig を起動し、[安全な内部通信] を選択して、新しい SIC アクティベーション キーを入力します。画面に 「SIC は正常に初期化されました」と表示され、メニューに戻ります。接続を確立しようとすると、動作中の接続ではなく、次のエラー メッセージが表示されます。

この動作の理由は何ですか?

A. まず、SmartDashboard で Gateway オブジェクトを初期化する必要があります (つまり、オブジェクトを右クリックし、[Basic Setup] > [Initialize] を選択します)。

B. SIC キーの変更に必要なゲートウェイの再起動が行われませんでした。

C. アクティベーション キーには、ローカライズされたキーボードの異なるキーにある文字が含まれています。したがって、アクティベーションを一致する方法で入力することはできません。

D. まだ cpconfig ユーティリティを使用しているため、ゲートウェイ上のチェック ポイント サービスは再起動されませんでした。

Answer: (解答を表示する**)**

最新問題**: 11**

Endpoint Identity Agent のタイプではないものは次のうちどれですか?
A. カスタム
B. ターミナル
C. フル
D. ライト
Answer: A (メーッセージを残す**)**
説明
Endpoint Identity Agent には、フル、ライト、ターミナルの 3 つのタイプがあります。カスタムは有効な type2 ではありません。
参考資料: 2: Check Point R81 エンドポイント セキュリティ管理ガイド、18 ページ。

最新問題**: 12**
IP ルーティングを変更せずに既存の環境に Security Gateway を追加する導入はどれですか?
A. 分散
B. ブリッジモード
C. リモート
D. スタンドアロン
Answer: (解答を表示する**)**
説明
ブリッジ モード導入では、IP ルーティングを変更せずに既存の環境に Security Gateway を追加するため、答えは B です。ブリッジモードは、Security Gateway インターフェイスに IP アドレスを割り当てる必要のない透過モードです。分散展開は、Security Management Server と Security Gateway が別のマシンにインストールされる展開です。リモート展開は、Security Gateway がリモート サイトにインストールされ、VPN トンネル経由で Security Management Server に接続する展開です。スタンドアロン展開は、Security Management Server と Security Gateway が同じマシンにインストールされる展開です。参考資料: [Check Point R81 ブリッジ モード]、[Check Point R81 展開シナリオ]

最新問題**: 13**
R80 管理にデフォルトで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、サーバーのさまざまな非 HTTP プロトコルに対して信頼性の高い保護を提供します。
B. 最適化 - 最近の攻撃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を優れた保護します。
C. 厳密 - 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 (メーッセージを残す**)**
説明
R80 Management のデフォルトの脅威防御プロファイルは、Basic、Optimized、および Strict1 です。デフォルトでは推奨プロファイルはありません。カスタム プロファイルを作成して 推奨」という名前を付けることができますが、デフォルトでは含まれていません。参考資料: Check Point R81 脅威対策管理ガイド

最新問題**: 14**
空白を埋めてください: Check Point ソフトウェア ライセンスは _____ と _____ で構成されます。

A. ソフトウェア パッケージ。サイン
B. ソフトウェア ブレード。ソフトウェアコンテナ
C. ソフトウェアコンテナ。ソフトウェアパッケージ
D. 署名。ソフトウェアブレード
Answer: B (メーッセージを残す**)**

最新問題**: 15**
内部ルーターは、GRE でカプセル化され、R77 Security Gateway 経由でパートナー サイトに送信される UDP キープアライブ パケットを送信します。GRE トラフィックのルールが ACCEPT/LOG 用に設定されています。キープアライブ パケットは 1 分ごとに送信されますが、SmartView Tracker ログで GRE トラフィックを検索すると、1 日中 (ポリシー インストール後の早朝) のエントリが 1 つしか表示されません。
パートナー サイトは、GRE カプセル化されたキープアライブ 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。
ルーター上で 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 1 分ごとに表示します。
この動作について最も適切な説明は次のうちどれですか?
A. 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 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 分のセッション タイムアウトがあるため、各キープアライブ パケットは、その日の初めにログに記録された元の接続の一部とみなされます。
B. ログ統合プロセスで使用されている LUUID (Log Unification Unique Identification) は破損しています。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。
C. VPN トラフィックであるため、ログ サーバーは GRE トラフィックを適切にログに記録できません。適切なログを有効にするには、パートナー サイトへのすべての VPN 構成を無効にします。
D. ログ設定では、GRE のこのレベルの詳細はキャプチャされません。特定のタイプのトラフィックはこの方法でのみ追跡できるため、ルール追跡アクションを 監査」に設定します。
Answer: A (メーッセージを残す**)**

最新問題**: 16**
アクティブな同時接続の数を確認するにはどのコマンドを使用できますか?
A. すべての接続を表示します
B. 接続を表示
C. すべてを接続します
D. fw ctl pst pstat
Answer: D (メーッセージを残す**)**

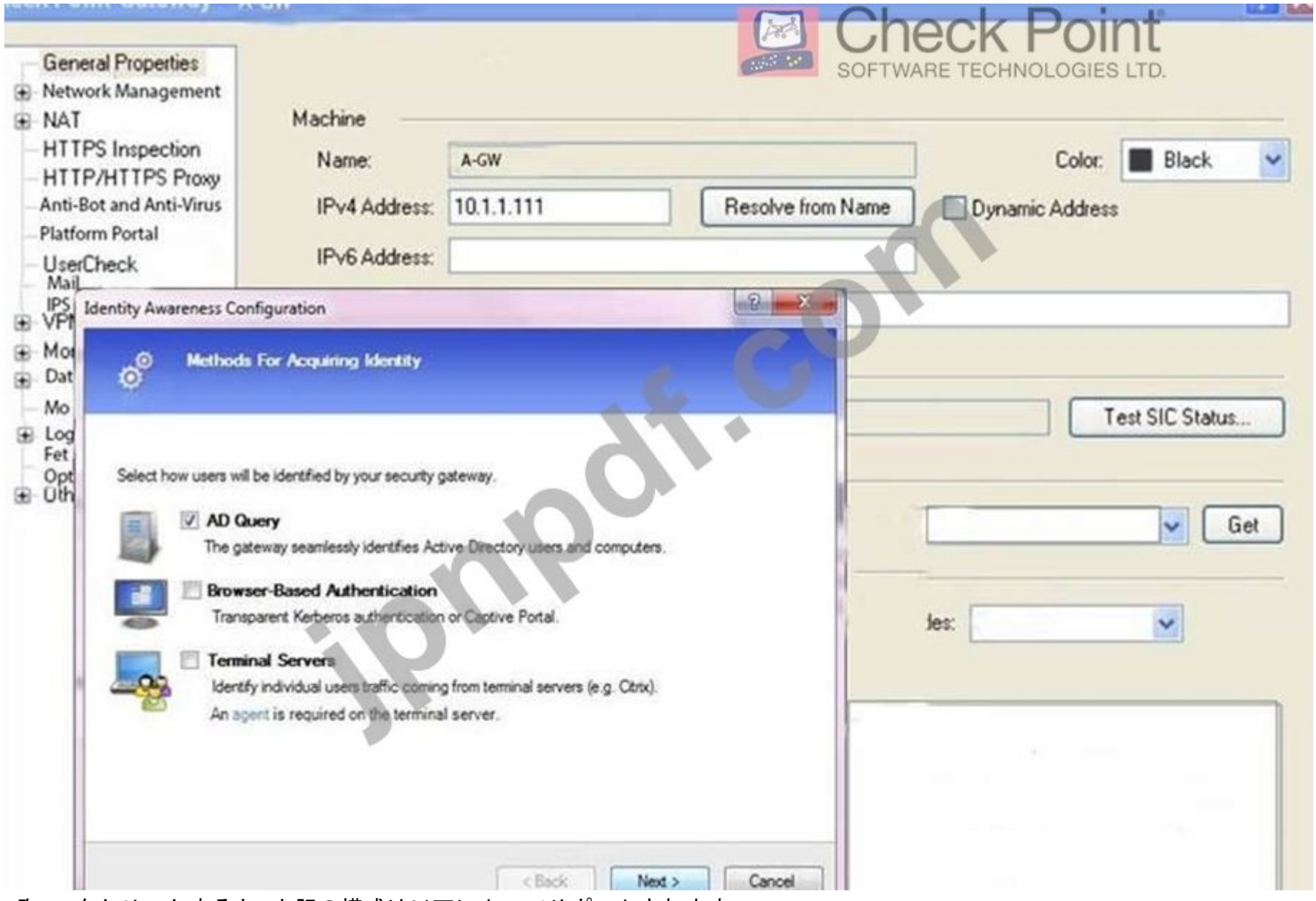
最新問題**: 17**
R80.x SmartConsole の主な機能の 1 つは同時管理です。AdminA、AdminB、AdminC が同じセキュリティ ポリシーを編集していることを考慮すると、不可能なのは次のうちどれですか?
A. AdminC には、ルールが別の管理者による編集のためにロックされていることを示す鍵アイコンが表示されます。
B. AdminA と AdminB は同じルールを同時に編集しています。
C. AdminB には、現在編集中のルールの横に鉛筆アイコンが表示されます。
D. AdminA、AdminB、AdminC は 3 つの異なるルールを同時に編集しています。
Answer: B (メーッセージを残す**)**
説明
R80.x SmartConsole の主な機能の 1 つは同時管理です。これにより、複数の管理者が同じセキュリティ ポリシーを同時に操作できます12。ただし、ルールを編集できるのは一度に 1 人の管理者だけです。AdminA と AdminB が同じルールを同時に編集すると、競合が発生し、変更を保存できなくなります12。したがって、正解は B です。管理者 A と管理者 B は、同じルールを同時に編集しています。

最新問題**: 18**
複数の LDAP サーバーを使用する利点がないものは次のうちどれですか?
A. データベースを含む LDAP サーバーをリモート サイトに配置すると、アクセス時間が短縮されます。
B. 多数のユーザーを複数のサーバーに分散できるようにすることで、区画化を実現します。
C. ユーザーに関する情報は隠されていますが、複数のサーバーに分散されています。
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: C (メーッセージを残す**)**
説明
ユーザーに関する情報は隠蔽されているものの、複数のサーバーに分散されているという記述は、複数の LDAP サーバーを使用する利点ではありません。LDAP (Lightweight Directory Access Protocol) は、ユーザー、グループ、デバイスなどに関する情報を保存する集中ディレクトリ サービスへのアクセスを可能にするプロトコルです。複数の LDAP サーバーを使用すると、アクセス時間の短縮、区画化、高可用性などの利点が得られますが、情報を隠蔽していないこと。ユーザーに関する情報は、複数の LDAP サーバーを使用しても隠蔽されず、複数の LDAP サーバー間で複製または分割されます。レプリケーションは同じ情報がすべての LDAP サーバーにコピーされることを意味し、パーティショニングは異なる情報が異なる LDAP サーバーに保存されることを意味します。どちらの方法も、セキュリティやプライバシーではなく、パフォーマンスと信頼性の向上を目的としています。参考文献: [LDAP Integration]、
[LDAP]

最新問題**: 19**
次のうち正しいのはどれですか?
A. R80 より前のゲートウェイは順序付けされたレイヤーをサポートしていません
B. インライン レイヤーをルール アクションとして定義できます。
C. 順序付けされたポリシーは別のポリシー内のサブポリシーです
D. 1 つのポリシーをインラインまたは順序付けできますが、両方にすることはできません。
Answer: (解答を表示する**)**

最新問題**: 20**
アプリケーション セキュリティと ID 制御を提供する Check Point ソフトウェア ブレードはどれですか?
A. アイデンティティの認識
B. データ損失防止
C. アプリケーション制御
D. URL フィルタリング
Answer: C (メーッセージを残す**)**

最新問題**: 21**
次の図では、管理者が ID 認識を構成しています。



次へ」をクリックすると、上記の構成は以下によってサポートされます。
A. Active Directory 統合に機能する Kerberos SSO
B. キャプティブ ポータルの使用義務
C. ブラウザベースの構成された認証で使用されるポート 443 または 80

D. Active Directory 統合に基づいており、ユーザーに対して完全に透過的な方法で、Security Gateway が Active Directory ユーザーおよびマシンを IP アドレスに関連付けることができます。
Answer: D (メーッセージを残す)

最新問題**: 22**
アクセス ロールにより、ファイアウォール管理者は次に従ってネットワーク アクセスを構成できます。
A. リモート アクセス クライアント。
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. ユーザーとユーザー グループ。
D. 上記のすべて。
Answer: D (メーッセージを残す)
アクセス役割を作成するには:
「アクセスロール」ウィンドウが開きます。
選択した内容は、[ロール 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 エントリを検索したり、リストから選択したりできます。
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。
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Access-Roles.htm

最新問題**: 23**
専用の R81 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. 少なくとも 20GB
B. 10GB以上20GB未満
C. 20GB 未満
D. 任意のサイズ
Answer: A (メーッセージを残す)

最新問題**: 24**
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 として保存されます
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 として保存されます
Answer: (解答を表示する)
説明
バックアップは、Check Point アプライアンスの /var/CPbackup 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場所です。したがって、正解は B です。/var/CPbackup に *.tgz として保存されます。

最新問題**: 25**
HTTPS 検査ポリシーを構成するにはどのような手順を実行しますか?
A. SmartDashboard で [管理と設定] > [ブレード] > [HTTPS 検査] > [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 > [詳細設定] > [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: C (メーッセージを残す**)**
説明
HTTPS 検査ポリシーを設定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。
ルールのソースと宛先を定義します。アクションは、検査、バイパス、または確認のいずれかです。
[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。参考文献: HTTPS インスペクション R81 管理ガイド、Check Point CCSA - R81: 実践テストと解説

最新問題**: 26**
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. HTTP
B. FTP
C. Rログイン
D. SMTP
Answer: D (メーッセージを残す**)**

最新問題**: 27**
ルール ベースの先頭に、ゲスト ワイヤレスによるインターネットへのアクセスを許可するルールが作成されました。ただし、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、サービス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。どうすればこれを修正できますか?

No.	Hits	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	0	Guest Access	GuestUsers	* Any	* Any	* Any	Accept	Log

A. ルール内の [承認] を右クリックし、[詳細] を選択して、[Identity Captive Portal を有効にする] をオンにします。
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、[Identity Captive Portal を有効にする] をオンにします。
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、[ID キャプティブ ポータルを有効にする] にチェックを入れます。
D. Security Management Server オブジェクトで、[ID ログ] ボックスをオンにします。
Answer: A (メーッセージを残す**)**
説明
Identity Captive Portal は、Check Point Identity Awareness Web ポータルであり、ブラウザベースの認証 2 を使用する場合、ユーザーは Web ブラウザで接続してログインと認証を行います。特定のルールに対して Identity Captive Portal を有効にするには、ルール内で

[同意する] を右クリックし、[詳細] を選択して、[Identity Captive Portal を有効にする] をオンにする必要があります3。参考資料: ID 認識管理ガイド R80、Checkpoint R80 のキャプティブ ポータルによる ID 認識

最新問題: **28**
ID 認識に使用される ID ソースではないものは次のうちどれですか?
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 (メーッセージを残す**)**
説明
UserCheck は、アイデンティティ認識に使用されるアイデンティティ ソースではありません。UserCheck は、ユーザーがデータ損失防止または脅威防止のインシデントをトリガーしたときにユーザーと対話できるようにする機能です2。ID 認識は、AD クエリ、アイデンティティ エージェント、ブラウザベースの認証、ターミナル サーバー、キャプティブ ポータル、RADIUS3 などのさまざまな方法を使用して ID を取得します。したがって、正解は B:UserCheck です。

最新問題: **29**
警告オプションではないものは次のうちどれですか?
A. メール
B. 厳戒態勢
C. ユーザー定義のアラート
D. SNMP
Answer: B (メーッセージを残す**)**

最新問題: **30**
ユーザー、グループ、マシンの可視性を提供しながら、ID ベースのポリシーによるアクセス制御も提供する Check Point Software Wade 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: (解答を表示する**)**
説明
Identity Aware は、ユーザー、グループ、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 Check Point ソフトウェア ブレードです。ID 認識を使用すると、管理者は IP アドレスだけではなく、ユーザーまたはマシンの ID に基づいて詳細なアクセス ルールを定義できます。ID 認識により、管理者はユーザーのアクティビティを監視し、ユーザーまたはマシンの ID に基づいてレポートを生成することもできます。

最新問題: **31**
SmartUpdate を使用したユーザー センターとの通信にはどのポートが使用されますか?

A. CPMI200
B. HTTPS443
C. TCP 8080
D. HTTP80
Answer: (解答を表示する**)**

最新問題: **32**
問題のあるホストからの不審な接続が見つかりました。あなたは、問題のあるホストだけでなく、そのネットワーク全体からすべてをブロックすることに決めました。さらに調査する間、これを 1 時間ブロックしたいと考えていますが、ルール ベースにはルールを追加したくありません。どうやってこれを達成しますか?
A. Smart Monitor で不審なアクティビティのルールを作成します。
B. dbedit を使用して、Rule Bases_5_0.fws 構成ファイルにルールを直接追加するスクリプトを作成します。
C. SmartView Tracker の [ツール] メニューから [侵入者をブロック] を選択します。
D. SmartDashboard を使用して一時ルールを追加し、ルールの非表示を選択します。
Answer: (解答を表示する**)**

最新問題: **33**
スプーフィング対策について正しいのはどれですか?
A. 動的ルーティングが有効になっていると、ルーティングが変更されるたびにスプーフィング対策グループが自動的に更新されます。
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. IPS ソフトウェア ブレードが有効な場合、スプーフィング対策は必要ありません
Answer: C (メーッセージを残す**)**

最新問題: **34**
以下のルールをご覧ください。左の列のペンのマークは何を意味しますか?

A. これらのルールは現在のセッションで公開されています。
B. ログインした管理者によってルールが編集されましたが、ポリシーはまだ公開されていません。
C. 現在、別のユーザーがルールの編集をロックしています。
D. 構成ロックが存在します。ロックを取得するには、ペンのシンボルをクリックします。
Answer: B (メーッセージを残す)
説明
左側の列のペン記号は、ログインした管理者によってルールが編集されましたが、ポリシーはまだ公開されていないことを意味します。これは、変更がまだ有効になっていないため、破棄できることを示します。参考資料: ポリシー エディター、変更の公開

最新問題: **35**
Security Gateway 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. Security Gateway 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)
セキュリティ管理およびセキュリティ ゲートウェイ ソフトウェア ブレードは、ライセンスを取得するにはソフトウェア コンテナに接続する必要があります。https://downloads.checkpoint.com/dc/download.htm?ID=11608

最新問題: **36**
ゲートウェイでクラスターのメンバーシップを有効にするためにどのツールが使用されますか?
A. スマートアップデート
B. cpconfig
C. スマートコンソール
D. sysconfig
Answer: B (メーッセージを残す)
説明
ゲートウェイでクラスターのメンバーシップを有効にするために使用されるツールは cpconfig2 です。このツールを使用すると、クラスタ メンバーシップ、管理者名とパスワード、GUI クライアント、Secure Internal Communication (SIC)2 などの Check Point 製品の基本設定を構成できます。参考資料：次世代セキュリティゲートウェイガイド R80

最新問題: **37**
次のチェック ポイント プロトコルのうち、どの 2 つが使用されますか?
A. ELA と CPLOG
B. ELA と CPD
C. FWD および LEA
D. FWD および CPLOG
Answer: C (メーッセージを残す)

最新問題: **38**
Gaia CLI のデフォルトのシェルは cli.sh です。Linux コマンドを実行するには、cli.sh シェルから高度なシェルにどのように変更しますか?
A. cli.sh シェルでコマンド ēnable」を実行します。
B. cli.sh シェルで ēonf t」コマンドを実行します。
C. cli.sh シェルでコマンド ēxpert」を実行します。
D. cli.sh シェルで ēxit」コマンドを実行します。
Answer: (解答を表示する)
説明
Gaia CLI のデフォルトのシェルは cli.sh で、基本的な構成とトラブルシューティング用の限定されたコマンド セットが提供されます。cli.sh シェルからアドバンスト シェル (エキスパート モードとも呼ばれる) に変更して Linux コマンドを実行するには、管理者は cli.sh シェルでコマンド ēxpert」を実行する必要があります。

最新問題: **39**
Gaia OS および Gaia OS にインストールされている Check Point 製品の自動アップデートを可能にするツールはどれですか?
A. CPUSE - チェック ポイント アップグレード サービス エンジン
B. CPAUE - チェック ポイント自動更新エンジン
C. CPDAS - チェック ポイント導入エージェント サービス
D. CPASE - チェック ポイント自動サービス エンジン
Answer: A (メーッセージを残す)

最新問題: **40**
空白を埋めてください: 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: B (メーッセージを残す)
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: **41**
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次のうちどれですか?
A. ソースサーバー
B. ソースネットワーク
C. ソース マシン
D. 送信元ユーザー
Answer: A (メーッセージを残す)

最新問題: **42**
空白を埋めてください: ____ ライセンスでは管理者が接続用のゲートウェイを指定する必要がありますが、
_____ ライセンスは Security Gateway に自動的にアタッチされます。
A. 正式な; 企業
B. ローカル。フォーマル
C. ローカル。中央
D. 中央。地元
Answer: D (メーッセージを残す)
説明
中央ライセンスは、Security Gateway のインストール時に自動的にアタッチされます。ローカル ライセンスでは、管理者が添付ファイル用のゲートウェイを指定する必要があります1、p. 8. 参考文献: Check Point CCSA - R81: 模擬テストと解説

最新問題: **43**
管理者に以下のメッセージが表示されるのはなぜですか?

A. 管理上で作成された新しいポリシー パッケージは、既存のゲートウェイにインストールされます。
B. ゲートウェイで作成された新しいポリシー パッケージは、既存の管理にインストールされます。
C. ゲートウェイ上で作成され、管理に転送された新しいポリシー パッケージは、現在ゲートウェイ上にあるポリシー パッケージによって上書きされますが、ゲートウェイ上の定期的なバックアップから復元できます。
D. 管理とゲートウェイの両方で作成された新しいポリシー パッケージは削除されるため、続行する前に最初にパッケージ化する必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 44**
空白を埋めてください: 特定の場所への、または特定の場所から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. 地域ポリシー共有ポリシー
C. Mobile Access 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**)**
共有ポリシー

 ゼキュリティ ポリシー」の 共有ポリシー」セクションには、ポリシー パッケージに含まれていないポリシーが表示されます。これらはすべてのポリシー パッケージ間で共有されます。
共有ポリシーは、アクセス コントロール ポリシーとともにインストールされます。
ソフトウェアブレード
説明
モバイルアクセス
SmartConsole でモバイル アクセス ポリシーを起動します。リモート ユーザーがモバイル時に電子メール アカウントなどの内部リソースにアクセスする方法を構成します。
DLP
SmartConsole でデータ損失防止ポリシーを起動します。高度なツールを構成して、ネットワークの外に出してはいけないデータを自動的に識別し、漏洩をブロックし、ユーザーを教育します。
地域ポリシー
特定の地理的または政治的な場所との間のトラフィックに関するポリシーを作成します。

最新問題**: 45**
1 ～ 3 年ごとに更新が必要な 艸ブスクリプション ブレード」とみなされるものは次のうちどれですか?
A. ファイアウォール ブレード
B. IPSEC VPN ブレード
C. IPS ブレード
D. アイデンティティ認識ブレード
Answer: (解答を表示する**)**

最新問題**: 46**
正誤問題: 複数の管理者が、書き込み権限を持つ SmartConsole を使用して Security Management Server に同時にログインできます。
A. True、すべての管理者は他の管理者から独立した異なるデータベースで作業します。
B. False。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。
C. True、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。
D. False、書き込み権限でログインできる管理者は 1 人だけです
Answer: C (メーッセージを残す**)**
説明
SmartConsole は、管理者が単一のコンソールから複数の Check Point セキュリティ製品を管理できるようにする統合グラフィカル ユーザー インターフェイスです。複数の管理者が、書き込み権限を持つ SmartConsole を使用して Security Management Server に同時にログインできます。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。ある管理者が行った変更は、公開されるまで他の管理者には表示されません2。参考資料: Check Point R81 SmartConsole R81 ユーザー ガイド

最新問題: **47**
空白を埋めてください: _____情報は 「完全なログ」追跡オプションに含まれていますが、「ログ」追跡オプションには含まれていませんか?
A. アプリケーション
B. データ型
C. ファイル属性
D. 宛先ポート
Answer: (解答を表示する**)**

最新問題: **48**
Secure Internal Communication (SIC) はどのようなプロセスによって処理されますか?
A. CPM
B. HTTPS
C. 前輪駆動
D. CPD
Answer: D (メーッセージを残す**)**
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk97638

最新問題: **49**
別々の管理システムを持つ 2 つのゲートウェイ間の証明書ベースの VPN トンネルには何が必要ですか?
A. 共有シークレットのパスワード
B. 一意のパスワード
C. 共有ユーザー証明書
D. 相互に信頼された認証局
Answer: D (メーッセージを残す**)**
説明
証明書ベースの VPN トンネルの場合、両方のゲートウェイが信頼する認証局 (CA) によって発行された証明書を持っている必要があるため、この答えは正解です1。CA は、ゲートウェイの ID を検証し、その証明書に署名する信頼できるエンティティです2。ゲートウェイは、互いの CA3 を信頼している限り、同じ CA を使用することも、異なる CA を使用することもできます。このようにして、ゲートウェイは証明書を使用して相互に認証し、安全な VPN トンネルを確立できます。
他の回答は、証明書ベースの VPN トンネルと無関係であるか互換性がないため、不正解です。共有秘密パスワードと一意のパスワードは、証明書認証とは異なる方法である事前共有キー (PSK) 認証に使用されます4。PSK 認証は証明書認証に比べて安全性が低く、ブルート フォース攻撃に対して脆弱です。共有ユーザー証明書はゲートウェイ認証ではなく、ゲートウェイ認証とは異なる認証レベルであるユーザー認証に使用されます。ユーザー認証はオプションであり、ゲートウェイ認証に加えて使用して、より詳細なアクセス制御を提供できます。
* P2S VPN ゲートウェイ接続のサーバー設定を構成する - 証明書認証
* VPN 証明書とその仕組み

* 2 つの Check Point ゲートウェイ間に証明書ベースのサイト間 VPN を作成
* Check Point アプライアンスを使用して証明書ベースの VPN をセットアップする方法

最新問題: **50**
セキュリティ ゾーンは、集中管理されているさまざまなゲートウェイからの 1 つ以上のネットワーク インターフェイスのグループです。何がゾーンの一部とみなされますか?
A. ゾーンはネットワーク トポロジに基づいており、インターフェイスの接続先に従って決定されます。
B. セキュリティ ゾーンは Check Point ファイアウォールではサポートされていません。
C. ゾーンに 1 つ以上のサブネットを含めるようにファイアウォール ルールを構成できます。
D. サブネット IP とサブネット マスクによって定義されたローカルの直接接続されたサブネット。
Answer: A (メーッセージを残す**)**
「インターフェース」ウィンドウが開きます。[全般] ペインの [トポロジ] 領域には、インターフェイスがすでにバインドされているセキュリティ ゾーンが表示されます。デフォルトでは、セキュリティ ゾーンはインターフェイスの接続先に従って計算されます。https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Security-Zones.htm

最新問題: **51**
次の状況のうち、新しいライセンスを生成してインストールする必要がないのはどれですか?
A. Security Management または Security Gateway の IP アドレスが変更されました。
B. Security Gateway がアップグレードされています。
C. 既存のライセンスの有効期限が切れます。
D. ライセンスがアップグレードされます。
Answer: (解答を表示する**)**

最新問題: **52**
ログ クエリの結果はどのようなファイル形式にエクスポートできますか?
A. Word ドキュメント (docx)
B. カンマ区切り値 (csv)
C. ポータブル ドキュメント形式 (pdf)
D. テキスト (txt)
Answer: (解答を表示する**)**

最新問題: **53**
次のライセンスのうち、一時的なライセンスとみなされるものはどれですか?
A. 評価とサブスクリプション
B. サブスクリプションと永久
C. プラグアンドプレイ (トライアル) と評価
D. 無期限および試用版
Answer: (解答を表示する**)**

最新問題: **54**
空白を入力してください RADIUS プロトコルはゲートウェイとの通信に_____を使用します
A. UDP
B. 中国共産党
C. TDP
D. HTTP
Answer: A (メーッセージを残す**)**
説明
RADIUS プロトコルは、UDP (User Datagram Protocol) を使用してゲートウェイと通信します。UDP は、データを送受信する前にハンドシェイクや確認を必要としないコネクションレス型プロトコルです2。
参考資料: 2: 『Check Point R81 Identity Awareness 管理ガイド』、14 ページ。

最新問題: **55**
セキュリティ ポリシーを正しく適用するには、Security Gateway に以下が必要です。
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 (メーッセージを残す**)**
説明
セキュリティ ポリシーを正しく適用するには、セキュリティ ゲートウェイがネットワーク トポロジを認識している必要があります。これは、ゲートウェイがどのネットワークとインターフェイスが内部と外部であるか、およびそれらの間でパケットをルーティングする方法を認識していることを意味します。参考文献: [Check Point R81 Security Gateway 技術管理ガイド]、Check Point CCSA - R81: 実践テストと解説

最新問題: **56**
パッケージまたはライセンスを SmartUpdate の適切なリポジトリにアップロードするとき。パッケージまたはライセンスはどこに保存されていますか?
A. Check Point ユーザー センター
B. SmartConsole がインストールされているデバイス
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 (メーッセージを残す**)**

最新問題: **57**
スプーフィング対策を設定する場合、管理者はどの追跡オプションを選択できますか?
A. ログ、アラート、なし
B. ログ、パケットの許可、電子メール
C. パケットのドロップ、アラート、なし
D. ログ、SNMP トラップの送信、電子メール

Answer: (解答を表示する**)**
スプーフ追跡の構成 - スプーフされたパケットが検出されたときに実行される追跡アクションを選択します。
ログ - ログエントリを作成します (デフォルト)
アラート - アラートを表示します
なし - ログや警告を行いません
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Preventing-IP-Spoofing.htm

最新問題**: 58**
次のライセンスのうち、一時的なライセンスとみなされるものはどれですか?
A. 無期限および試用版
B. プラグアンドプレイと評価
C. サブスクリプションと永久
D. 評価とサブスクリプション
Answer:
B
試用版または評価版、さらにはプラグアンドプレイである必要があります (すべて同義語です)。答え B が最良の選択です。

最新問題**: 59**
MyCorp には次の NAT ルールがあります。Alpha 内部ネットワークが Google DNS (8.8.8.8) サーバーにアクセスしようとする場合は、NAT 機能を無効にする必要があります。
この場合何ができるでしょうか?
A. グローバル プロパティの NAT 設定を使用します。
B. VPN コミュニティ内の NAT を無効にする
C. アルファ内部ネットワーク オブジェクトでネットワーク例外を使用します。
D. 手動 NAT ルールを使用して例外を作成します
Answer: (解答を表示する**)**

最新問題**: 60**
SmartView Tracker では、スプーフィング対策によりパケットがドロップされた場合、どのルールが表示されますか?
A. ルール番号の下の空白フィールド
B. ルール 1
C. ルール 0
D. クリーンアップ ルール
Answer: (解答を表示する**)**

最新問題**: 61**
空白を埋めてください: 特定の場所への、または特定の場所から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. 地域ポリシー共有ポリシー

B. Mobile Access ソフトウェア ブレード
C. DLP 共有ポリシー
D. HTTPS 検査
Answer: A (メーッセージを残す**)**

最新問題**: 62**
cli エキスパート モードでクラスターのステータスを確認するコマンドは何ですか?
A. クラスターXLのステータス
B. クラスターXL統計
C. cphaprob 統計
D. FW CTL 統計
Answer: D (メーッセージを残す**)**

最新問題**: 63**
Gaia CLI のデフォルトのシェルは何ですか?
A. モニター
B. CLI.sh
C. 読み取り専用
D. バッシュ
Answer: (解答を表示する**)**
この章では、Gaia コマンド ライン インターフェイス (CLI) について説明します。
CLI のデフォルトのシェルは clish と呼ばれます。

最新問題**: 64**
ステートフル インスペクション ファイアウォールは、接続データを登録し、この情報を編集することによって機能します。情報はどこに保存されますか?
A. システム SMEM メモリ プール内。
B. 状態テーブル内。
C. セッション テーブル内。
D. $FWDIR/conf/ にあるファイアウォール ハード ドライブ上の CSV ファイル内。
Answer: B (メーッセージを残す**)**
説明

ステートフル インスペクション ファイアウォールは、接続データを登録し、この情報を状態テーブルにコンパイルすることによって機能します。状態テーブルは、送信元、宛先、サービス、プロトコル、シーケンス番号、フラグなど、各接続の状態とコンテキストに関する情報を保存するデータ構造です。状態テーブルにより、ファイアウォールは各パケットのヘッダーとペイロードの両方を検査できます。そして、それに応じてセキュリティ ポリシーを適用します。
[ステートフルインスペクション]、[ステートテーブル]

最新問題: **65**
ログのクエリが非常に高速になった理由を最もよく説明するものを選択してください。
A. 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。
B. SmartConsole は、Security Gateway から直接結果をクエリするようになりました。
C. 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。
D. 保存されているログの量は、以前のバージョンよりも減少しています。
Answer: C (メーッセージを残す**)**

最新問題: **66**
Security Gateway がそのログを自身以外の IP アドレスに送信する場合、どの導入オプションがインストールされますか?
A. 分散
B. スタンドアロン
C. ブリッジモード
D. ターゲット
Answer: (解答を表示する**)**
説明
Security Gateway がそのログを自身以外の IP アドレスに送信する場合、それは展開オプションが配布されていることを意味します。分散展開では、Security Management Server と Security Gateway が別のマシンにインストールされます。Security Management Server は、1 つ以上の Security Gateway からログを収集し、それらを一元管理します。スタンドアロン展開では、Security Management Server と Security Gateway が同じマシンにインストールされます。Security Gateway は、自身の IP アドレスにログを送信します。ブリッジ モード導入では、Security Gateway は 2 つのネットワーク セグメント間の透過的なブリッジとして機能し、独自の IP アドレスを持ちません。ターゲットを絞った展開では、Security Gateway は、ゲートウェイ オブジェクトのプロパティで設定されている特定のログ サーバーにログを送信します34 参考資料: パート 4 - Security Gateway のインストール、展開オプション

最新問題: **67**
Sticky Decision Function (SDF) は、次のどれを防ぐために必要ですか? アクティブアクティブ クラスターをセットアップすると仮定します。
A. フェイルオーバー
B. 対称ルーティング
C. 非対称ルーティング
D. スプーフィング対策
Answer: A (メーッセージを残す**)**

最新問題: **68**

サリーは、GAiA で動作するセキュリティ ゲートウェイにインストールしたいホット フィックス アキュムレータ (HFA) を持っていますが、HFA をシステムに SCP できません。彼女は Security Gateway に SSH 接続できますが、SCP ファイルを Security Gateway に送信することはできませんでした。彼女がそうすることができない最も可能性の高い理由は何でしょうか?
A. /etc/scpusers を編集し、標準モードのアカウントを追加する必要があります。
B. sysconfig を実行して SSH プロセスを再起動する必要があります。
C. SCP ファイルの機能を有効にするために cpconfig を実行する必要があります。
D. /etc/SSHd/SSHd_config を編集し、標準モードのアカウントを追加する必要があります。
Answer: (解答を表示する**)**

最新問題**: 69**
各ホストが一意のアドレスに変換される 1 対 1 の関係は、どのタイプの NAT ですか?
A. ソース
B. 静的
C. 非表示
D. 宛先
Answer: B (メーッセージを残す**)**
説明
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。これは、内部ホストごとに、それを表す対応する外部アドレスがあることを意味します3。したがって、正解はBです

最新問題**: 70**
空白を埋めてください: Check Point ソフトウェア ライセンスは、_____ と _____ で構成されます。
A. ソフトウェア ブレード。ソフトウェアコンテナ
B. ソフトウェア パッケージ: 署名
C. 署名。ソフトウェアブレード
D. ソフトウェア コンテナ ソフトウェア パッケージ
Answer: A (メーッセージを残す**)**
説明
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 コンテナで構成されます。ソフトウェア ブレードは、ゲートウェイまたは管理サーバーにセキュリティ機能を提供するモジュール式のセキュリティ機能です。ソフトウェア コンテナは、バンドルとして購入できるソフトウェア ブレードのセットです。
参考資料: Check Point R81 セキュリティ管理管理ガイド、14 ページ。

最新問題**: 71**
Gaia OS および Gaia OS にインストールされている Check Point 製品の自動アップデートを可能にするツールはどれですか?
A. CPASE - チェック ポイント自動サービス エンジン
B. CPAUE - チェック ポイント自動更新エンジン
C. CPDAS - チェック ポイント導入エージェント サービス
D. CPUSE - チェック ポイント アップグレード サービス エンジン

Answer: D (メーッセージを残す)
Check Point Update Service Engine (CPUSE) は、Deployment Agent (DA) とも呼ばれ、Gaia OS 上でソフトウェアを展開するための高度で直感的なメカニズムであり、単一の HotFix (HF)、HotFix Accumulator (Jumbo)、およびメジャーバージョン。https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk92449&js_peid=P-14d3e809b51-10001

最新問題: **72**
クリーンアップ ルールの目的は何ですか?
A. クリーンアップ ルールは何の目的も果たしません。
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 (メーッセージを残す)
これらは、すべてのルール ベースに対して推奨される基本的なアクセス コントロール ルールです。
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。

最新問題: **73**
各ポリシー パッケージで使用できるポリシー タイプは 4 つあります。それらのポリシーの種類は何ですか?
A. アクセス制御、脅威防御、モバイル アクセス、および HTTPS 検査
B. アクセス制御、カスタム脅威防御、自律型脅威防御、および HTTPS インスペクション
C. ポリシー タイプは、アクセス制御、脅威防止、NAT の 3 つだけです。
D. アクセス制御、脅威防止、NAT および HTTPS 検査
Answer: (解答を表示する)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Working-with-Policy-Packages.htm

最新問題: **74**
ネットワーク トラフィックを拒否または許可する Check Point テクノロジーはどれですか?
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)

最新問題: **75**
空白を埋めてください: ポリシー パッケージがインストールされると、_____ はターゲット インストールの Security Gateway にも配布されます。
A. ユーザー データベース
B. ネットワーク データベース

C. SmartConsole データベース
D. ユーザーおよびオブジェクトのデータベース
Answer: D (メーッセージを残す)

最新問題: **76**
Gaia には、削除できないデフォルトのユーザー アカウントが 2 つあります。それらのユーザー アカウントは何ですか?
A. 管理者とデフォルト
B. エキスパートとクリシュ
C. 制御と監視
D. 管理者と監視者
Answer: (解答を表示する)
参照：
トピック=ドキュメント/R80.30/WebAdminGuides/EN/CP_R80.30_Gaia_AdminGuide/198184

最新問題: **77**
ログとモニタリングでは、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どれですか?
A. アカウンティング/抑制
B. 抑制
C. 会計
D. アカウンティング/拡張
Answer: A (メーッセージを残す)

最新問題: **78**
URL フィルタリングは、ユーザーに Web 使用ポリシーをリアルタイムで教育するテクノロジーを採用しています。その技術の名前は何ですか?
A. WebCheck
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: (解答を表示する)
説明

URL フィルタリングは、ユーザーに Web 使用ポリシーをリアルタイムで教育する UserCheck と呼ばれるテクノロジーを採用しています。UserCheck は、ファイアウォールがユーザーと対話し、Web 使用ポリシーとその違反についてユーザーに通知できるようにする機能です。UserCheck を使用すると、ユーザーがブロックされた Web サイトへのアクセスを要求したり、誤検知を報告したりすることもできます。UserCheck は、ユーザーが Web 使用ポリシーを理解して遵守するのに役立ち、管理者の作業負荷を軽減します。

最新問題: **79**
セッションを最もよく表すものを選択してください。
A. ポリシーが Security Gateway にプッシュされると、セッションが終了します。
B. セッションは編集のためにポリシー パッケージをロックします。
C. 管理者が SmartConsole を通じて Security Management Server にログインすると開始され、公開されると終了します。
D. 管理者が SmartConsole で行われたすべての変更を公開すると開始されます。
Answer: (解答を表示する**)**

最新問題: **80**
空白を埋めてください: A(n)_____ルールは管理者によって作成され、指定された基準に基づいてトラフィックを許可またはブロックするように構成されます。
A. インライン
B. 明示的
C. 暗黙的な削除
D. 暗黙的な受け入れ
Answer: B (メーッセージを残す**)**
説明
明示的なルールは管理者によって作成され、指定された基準に基づいてトラフィックを許可またはブロックするように構成されます。明示的なルールはルール ベースに表示され、管理者が変更できます。参考資料: Certified Security Administrator (CCSA) R81.20 コースの概要、12 ページ。

最新問題: **81**
R80 は、次のオペレーティング システムのどれでサポートされていますか。
A. Windows のみ
B. ガイアのみ
C. Gaia、SecurePlatform、および Windows
D. SecurePlatform のみ
Answer: B (メーッセージを残す**)**
説明
R80 は、すべての Check Point アプライアンス、オープン サーバー、および仮想化ゲートウェイ用の Check Point の統合セキュリティ オペレーティング システムである Gaia のみでサポートされています1、p. 10。14. Windows および SecurePlatform は R80 ではサポートされていません。参考資料: Check Point CCSA - R81: 演習テストと説明、[Check Point の学習とトレーニングに関するよくある質問 (FAQ)]

最新問題: **82**

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. ゲートウェイ履歴
C. ゲートウェイのインストール
D. インストール履歴
Answer: D (メーッセージを残す**)**

最新問題**: 83**
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することが知られている Web サイトをブロックできる単一のセキュリティ ブレードはどれですか?
A. 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
B. アンチボット
C. ウイルス対策
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: D (メーッセージを残す**)**

最新問題**: 84**
クラスタ メンバー間の完全な同期は、ファイアウォール カーネルによって処理されます。これにはどのポートが使用されますか?
A. UDP ポート 265
B. TCP ポート 265
C. UDP ポート 256
D. TCP ポート 256
Answer: (解答を表示する**)**
説明
クラスタ メンバー間の完全な同期に使用されるポートは、TCP ポート 2654 です。このポートは、接続テーブル、NAT テーブル、VPN キーなどの同期データを送受信するためにファイアウォール カーネルによって使用されます4。UDP ポート 8116 は、クラスタ メンバー間の内部通信にクラスタ制御プロトコル (CCP) によって使用されます4。参考資料: ゲートウェイ クラスターの動作シナリオと障害シナリオで、クラスター制御プロトコルはどのように機能しますか?

最新問題**: 85**
TCP/IP モデルのトランスポート層は何を担当しますか?
A. 宛先に到達するために、さまざまなルートに沿ってパケットをデータグラムとして転送します。
B. 2 つのホスト間のデータ フローを管理し、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あらゆる側面を扱い、さまざまな種類のネットワークに接続します。
Answer: B (メーッセージを残す**)**
説明

TCP/IP モデルのトランスポート層は、パケットが正しく組み立てられてターゲット アプリケーションに配信されるように、2 つのホスト間のデータ フローを管理する役割を果たします。また、エラーの検出と修正、フロー制御、多重化も提供します。トランスポート層は、TCP や UDP などのプロトコルを使用します。
参考文献: Check Point セキュリティ エンジニアリング スタディ ガイド、p. 10-11

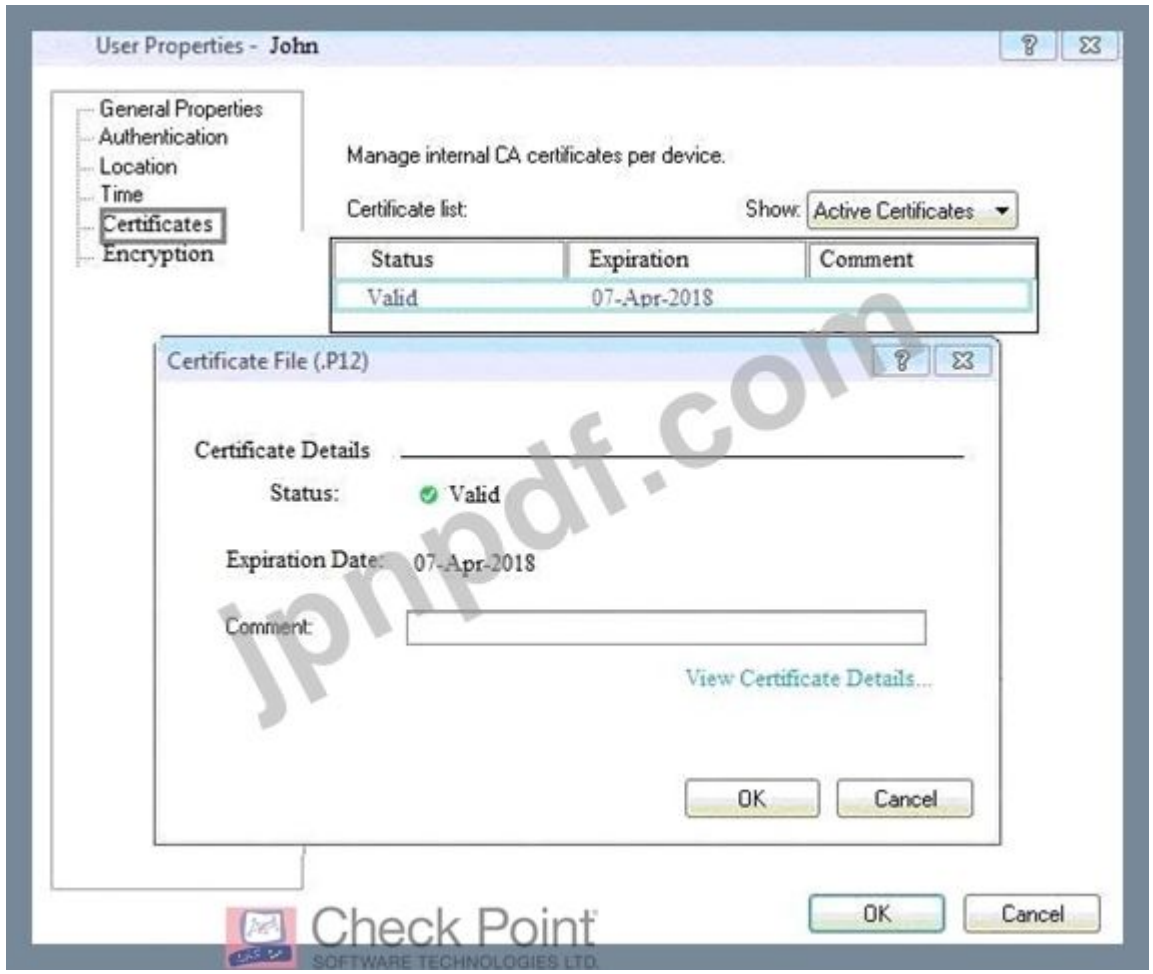
最新問題: **86**
Core Protection はどのポリシーの一部としてインストールされますか?
A. アクセス制御ポリシー。
B. デスクトップ ファイアウォール ポリシー
C. モバイル アクセス ポリシー。
D. 脅威防止ポリシー。
Answer: (解答を表示する**)**
説明
Core Protection は、脅威防御ポリシーの一部としてインストールされます。コア保護は、悪意のあるトラフィックからネットワークを保護するために不可欠な IPS 保護のセットです4。他のポリシーにはコア保護は含まれません。
参考資料: 1: Check Point CLI リファレンス カード 2: スプーフィング対策 3: SmartView Tracker 4: コア保護

最新問題: **87**
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. エキスパート
B. 管理者
C. クリッシュ
D. 通常
Answer: C (メーッセージを残す**)**

最新問題: **88**
Check Point Capsule の 3 つのコンポーネントは何ですか?
A. Capsule Docs、Capsule Cloud、Capsule Connect
B. Capsule Workspace、Capsule Cloud、Capsule Connect
C. Capsule Workspace、Capsule Docs、Capsule Connect
D. Capsule Workspace、Capsule Docs、Capsule Cloud
Answer: D (メーッセージを残す**)**
説明
Check Point Capsule の 3 つのコンポーネントは、Capsule Workspace、Capsule Docs、および Capsule Cloud123 です。Capsule Workspace は、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モバイル デバイス上に提供します2。Capsule Docs は、暗号化とアクセス制御によってビジネス文書をどこにいても保護します1。Capsule Cloud は、モバイル ユーザーを脅威から保護するクラウドベースのセキュリティ サービスを提供します3。参考資料: Check Point Capsule、Check Point Capsule Workspace、Mobile Secure Workspace with Capsule

最新問題: **89**

次の図が表示されます。



そこには何が提示されているのでしょうか？

A. 個人のプロパティ。ユーザー John に対して発行された p12 証明書ファイル。

B. John のパスワードの共有秘密プロパティ。

C. John のゲートウェイの VPN 証明書プロパティ。

D. 有効期限が切れています。ユーザー John の p12 証明書プロパティ。

Answer: A (メーッセージを残す)

説明

この図は、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を示しているため、答えは A です。.p12 ファイルは、ユーザーの秘密キーと公開キー証明書を含むファイル形式です。この図は、証明書ファイルが有効で、有効期限が 2018 年 4 月 7 日であることを示しています。この図は、証明書ファイルが内部 CA によって発行されていることも示しています。内部 CA は、ユーザーとゲートウェイの証明書を管理する Check Point コンポーネントです。参考資料: Check Point R81 証明書管理、Check Point R81 内部 CA

最新問題**: 90**

セキュリティ管理者は SmartDashboard 内のどこで ID 認識を有効にしますか?

A. セキュリティ管理サーバー > ID 認識

B. ゲートウェイ オブジェクト > 一般プロパティ

C. LDAP サーバー オブジェクト > 一般プロパティ

D. ポリシー > グローバル プロパティ > ID 認識

Answer: B (メーッセージを残す)

最新問題: **91**
SandBlast は、個々のビジネス ニーズに基づいて柔軟に実装できます。
Check Point SandBlast Zero-Day Protection の展開オプションは何ですか?
A. 負荷共有モードのサービス
B. パブリック クラウド サービス
C. 脅威エージェントのソリューション
D. スマート クラウド サービス
Answer: D (メーッセージを残す)

最新問題: **92**
ルールで追跡を有効にする場合、デフォルトのオプションは何ですか?
A. ログ
B. 拡張ログ
C. アカウンティング ログ
D. 詳細ログ
Answer: (解答を表示する)

最新問題: **93**
トークン認証を必要とする認証方法に名前を付けます。
A. SecureID
B. 半径
C. 動的ID
D. TACACS
Answer: A (メーッセージを残す)
説明
SecureIDはトークンauthenticator2を必要とする認証方式です。SecureID は、ハードウェア トークンまたはソフトウェア トークンを使用してワンタイム パスワードを生成する 2 要素認証方法です。ユーザーは、認証のためにユーザー名とパスワードとともにトークン コードを入力する必要があります。参考資料: Check Point R81 ID 認識管理ガイド

最新問題: **94**
分散導入では、Security Gateway と Security Management ソフトウェアはどのプラットフォームにインストールされますか?

A. 別のコンピューターまたはアプライアンス。
B. 同じコンピュータまたはアプライアンス。
C. 両方が仮想マシン上、または両方がアプライアンス上にありますが、混合はできません。
D. Azure および AWS クラウド環境。
Answer: A (メーッセージを残す)
「Security Management ServerClosed (1) と Security GatewayClosed (3) は、ネットワーク接続 (2) を備えた別のコンピュータにインストールされています。」https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_Installation_and_Upgrade_Guide/Topics-IUG/Getting-Started.htm

最新問題: **95**
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が利用可能ですか?
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)
説明
HTTPS 検査ポリシーのルールの 「アクション」列で使用できるアクションは、 「検査」と 「検査」です。
"バイパス"。 「検査」は、アクセス コントロール ポリシーに従って HTTPS トラフィックが復号化され、検査されることを意味します。 「バイパス」とは、HTTPS トラフィックが復号化されず、検査なしで許可されることを意味します1。他のオプションは、HTTPS 検査ポリシーの有効なアクションではありません。

最新問題: **96**
SmartConsole のゲートウェイ ステータス ビューには、セキュリティ ゲートウェイとソフトウェア ブレードの全体的なステータスが表示されます。ステータス アテンションとは何を意味しますか?
A. Security Gateway に到達できません。
B. ゲートウェイとそのすべての Software Blade は正常に動作しています。
C. 少なくとも 1 つの Software Blade に軽微な問題がありますが、ゲートウェイは機能します。
D. Security Management Server と Security Gateway の間で SIC を作成できません
Answer: C (メーッセージを残す)
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Monitoring-Gateway-Status.htm

最新問題: **97**
空白を埋めてください: ライセンスがアクティベートされたら、_____ をインストールする必要があります。
A. ライセンス契約ファイル
B. ライセンス管理ファイル
C. Security Gateway 契約ファイル
D. サービス契約ファイル

Answer: (解答を表示する)

最新問題: **98**
空白を埋めてください: 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. トークン
B. 証明書
C. 共有シークレット
D. ユーザー名/パスワードまたは Kerberos チケット
Answer: D (メーッセージを残す)

最新問題: **99**
イベントとログの違いは何ですか?
A. イベントは SmartWorkflow を使用してトラブル チケット システムから収集されます
B. ログとイベントは同義語です
C. イベントはイベント ポリシーに従ってゲートウェイで生成されます
D. ログ エントリは、イベント ポリシーで定義されたルールに一致するとイベントになります。
Answer: D (メーッセージを残す)

最新問題: **100**
どの構成要素が、どのトラフィックを VPN トンネルに暗号化して送信するのか、平文で送信するのかを決定しますか?
A. VPN ドメイン
B. ファイアウォール トポロジ
C. ルールベース
D. NAT ルール
Answer: (解答を表示する)

最新問題: **101**
パケットから詳細情報を抽出し、その情報を状態テーブルに保存するテクノロジーは次のうちどれですか?
A. 検査エンジン
B. 次世代ファイアウォール
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: B (メーッセージを残す)
Check Point FireWall-1 のステートフル インスペクションは、クライアント/サーバー モデルを壊さずにアプリケーション層の完全な認識を提供することで、前の 2 つのアプローチの制限を克服します。ステートフル インスペクションでは、パケットはネットワーク層で傍受されますが、その後は INSPECT エンジンが引き継ぎます。すべてのアプリケーション層からセキュリティの決定に必要な状態関連情報を抽出し、後続の接続試行を評価するためにこの情報を動的状態テーブルに保持します。これにより、安全性が高く、最大のパフォーマンス、スケーラビリティ、拡張性を備えたソリューションが提供されます。

最新問題: **102**

トムは、SmartConsole を使用して Management Server にリモートで接続し、ルール ベースの変更を行っている途中で、突然接続が切断されました。その後すぐに接続が回復します。すでに行われた変更はどうなりますか?
A. トムの変更は再接続時に管理に保存されており、作業内容は失われません。
B. トムは SmartConsole コンピュータを再起動し、キャッシュをクリアし、変更を復元する必要があります。
C. トムは SmartConsole コンピュータを再起動し、そのコンピュータ上の管理キャッシュ ストアにアクセスする必要があります。これは再起動後にのみアクセス可能です。
D. 接続が失われたため、トムの変更は失われ、最初からやり直す必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 103**
アプリケーション セキュリティと ID 制御を提供する Check Point ソフトウェア ブレードはどれですか?
A. アイデンティティの認識
B. データ損失防止
C. URL フィルタリング
D. アプリケーション制御
Answer: D (メーッセージを残す**)**
Check Point Application Control は、業界最強のアプリケーション セキュリティと ID 管理をあらゆる規模の組織に提供します。

最新問題**: 104**
管理者の Dave は、R80 Management Server にログインしてルールを確認し、いくつかの変更を加えます。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しょうか?
A. DNS ルールは、R80 の新機能の 1 つを使用しています。この機能では、管理者がルールに南京錠のアイコンをマークして、他の管理者にそのルールが重要であることを知らせることができます。
B. 別の管理者が管理にログインしており、現在 DNS ルールを編集しています。
C. 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。
D. これは、ルール ベースに重複したルールがある場合の R80 の通常の動作です。
Answer: (解答を表示する)
説明

ルール ベースの DNS ルールの横にある南京錠の記号は、別の管理者が管理にログインし、現在 DNS ルール 1 を編集していることを示します。これは、複数の管理者が同じポリシーに対して同時に作業できるようにする R80 の機能です。南京錠の記号は、編集管理者が変更を公開または破棄するまで、他の管理者が同じルールを変更できないようにします2。他のオプションは南京錠記号の有効な説明ではありません。参考資料: 156-215.80 : Check Point Certified Security Administrator (CCSA R80) : パート 19、マルチユーザー ポリシーの編集

最新問題**: 105**
あるハードウェア デバイスから別のハードウェア デバイスにライセンスを転送するのは、どのシナリオで有効なオプションですか?
A. IBM オープン サーバーから HP オープン サーバーへ
B. 4400 アプライアンスから 2200 アプライアンスへ
C. 4400 アプライアンスから HP Open Server へ
D. IBM オープンサーバーから 2200 アプライアンスへ
Answer: A (メーッセージを残す**)**

最新問題**: 106**
NAT の優先順位は何ですか?
A. IP プール NAT 静的 NAT。NATを隠す
B. 静的 NAT 非表示 NAT、IP プール NAT
C. 静的 NAT、IP プール NAT 非表示 NAT
D. 静的 NAT 自動 NAT 非表示 NAT
Answer: (解答を表示する)
説明
NAT の優先順位は、スタティック NAT、IP プール NAT、隠蔽 NAT の順です。静的 NAT はプライベート IP アドレスとパブリック IP アドレスの 1 対 1 のマッピングであるため、最も高い優先順位が付けられます。IP プール NAT は、プライベート IP アドレスからパブリック IP アドレスのプールへの 1 対多のマッピングであるため、優先順位が 2 番目に高くなります。Hide NAT は、複数のプライベート IP アドレスを 1 つのパブリック IP アドレスに多対 1 でマッピングするため、優先順位が最も低くなります1。
参考資料: 1: Check Point R81 Security Gateway 管理ガイド、23 ページ。

最新問題**: 107**
以下のルールをご覧ください。左の列のペンのマークは何を意味しますか?

A. これらのルールは現在のセッションで公開されています。
B. ログインした管理者によってルールが編集されましたが、ポリシーはまだ公開されていません。
C. 現在、別のユーザーがルールの編集をロックしています。
D. 構成ロックが存在します。ロックを取得するには、ペンのシンボルをクリックします。
Answer: B (メーッセージを残す)
説明
左側の列のペン記号は、ログインした管理者によってルールが編集されましたが、ポリシーはまだ公開されていないことを意味します。これは、変更がまだ有効になっていないため、破棄できることを示します。参考資料: ポリシー エディター、変更の公開

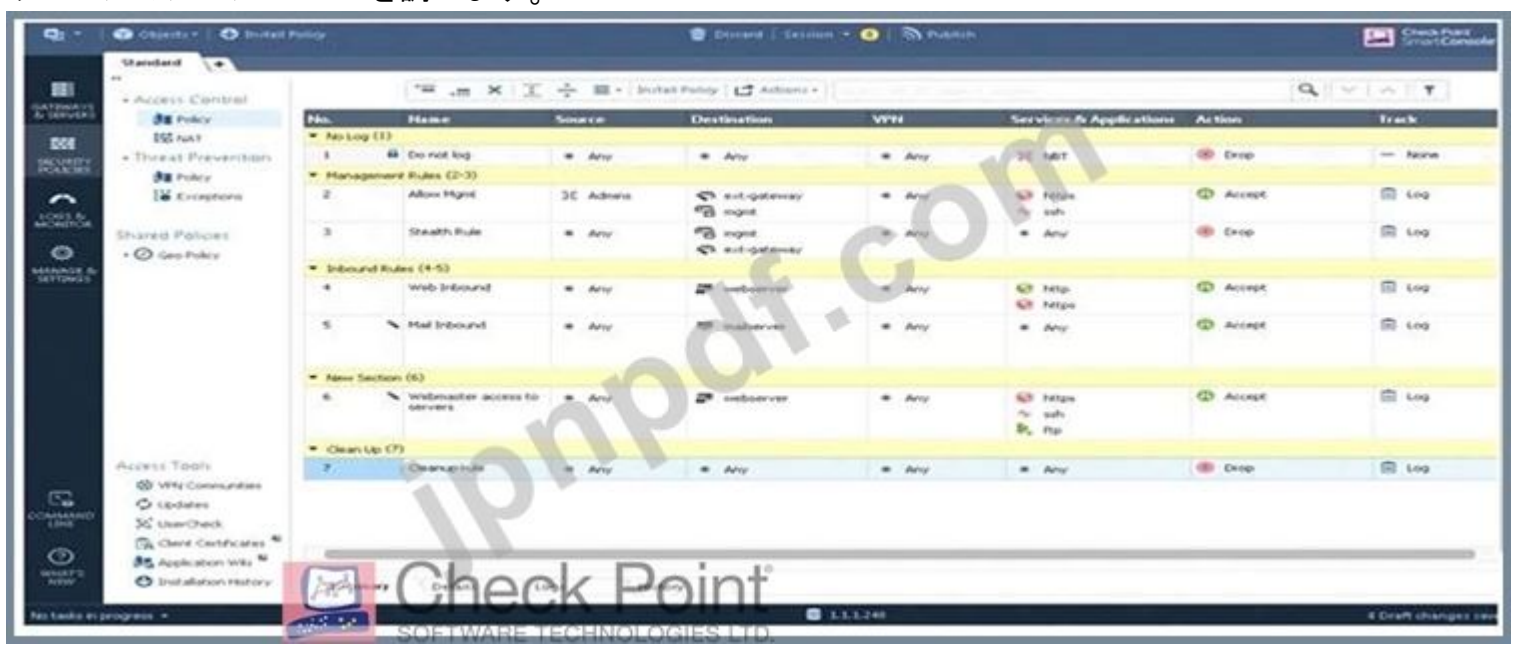
最新問題**: 108**
ユーザーチェックとは何ですか?
A. ユーザーの資格情報を検証するためのメッセージング ツール ユーザー
B. アクセスしようとしている Web サイトまたはアプリケーションについてユーザーに通知するために使用されるコミュニケーション ツール
C. ネットワーク上のユーザーを監視するために使用される管理者ツール
D. 新しいユーザーが作成されたときに管理者に通知するために使用される通信ツール
Answer: (解答を表示する)
説明
UserCheck は、アクセスしようとしている Web サイトまたはアプリケーションについてユーザーに通知するために使用されるコミュニケーション ツールです。UserCheck を使用すると、管理者は、確認の要求、リスクについての通知、アクセスのブロックなど、ユーザーの対話を必要とするアクションを定義できます3、p. 38. UserCheck は、メッセージング ツール、管理者ツール、または通知ツールではありません。参考文献: Check Point CCSA - R81: 模擬テストと解説、
[Check Point UserCheck 管理ガイド R81]

最新問題**: 109**
Security Gateway でサポートされる 2 種類の NAT は何ですか?
A. 静的およびソース
B. 送信元と宛先
C. 非表示および静的
D. 宛先と非表示
Answer: C (メーッセージを残す)

最新問題: **110**
脅威抽出の背後にあるメカニズムは何ですか?
A. 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 データベースに入れる新しいメカニズムです (不審なアクティビティの監視)。
B. 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。
C. JavaScript、マクロ、リンクなどのドキュメントのアクティブなコンテンツはドキュメントから削除され、目的の受信者に転送されるため、このソリューションは非常に高速になります。
D. 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、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。
Answer: C (メーッセージを残す**)**

最新問題: **111**
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が許可されるオプションはどれですか?
A. すべての暗号化されたトラフィックを受け入れます
B. すべての接続 (クリアまたは暗号化)
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: A (メーッセージを残す**)**

最新問題: **112**
サンプルのルール ベースを調べます。



SmartConsole からのポリシーの検証の結果はどうなりますか?
A. エラーや警告はありません
B. 検証エラー。ルール 5 の空のソースリスト (メール受信)
C. 検証エラー。ルール 4 (Web インバウンド) はルール 6 (Web マスター アクセス) を非表示にします
D. 検証エラー。ルール 7 (クリーンアップ ルール) は暗黙的なクリーンアップ ルールを非表示にします

Answer: C (メーッセージを残す)
説明
検証エラー。ルール 4 (Web インバウンド) はルール 6 (Web マスター アクセス) を隠しますが、これが正解です。これは、ルール 4 の送信元と宛先がルール 6 よりも広く、両方のルールが同じサービス (HTTP) を持っているためです。したがって、ルール 6 が一致することはなく、Web マスターのアクセスは拒否されます。参考文献:
チェックポイント R80.10 - パート 3 - ルールベースの順序

最新問題**: 113**
交通方向を計算するオプションではないものは次のうちどれですか?
A. 内部
B. 発信
C. 受信中
D. 外部
Answer: B (メーッセージを残す)

最新問題**: 114**
NAT ルールを手動で作成する理由は何ですか?
A. インターネットにアクセスするには、RFC1918 準拠のネットワークのネットワーク アドレス変換が必要です。
B. 一部のサービスではネットワーク アドレス変換が必要ですが、他のサービスでは必要ありません。
C. パブリック IP アドレスはゲートウェイの外部 IP とは異なります
D. R80 では、すべてのネットワーク アドレス変換が自動的に行われるため、NAT ルールを手動で定義する必要はありません。
Answer: C (メーッセージを残す)

最新問題**: 115**
空白を埋めてください: ライセンスがアクティベートされたら、_____ 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 契約ファイル
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 (メーッセージを残す)
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され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 経由でインストールされます。
サービス契約ファイルの詳細については、sk33089 を参照してください。

最新問題**: 116**
ネットワーク トラフィックを拒否または許可する Check Point テクノロジーはどれですか?
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: (解答を表示する**)**
説明
ネットワーク トラフィックを拒否または許可する Check Point テクノロジーには、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、およびアプリケーション層ファイアウォールがあります1、p. 15-16。パケット フィルタリングは、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パケットを検査する基本的なファイアウォール技術です2、p. 13. 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、その内容とシーケンスに基づいてパケットを検査する高度なファイアウォール技術です2、p. 13。13. アプリケーション層ファイアウォールは、OSI モデルのアプリケーション層で動作し、アプリケーション プロトコルとデータに基づいてパケットを検査するファイアウォール技術です。14. 参考文献: Check Point CCSA - R81: 模擬テストと説明、156-315.81 チェックポイント試験情報および無料模擬テスト

最新問題**: 117**
セッションを最もよく表すものを選択してください。
A. 管理者が SmartConsole で行われたすべての変更を公開すると開始されます。
B. 管理者が SmartConsole を通じて Security Management Server にログインすると開始され、公開されると終了します。
C. ポリシーが Security Gateway にプッシュされると、セッションが終了します。
D. セッションは編集のためにポリシー パッケージをロックします。
Answer: (解答を表示する**)**
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 を通じて 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。管理者がセッション中に行った変更は、その管理者のみが使用できます。他の管理者には、編集中のオブジェクトとルールに鍵の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**: 118**
NAT ルールを手動で作成する理由は何ですか?
A. 一部のサービスではネットワーク アドレス変換が必要ですが、他のサービスでは必要ありません。
B. パブリック IP アドレスはゲートウェイの外部 IP とは異なります
C. インターネットにアクセスするには、RFC1918 準拠のネットワークのネットワーク アドレス変換が必要です。
D. R81 では、すべてのネットワーク アドレス変換が自動的に行われるため、NAT ルールを手動で定義する必要はありません。
Answer: B (メーッセージを残す**)**

最新問題**: 119**
指定された期間、特定の IP アドレスをブロックできる R77 の機能はどれですか?
A. ローカル インターフェイスのスプーフィング
B. HTTP メソッド
C. 不審なアクティビティの監視

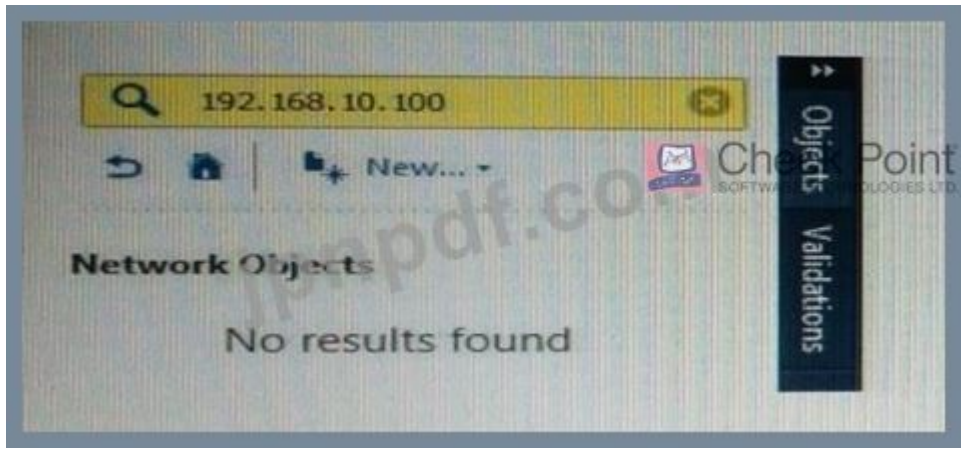
D. ポートのオーバーフローをブロック
Answer: C (メーッセージを残す**)**

最新問題**: 120**
管理者が作成した自動非表示 NAT ルールの場合、TRUE ステートメントとは何ですか?
A. 自動 NAT ルールはホスト オブジェクトに対してのみサポートされます。
B. 送信元ポート アドレス変換 (PAT) はデフォルトで無効になっています
C. 自動 NAT ルールは、ネットワーク オブジェクトに対してのみサポートされます。
D. 送信元ポート アドレス変換 (PAT) はデフォルトで有効になっています
Answer: (解答を表示する**)**

最新問題**: 121**
出版の役割とは何ですか?
A. 公開操作は、プライベート セッションで SmartConsole 経由で行われた変更を送信し、公開します。
B. 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。
C. Security Management Server は、更新されたセッションとルール ベース全体を Security Gateway にインストールします。
D. サーバー、ユーザー、サービス、IPS プロファイルなどのネットワーク オブジェクトを変更しますが、ルール ベースは変更しません
Answer: A (メーッセージを残す**)**
説明
公開操作では、プライベート セッションで SmartConsole 経由で行われた変更を送信し、公開するのが正解です。これは、公開とは、変更をデータベースに保存し、他の管理者が使用できるようにするプロセスであるためです。公開すると、Security Gateway にポリシーをインストールすることもできます。参考資料: [公開の変更点]

最新問題**: 122**
ブリッジ モード Check Point Security Gateway でサポートされていないものは次のうちどれですか?
A. NAT
B. アプリケーション制御
C. ウイルス対策
D. データ損失防止
Answer: A (メーッセージを残す**)**

最新問題**: 123**
ボブがオブジェクト検索でこの結果を得た場合、それは何を意味しますか? 下の画像を参照してください。最良の答えを選択する。



A. オブジェクトには NAT IP アドレスがありません。
B. 詳細検索にサブネット マスクがありません。
C. その名前または IP アドレスを持つオブジェクトはデータベース上にありません。
D. その IP アドレスを持つオブジェクトはデータベース上にありません。
Answer: C (メーッセージを残す)

最新問題**: 124**
Gaia OS に含まれる事前定義されたロールに名前を付けます。
A. AdminRole および MonitorRole
B. ReadWriteRole および ReadyOnly ロール
C. AdminRole、cloningAdminRole、および Monitor ロール
D. 管理者ロール
Answer: A (メーッセージを残す)
説明
Gaia OS に含まれる事前定義されたロールは、AdminRole と MonitorRole です。AdminRole は、すべての GAIA 機能とコマンドへの完全なアクセス権を持つロールです。MonitorRole は、Gaia の機能とコマンドへの読み取り専用アクセス権を持つロールです1。他のオプションは、Gaia OS の有効な事前定義ロールではありません。

最新問題**: 125**
あなたは、R80 Check Point 資産を持つ Alpha Corp の Check Point 管理者です。管理ユーザーの 1 人から、会社のワイヤレスに接続した新しいタブレットでインターネットを閲覧できないという電話を受けました。ワイヤレス システムはチェック ポイント ゲートウェイを通過します。ログを確認して問題の内容を確認するにはどうすればよいでしょうか?
A. SmartLog を開き、ワイヤレス コントローラーの IP にリモート接続します。
B. SmartLog を開き、マネージャーのタブレットの IP アドレスをクエリします。
C. SmartView Tracker を開き、タブレットの IP アドレスのログをフィルタリングします。
D. SmartView Tracker を開き、タブレットのすべての IP ログを確認します。
Answer: C (メーッセージを残す)

最新問題**: 126**
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**)**
説明
Clish は、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です。これは、メニューベースのモードとコマンドライン モードを提供するユーザーフレンドリーなシェルです。Admin、Normal、および Expert は有効なシェル名ではありません1。

最新問題**: 127**
ネットワーク オペレーション センター管理者は、主にトラブルシューティングの目的で Check Point Security デバイスにアクセスする必要があります。彼女にエキスパート モードへのアクセスを許可したくありませんが、それでも tcpdump を実行できるはずです。どうすればこの要件を達成できるでしょうか?
A. 新しいアクセス ロールを作成します。ロールにエキスパート モード アクセスを追加します。UID 0 で新しいユーザーを作成し、ユーザーにロールを割り当てます。
B. add コマンドを使用して tcpdump を CLISH に追加します。新しいアクセス ロールを作成します。tcpdump をロールに追加します。任意の UID で新しいユーザーを作成し、そのユーザーにロールを割り当てます。
C. add コマンドを使用して tcpdump を CLISH に追加します。新しいアクセス ロールを作成します。tcpdump をロールに追加します。UID 0 で新しいユーザーを作成し、そのユーザーにロールを割り当てます。
D. 新しいアクセス ロールを作成します。ロールにエキスパート モード アクセスを追加します。任意の UID で新しいユーザーを作成し、ユーザーにロールを割り当てます。
Answer: (解答を表示する**)**

最新問題**: 128**
あるハードウェア デバイスから別のハードウェア デバイスにライセンスを転送するのは、どのシナリオで有効なオプションですか?
A. IBM オープンサーバーから 2200 アプライアンスへ
B. IBM オープン サーバーから HP オープン サーバーへ
C. 4400 アプライアンスから HP Open Server へ
D. 4400 アプライアンスから 2200 アプライアンスへ
Answer: B (メーッセージを残す**)**

最新問題**: 129**
Secure Internal Communication (SIC) はどのようなプロセスによって処理されますか?
A. CPM
B. HTTPS
C. 前輪駆動
D. CPD
Answer: (解答を表示する**)**
説明

Secure Internal Communication (SIC) は CPD プロセスによって処理されます3。CPD は、すべての Check Point モジュール上で実行され、内部ライセンスおよび SIC 操作を処理する Check Point デーモンです。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保証するメカニズムです。
参考資料: Check Point R81 セキュリティ管理管理ガイド

最新問題**: 130**
通信初期化プロセスの目的は、Security Management Server と Check Point ゲートウェイの間に信頼を確立することです。この安全な内部通信 (SIC) を最もよく説明しているのはどれですか?
A. 初期化が成功すると、ゲートウェイは、同じ ICA によって署名された SIC 証明書を所有する任意の Check Point ノードと通信できます。
B. Secure Internal Communications は、http 通信が許可される前に、SMS に対するセキュリティ ゲートウェイを認証します。
C. ゲートウェイは SMS ICA の下位 CA をホストしているため、SIC 証明書はゲートウェイ上で自動的に生成されます。
D. 新しいファイアウォールは、SMS で定義されたエキスパート パスワードと SMS IP アドレスを使用して、信頼を簡単に確立できます。
Answer: A (メーッセージを残す**)**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_SecurityManagement_AdminGuide/Topics-SECMG/Secure-Internal-Communication.htm

最新問題**: 131**
効果的なセキュリティ ポリシーを構築するために Check Point が推奨する 2 つの基本的なルールは何ですか?
A. 明示的なルールと暗黙的なルール
B. ルールの受け入れとルールの削除
C. NAT ルールと拒否ルール
D. クリーンアップ ルールとステルス ルール
Answer: D (メーッセージを残す**)**

最新問題**: 132**
AdminA と AdminB は両方とも SmartConsole にログインしています。
AdminB がルール上でロックされたアイコンを確認した場合、それは何を意味しますか? 最良の答えを選択する。
A. 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。
B. ルールのオブジェクトが編集されているため、ルールは AdminA によってロックされています。
C. 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ると使用可能になります。
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は使用可能になります
Answer: C (メーッセージを残す**)**

最新問題**: 133**
UserCheck メッセージには 3 種類ありますか?
A. 通知、質問、ブロック
B. ブロック、アクション、警告
C. アクション、通知、および質問

D. 質問、ブロック、通知
Answer: (解答を表示する**)**
ユーザーに通知する
知らせる
ruleClosed のアクションが通知である場合を示します。これは、そのサイトに対する会社のポリシーが何であるかをユーザーに通知します。
ブロックされたメッセージ
ブロック
リクエストがブロックされた場合に表示されます。
ユーザーに質問する
聞く
ルールのアクションが ask である場合に表示されます。これにより、そのサイトに対する会社のポリシーがユーザーに通知され、サイトに進むには [OK] をクリックする必要があります。
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_DataLossPrevention_AdminGuide/Topics-DLPG/UserCheck-Page.htm?tocpath=UserCheck%20Interaction%20Objects%7C_____3

最新問題**: 134**
アドレス変換ルールの 2 つの要素は何ですか?
A. 未翻訳のパケットと操作されたパケット
B. 翻訳済みパケットと未翻訳パケット
C. 元のパケットと変換されたパケット
D. 操作されたパケットと元のパケット
Answer: C (メーッセージを残す**)**

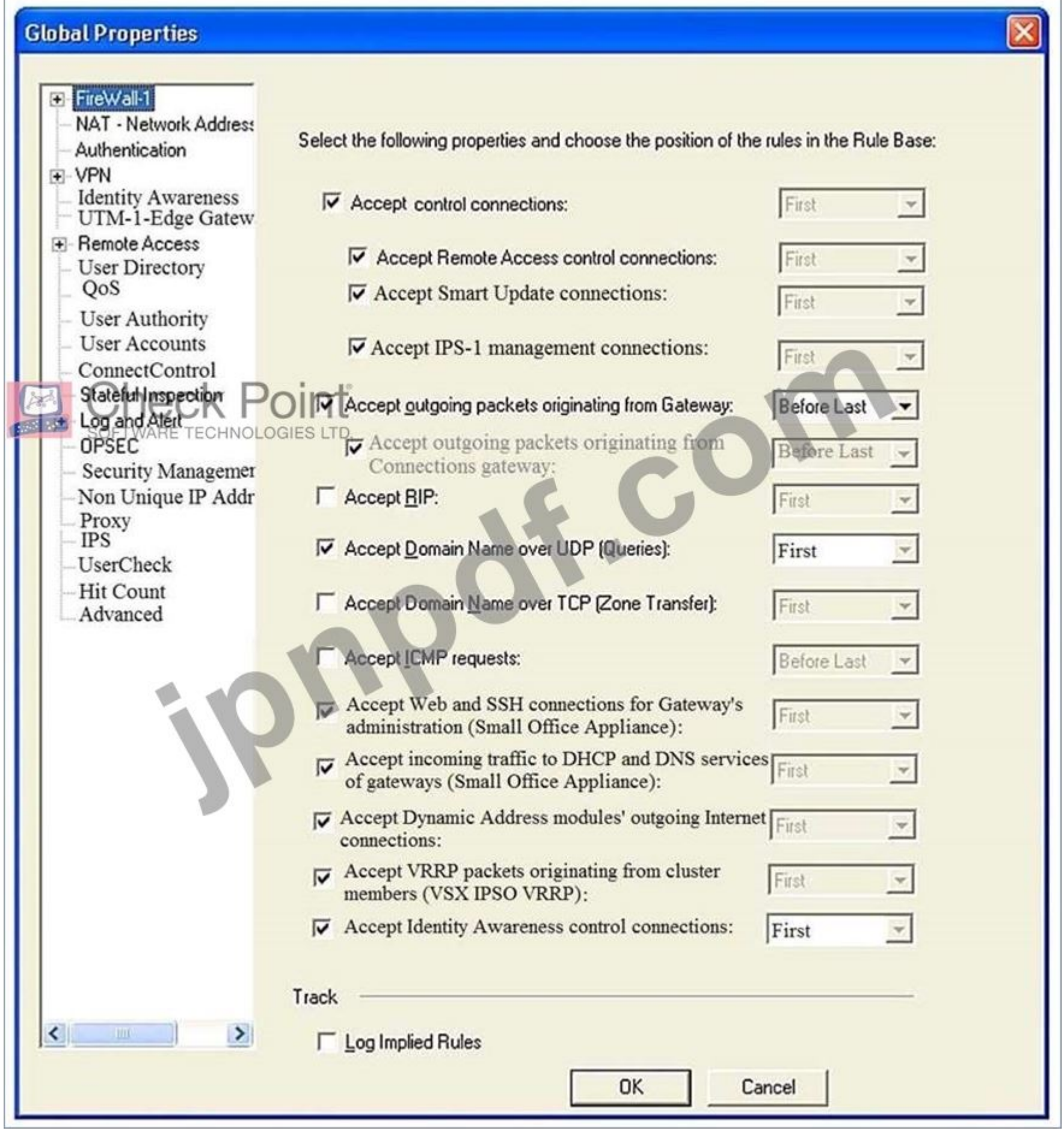
最新問題**: 135**
次のモバイル アクセスの認証タイプのうち、最初の認証方法として使用できないものはどれですか?
A. 動的ID
B. ユーザー名とパスワード
C. 半径
D. 証明書
Answer: A (メーッセージを残す**)**

最新問題**: 136**
アクセス ロールにより、ファイアウォール管理者は次に従ってネットワーク 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. 上記のすべて
D. リモート アクセス クライアント
Answer: C (メーッセージを残す**)**
アクセス役割を作成するには:

「アクセスロール」ウィンドウが開きます。
選択した内容は、[ロール 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 エントリを検索したり、リストから選択したりできます。
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**: 137**
現在の CPView ページをファイル名形式 cpview_"cpview process ID" で保存するために使用されるキー。
キャップ 「キャプチャ数」?
A. S
B. W
C. C
D. スペースバー
Answer: C (メーッセージを残す**)**
説明
キー C は、現在の CPView ページをファイル名形式 cpview_"cpview process ID" で保存するために使用されます。キャップ 「キャプチャ数」2. 参考資料: 無料の Check Point CCSA サンプル質問および学習ガイド

最新問題**: 138**
グローバル プロパティの次の設定を考慮してください。



選択したオプション「UDP 経由の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. すべての UDP クエリは、すべてのインターフェイスを介して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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。
B. UDP クエリは、外部スプーフィング防止トポロジ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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。
C. すべてのインターフェイスを介して許可されるトラフィックでは 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 ポリシーに最初に記述する明示的なルールの前に行われます。
D. すべての UDP クエリは、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: B (メーッセージを残す**)**

最新問題**: 139**
SmartConsole では、どのタブで権限と管理者が定義されていますか?
A. 管理と設定
B. ログとモニター
C. セキュリティ ポリシー
D. ゲートウェイとサーバー
Answer: (解答を表示する**)**
説明
権限と管理者は、SmartConsole3 の [管理と設定] タブで定義されます。このタブでは、SmartConsole やその他の Check Point 管理インターフェイスにアクセスするための管理者アカウント、役割、権限、認証方法を作成および管理できます。参考資料: Check Point R81 セキュリティ管理管理ガイド

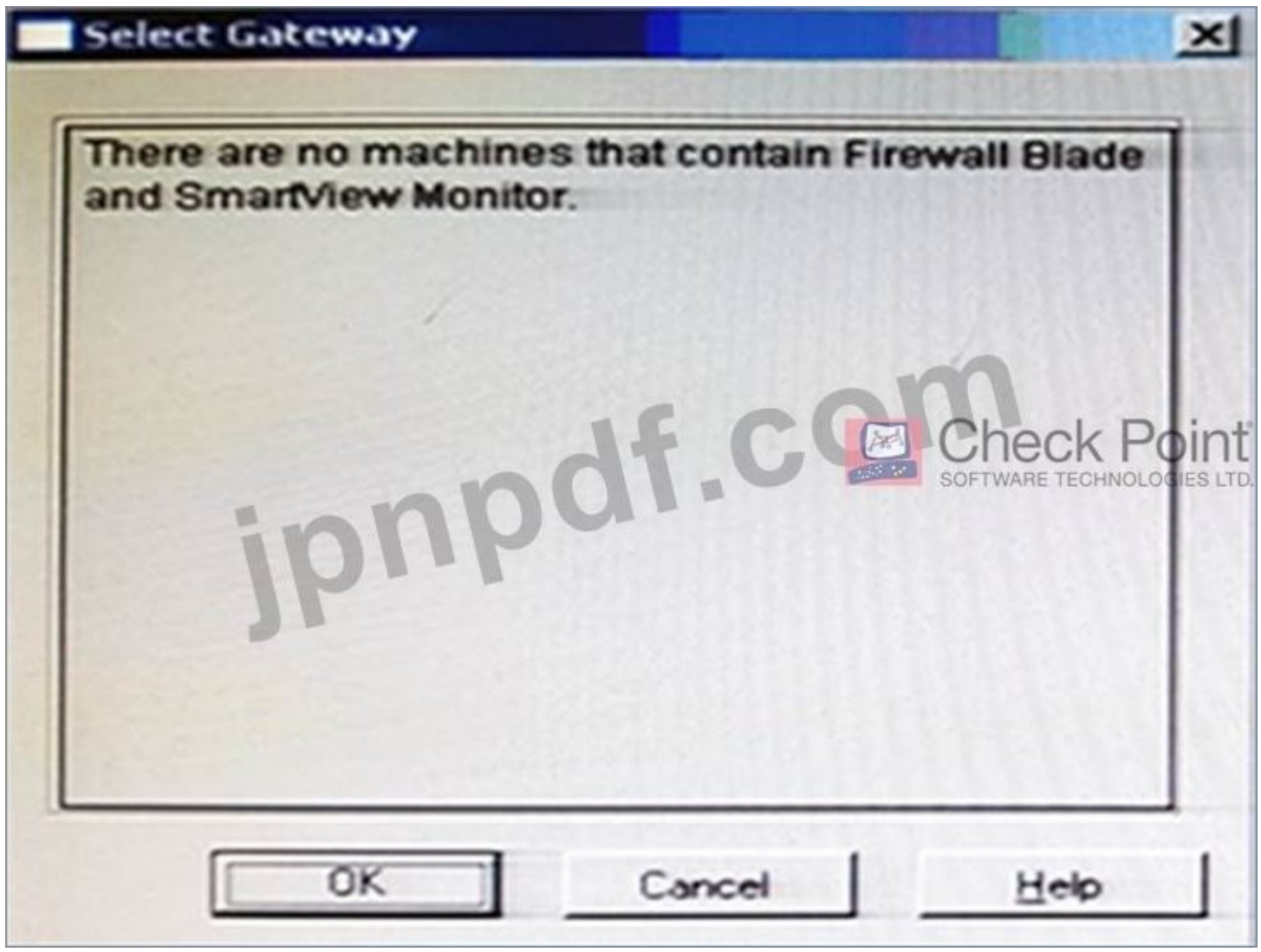
最新問題**: 140**
銀行に記入してください: オフィス モードでは、Security Gateway はリモート クライアントに IP アドレスを 1 回割り当てます _____。
A. ユーザーが接続して認証します
B. オフィス モードが開始されます
C. ユーザーが接続を要求します
D. ユーザーが接続します
Answer: (解答を表示する**)**
説明
Office モードでは、ユーザーが接続して認証すると、Security Gateway がリモート クライアントに IP アドレスを割り当てます。オフィス モードでは、リモート クライアントが組織の内部ネットワークから IP アドレスを取得できます。IP アドレスは、ユーザーが Security Gateway3 で正常に認証された後、IKE ネゴシエーション中に割り当てられます。他のオプションは、オフィス モードで IP アドレスを割り当てるための正しいタイミングではありません。参考 :オフィスモード

最新問題**: 141**
暗号化されたパケットが復号化されるとき、これはどこで行われるのでしょうか?
A. インバウンドチェーン
B. アウトバウンドチェーン

C. セキュリティ ポリシー
D. 復号化はサポートされていません
Answer: C (メーッセージを残す**)**

最新問題**: 142**
ゲートウェイ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、次のようなメッセージが表示されます。
「ファイアウォール ブレードと SmartView モニター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何をすべきでしょうか? ベストアンサーを答えてください。



A. Security Management Server でモニタリングを有効にします。
B. Security Gateway の SmartView Monitor ライセンスを購入します。
C. Security Management Server の SmartView Monitor ライセンスを購入します。
D. Security Gateway でモニタリングを有効にします。
Answer: D (メーッセージを残す)

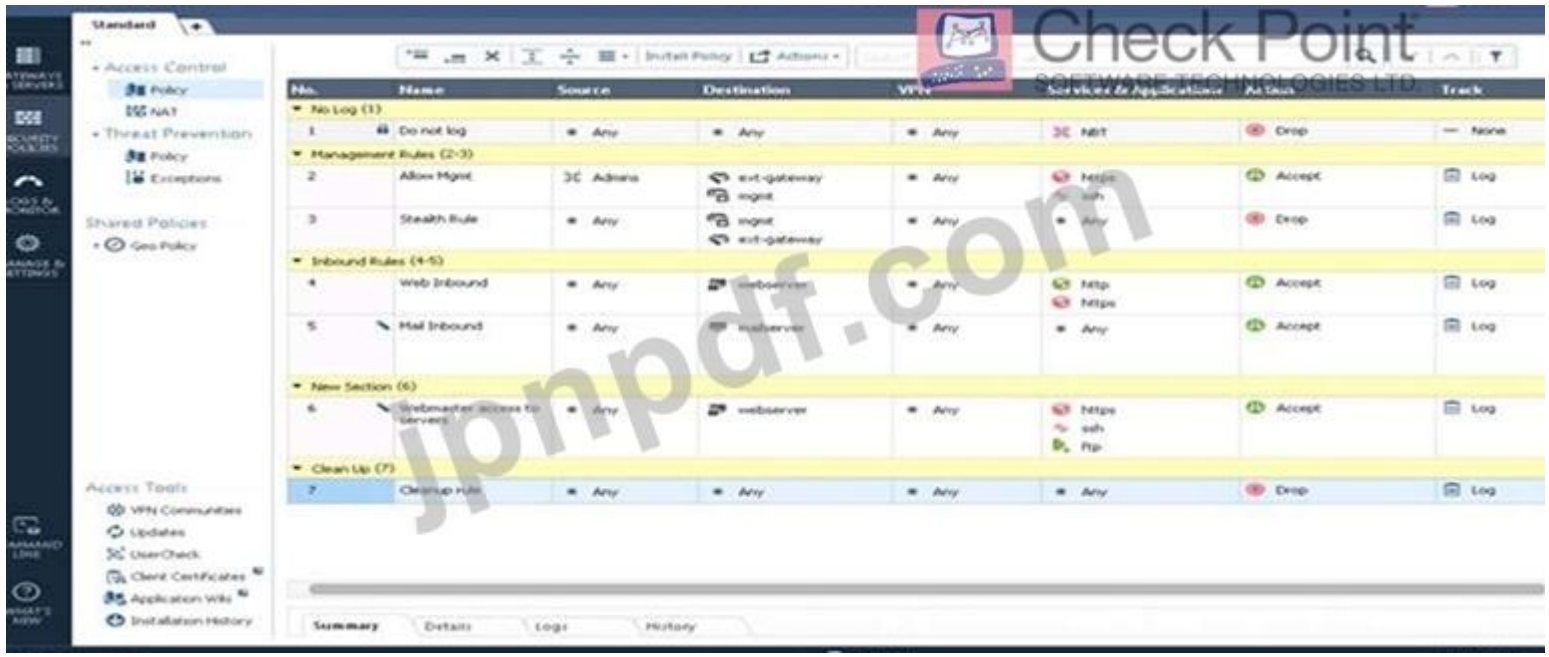
最新問題: **143**
空白を埋めてください:_____ はログを収集し、_____ に送信します。
A. ログサーバー。セキュリティゲートウェイ
B. ログサーバー。セキュリティ管理サーバー
C. セキュリティ管理サーバー。セキュリティゲートウェイ
D. セキュリティ ゲートウェイ。ログサーバー
Answer: (解答を表示する)
ゲートウェイはログをログ サーバーに送信します。

最新問題: **144**
SmartCenter の役割ではないものは次のうちどれですか:
A. ステータス監視

B. 認証局
C. ポリシー構成
D. アドレス変換
Answer: (解答を表示する**)**

最新問題**: 145**
あなたは、シカゴの拠点から東京、カルカッタ、ダラスまで広がるグローバル ネットワークを管理しています。経営陣は、各エンタープライズ クラス Security Gateway の現在のソフトウェア レベルを詳細に示すレポートを求めています。あなたは、この機会を利用して、ゲートウェイをアップグレードするための最もコスト効率の高い方法をリストした提案概要を作成する予定です。
このレポートと概要を作成するためにどの 2 つの SmartConsole アプリケーションを使用しますか?
A. SmartDashboard および SmartView Tracker
B. SmartView トラッカーおよび SmartView モニター
C. SmartView モニターと SmartUpdate
D. SmartLSM と SmartUpdate
Answer: C (メーッセージを残す**)**

最新問題**: 146**
サンプルのルール ベースを調べます。



SmartConsole からのポリシーの検証の結果はどうなりますか?
A. 検証エラー。ルール 4 (Web インバウンド) はルール 6 (Web マスター アクセス) を非表示にします
B. 検証エラー。ルール 5 の空のソースリスト (メール受信)
C. 検証エラー。ルール 7 (クリーンアップ ルール) は暗黙的なクリーンアップ ルールを非表示にします
D. エラーや警告はありません
Answer: A (メーッセージを残す**)**

最新問題**: 147**

Security Gateway で SNX を構成しました。クライアントは Security Gateway に接続し、ユーザーは認証資格情報を入力します。クライアントが Security Gateway の VPN ドメインに接続できるようにする認証の後は、何が起こる必要がありますか?
A. Active-X がクライアントで許可されている必要があります。
B. SNX クライアント アプリケーションがクライアントにインストールされている必要があります。
C. SNX はルーティング テーブルを変更して、VPN トラフィックを Security Gateway に転送します。
D. オフィス モード アドレスはクライアントによって取得される必要があります。
Answer: C (メーッセージを残す)

最新問題**: 148**
パケットのタグ付けとコンピュータ認証を含む Endpoint Identity Agent のタイプはどれですか?
A. フル
B. ライト
C. カスタム
D. 完了
Answer: (解答を表示する)
エンドポイント ID エージェント - ユーザーのコンピュータにインストールされ、ID を取得して Security Gateway に報告する専用のクライアント エージェント。

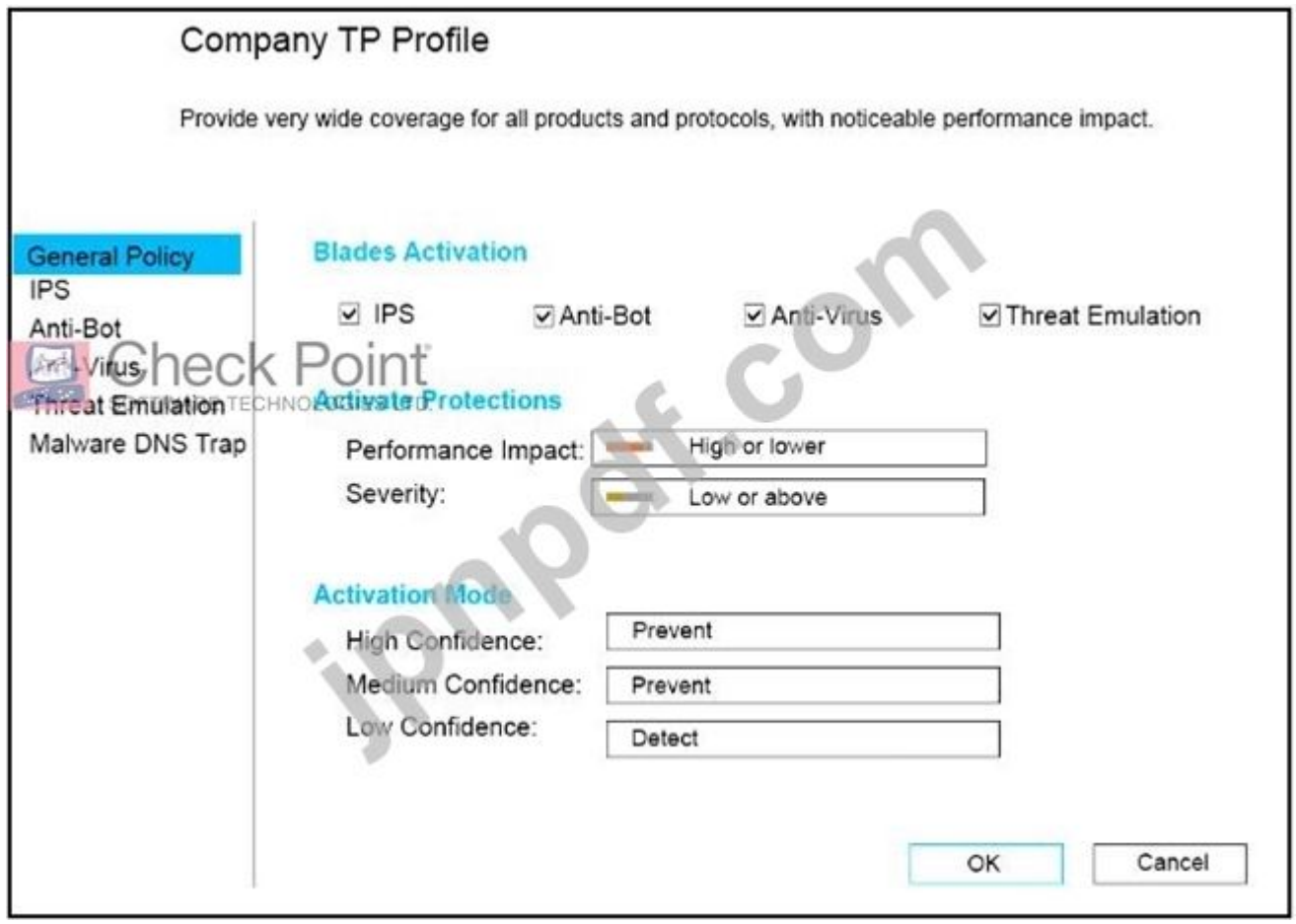
最新問題**: 149**
_____ ソフトウェア ブレード パッケージは、マルウェアを検出してブロックするために CPU レベルと OS レベルのサンドボックスを使用します。
A. 次世代の脅威防御
B. 次世代の脅威エミュレーション
C. 次世代の脅威の抽出
D. 次世代ファイアウォール
Answer: B (メーッセージを残す)
説明
次世代脅威エミュレーション ソフトウェア ブレード パッケージは、マルウェアを検出してブロックするために CPU レベルと OS レベルのサンドボックスを使用します1、p. 41. 仮想環境でファイルをエミュレートし、悪意のあるアクティビティの動作を検査します3。参考資料: Check Point CCSA - R81: 実践テストと解説、Check Point 脅威エミュレーション管理ガイド R81

最新問題**: 150**
複数の管理者が同時に Security Management Server に接続できますか?
A. いいえ、接続できるのは 1 つだけです
B. はい、すべての管理者が同時にネットワーク オブジェクトを変更できます
C. はい、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。
D. はい、ただし書き込み権限を持つのは 1 人だけです
Answer: C (メーッセージを残す)
説明

複数の管理者が同時に Security Management Server に接続でき、各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1。これにより、同時管理が可能になり、異なる管理者間の競合が防止されます。他のオプションは正しくありません。接続できる管理者は 1 人だけです。は false です。 ❜すべての管理者がネットワーク オブジェクトを同時に変更できる」は false です。オブジェクトをロックおよび編集できるのは一度に 1 人の管理者だけです。ロールまたは権限によって制限されない限り、すべての管理者が書き込み権限を持っているため、❜1 人だけが書き込み権限を持っている」は false です。
参考資料: Security Management Server - Check Point Software

最新問題**: 151**
SecureXL の観点から見ると、トラフィック フローのツリー パスは次のようになります。
A. 初期パス。中パス。加速されたパス
B. レイヤーパス。ブレードパス; ルールパス
C. ファイアウォール パス。パスを受け入れます。ドロップパス
D. ファイアウォール パス。加速されたパス。中パス
Answer: D (メーッセージを残す**)**
説明
SecureXL の観点から見ると、トラフィック フローの 3 つのパスはファイアウォール パス、アクセラレーテッド パス、およびミディアム パスであるため、正解は D です3。ファイアウォール パスは、SecureXL が無効になっている場合、またはトラフィックがアクセラレーションの対象ではない場合に使用されます3。高速パスは、SecureXL が接続全体を処理し、ファイアウォール カーネルをバイパスする場合に使用されます3。メディア パスは、SecureXL が接続の一部を処理し、さらなる検査のためにパケットをファイアウォール カーネルに転送するときに使用されます3。他のオプションは、SecureXL の観点からはトラフィック フローの有効なパスではありません3。参考資料: Check Point R81 パフォーマンス チューニング管理ガイド

最新問題**: 152**
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のではないかと思われます。
次の脅威防御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調整するにはどうすればよいでしょうか? 最良の回答を選択してください。

A. 問題は脅威防御プロファイルにありません。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. 高信頼性を低に設定し、低信頼性を非アクティブに設定します。

C. パフォーマンスへの影響を中以下に設定します。

D. 防止するには、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: C (メーッセージを残す)

最新問題**: 153**

R80は、次のオペレーティングシステムのどれでサポートされていますか。

A. Windowsのみ

B. ガイアのみ

C. SecurePlatformのみ

D. Gaia、SecurePlatform、およびWindows

Answer: B (メーッセージを残す)

最新問題**: 154**

アラートはどこで確認できますか?

A. アラートは SmartView Monitor で確認できます

B. アラートは脅威対策ポリシーで確認できます。

C. アラートは SmartUpdate で確認できます。

D. アラートはゲートウェイの CLI から確認できます。
Answer: A (メーッセージを残す**)**
説明
アラートは、トラフィック、VPN トンネル、脅威、パフォーマンスなどのネットワークおよびセキュリティ アクティビティに関するリアルタイム情報を提供するグラフィカル ツールである SmartView Monitor で表示できます4。
参考資料: 4: Check Point R81 セキュリティ管理管理ガイド、25 ページ。

最新問題**: 155**
ステートフル インスペクションとプロキシの間の競争は、パフォーマンス、プロトコル サポート、およびセキュリティに基づいていました。ステートフルなインスペクションとプロキシを考慮すると、どの記述が正しいでしょうか?
A. ステートフル インスペクションはレイヤー 3 の可視性に制限されており、レイヤー 4 からレイヤー 7 の可視性機能はありません。
B. パフォーマンスに関しては、ステートフル インスペクションはプロキシよりも大幅に高速でした。
C. パフォーマンスに関しては、プロキシはステートフル インスペクション ファイアウォールよりも大幅に高速でした。
D. プロキシはペイロード (データ) を可視化できるため、はるかに高いセキュリティを提供します。
Answer: D (メーッセージを残す**)**

最新問題**: 156**
セキュリティ ルールの追跡オプションとして 「拡張ログ」を有効にしました。ただし、データ型情報はまだ表示されません。最も考えられる理由は何ですか?
A. コンテンツ認識が有効になっていません。
B. ログのトリミングが有効になっています。
C. ログにディスク容量の問題があります
D. ID 認識が有効になっていません。
Answer: A (メーッセージを残す**)**

最新問題**: 157**
デジタル署名:
A. データを元の形式に復号します。
B. メッセージの信頼性と完全性を保証します。
C. インターネット上で安全なキー交換メカニズムを提供します。
D. 共有キーを自動的に交換します。
Answer: B (メーッセージを残す**)**

最新問題**: 158**
管理者は、ポリシーのルールでアプリケーション オブジェクトを使用したいと考えていますが、ルールの [サービスとアプリケーション] 列に新しい項目を追加するために [+] をクリックするときに、追加するオプションとしてアプリケーション オブジェクトがリストされていません。これを修正するにはどうすればよいでしょうか?
A. 管理者はまず、ルールに追加するアプリケーションをいくつか作成する必要があります。
B. 「アプリケーション コントロール」ブレードはゲートウェイで有効にする必要があります

C. まず、ルールが作成されているポリシー レイヤーで 「アプリケーションと URL フィルタリング」を有効にする必要があります。
D. 管理者は、必要なアプリケーション オブジェクトをオブジェクト エクスプローラーから新しいルールにドラッグ アンド ドロップする必要があります。
Answer: B (メーッセージを残す)

最新問題: **159**
トラフィック ルールで 「アカウンティング」追跡オプションが有効になっている場合、ログはどのように変化しますか?
A. 関係するトラフィック ログはログ サーバーに転送されます。
B. ログの詳細を表示する電子メールを管理者に提供します。
C. 関係するトラフィック ログは 10 分ごとに更新され、接続上で渡されたデータの量を示します。
D. 接続しているユーザーに追加情報を提供します。
Answer: C (メーッセージを残す)
説明
アカウンティング追跡オプションは、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。このオプションがトラフィック ルールで有効になっている場合、関連するトラフィック ログが 10 分ごとに更新され、接続上で渡されたデータの量が表示されます。この情報は、請求または監査の目的で使用できます3。
参考資料: Check Point R81 ログおよびモニタリング管理ガイド

最新問題: **160**
SmartDashboard から SIC をリセットする最も正しいプロセスは次のうちどれですか?
A. ファイアウォール オブジェクトの [通信] ボタンをクリックし、[リセット] をクリックします。ゲートウェイで cpconfig を実行し、新しいアクティベーション キーを入力します。
B. cpconfig を実行し、[リセット] をクリックします。
C. cpconfig を実行し、[安全な内部通信] > [ワンタイム パスワードの変更] を選択します。
D. ゲートウェイ オブジェクトで [通信] > [リセット] をクリックし、新しいアクティベーション キーを入力します。
Answer: A (メーッセージを残す)

最新問題: **161**
エキスパート モードでインストールされているライセンスを表示するコマンドはどれですか?
A. cplic を印刷します
B. fwlic 印刷
C. ライセンスを表示
D. cplic 印刷
Answer: (解答を表示する)

最新問題: **162**
Gaia プラットフォーム上のユーザーを最もよく表すものを選択してください。
A. 削除できるデフォルト ユーザーが 1 人あります。
B. デフォルト ユーザーは 2 人あり、1 人は削除できません。
C. 削除できないデフォルト ユーザーが 2 人、SmartConsole 管理者が 1 人います。

D. 削除できないデフォルト ユーザーが 1 つあります。
Answer: B (メーッセージを残す**)**

最新問題**: 163**
空白を入力します。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リクエストから_____データを取得します。
A. 場所
B. ペイロード
C. 宛先
D. アイデンティティ
Answer: D (メーッセージを残す**)**
説明
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リクエストから ID データを取得します。RADIUS アカウンティングは、ユーザーによるネットワーク サービスのリソース使用量を追跡および測定できる機能です。通常、ネットワーク アクセス サーバー (NAS) であるアカウンティング クライアントは、開始時間と終了時間、送受信バイト数、IP アドレスなどのユーザー セッションに関する情報を含むアカウンティング リクエストを RADIUS サーバーに送信します。RADIUS サーバーはこれを記録します。請求、監査、またはレポートの目的でデータベース内の情報を収集します。アカウンティング クライアントがすべてのアカウンティング リクエストに含める必要がある必須属性の 1 つは、ネットワーク サービスにアクセスしているユーザーを識別する User-Name 属性です。

最新問題**: 164**
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. システムのバックアップ
B. 設定の保存
C. 移行
D. スナップショット
Answer: (解答を表示する**)**
説明
Hewlett Packard Enterprise Support Center3 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。スナップショットは、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る、ディスク パーティションの特定時点のコピーです。参考資料: Hewlett Packard Enterprise サポート センター

最新問題**: 165**
ローミング ユーザーに ID 認識を導入する最良の方法は何ですか?
A. アイデンティティ エージェントを使用する
B. ゲートウェイ間でユーザー ID を共有します
C. キャプティブ ポータルを使用する
D. オフィス モードを使用する
Answer: A (メーッセージを残す**)**

最新問題: **166**
R80 では、異なる Check Point コンポーネント間の通信はどのように保護されますか? 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 を使用する
B. SIC を使用する
C. ICA を使用する
D. 3DES を使用する
Answer: B (メーッセージを残す**)**
説明
R80 では、SIC を使用して、異なる Check Point コンポーネント間の通信が保護されます。SIC は Secure Internal Communication の略で、Security Gateway、Security Management Server、Log Server などの Check Point コンポーネント間の通信の信頼性と機密性を保証するメカニズムです。SIC は内部 CA (ICA) によって発行された証明書を使用し、AES-25634 などの暗号化アルゴリズム。参考資料: Check Point R81 Quantum Security Gateway ガイド、Check Point R81 Quantum Security Management 管理ガイド

最新問題: **167**
ClusterXL を使用すると、スティッキー決定関数について正しいのはどれですか?
A. すべての接続はピボットによって処理され、同期されます。
B. 負荷共有実装の場合のみ変更可能
C. SecureXL を使用する場合にのみ関係します。
D. cpconfig を使用して構成されます
Answer: B (メーッセージを残す**)**

最新問題: **168**
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 レポートと矛盾していることが判明した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ルールをすべて削除します。
D. Security Gateway の重複したログ エントリを削除するには
Answer: A (メーッセージを残す**)**
これらは、すべてのルール ベースに対して推奨される基本的なアクセス コントロール ルールです。
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。

最新問題: **169**
ファイアウォール クラスタには 2 つの R77.30 セキュリティ ゲートウェイがあります。これらの名前は FW_A および FW_B です。クラスターは、デフォルトのクラスター構成で HA (高可用性) として機能するように構成されています。FW_A は FW_B よりも高い優先順位を持つように構成されています。FW_A は午前中にアクティブでトラフィックを処理していました。FW_B がスタンバイしていました。午前 11:00 頃、インターフェイスがダウンし、フェイルオーバーが発生しました。FW_B がアクティブになりました。1 時間後、FW_A のインターフェイスの問題は解決され、動作できるようになりました。
クラスターに再参加すると、自動的にアクティブになりますか?
A. はい、グローバル プロパティで [優先度の高いクラスター メンバーに切り替える] オプションがデフォルトで有効になっているため、
B. いいえ、グローバル プロパティで 「現在のアクティブなクラスター メンバーを維持する」オプションがデフォルトで有効になっているため、
C. はい。クラスター オブジェクト プロパティの [優先度の高いクラスター メンバーに切り替える] オプションがデフォルトで有効になっているためです。
D. いいえ、クラスター オブジェクト プロパティの 「現在のアクティブなクラスター メンバーを維持する」オプションがデフォルトで有効になっているため、
Answer: (解答を表示する)

最新問題: **170**
SmartView Tracker を使用している間、Brady は、侵入の可能性があると思われる非常に奇妙なネットワーク トラフィックに気づきました。彼は 60 分間交通を遮断することにしましたが、手順をすべて思い出せません。ブロックを設定するために必要な手順の正しい順序は何ですか?
1)SmartView Tracker で [アクティブ モード] タブを選択します。
2) [ツール] > [侵入者をブロック] 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: (解答を表示する)

最新問題: **171**
ヴァネッサは Gaia Web ポータルにログインしようとしています。彼女は正常にログインできます。次に、SmartConsole に対して同じユーザー名とパスワードを試みますが、下のスクリーンショット画像のメッセージが表示されます。彼女は、サーバーの IP アドレスが正しいこと、および Gaia へのログインに使用したユーザー名とパスワードも正しいことを確認しました。

最も考えられる理由は何ですか?

A. Check Point Management ソフトウェアの認証詳細は、オペレーティング システムの認証詳細と自動的には同じになりません。彼女が正しい詳細を使用していることを確認してください。

B. スーパー管理者が最初にログインし、他の管理者セッションをクリアするまで、Vanessa に対して SmartConsole 認証は許可されません。

C. Check Point R80 SmartConsole 認証は以前のバージョンよりも安全であり、Vanessa には 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。

D. Gaia ではこれらのチェックに合格しましたが、新しい脅威対策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: A (メーッセージを残す**)**

最新問題**: 172**

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迅速にブロックするために、Security Gateway で SAM ルールが必要な場合、管理者はどのようなアクションを実行する必要がありますか?

A. SmartView モニターを開くと、SAM ルールをすぐに適用できます。ポリシーのインストールは必要ありません。

B. ポリシー タイプ SAM をポリシー パッケージに追加し、新しい SAM ルールを適用する必要があります。変更を公開するだけで、ファイアウォールに SAM ルールが適用されます。

C. 管理者はファイアウォール CLI (SSH や PuTTY など) で作業する必要があり、コマンド 'sam block' を正しいパラメーターとともに使用する必要があります。

D. 管理者は、[ログとモニター] ビューを開いて、関連するログを見つける必要があります。ログ エントリを右クリックすると、[新しい SAM ルールの作成] オプションが表示されます。

Answer: A (メーッセージを残す**)**

SAM が有効になっている Security GatewayClosed には、セキュリティ ポリシーClosed によって制限されていない疑わしい接続をブロックするファイアウォール ルールがあります。これらのルールはすぐに適用されます (ポリシーのインストールは必要ありません)。https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_LoggingAndMonitoring_AdminGuide/Topics-LMG/Monitoring-Suspicious-Activity-Rules.htm

最新問題**: 173**

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: (解答を表示する**)**
説明
専用の R80 SmartEvent サーバーのルート パーティションの推奨サイズは少なくとも 20GB2 であるため、正解は D です。20 GB 未満、または 10 GB を超え 20 GB 未満のいずれのサイズも、SmartEvent サーバーには十分ではありません。参考資料: 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**: 174**
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. クラウドベースのインストール
B. SmartUpdate のインストール
C. Check Point ISOMorphic で作成された USB メディア
D. Check Point ISOMorphic で作成された DVD メディア
Answer: (解答を表示する**)**

最新問題**: 175**
3 つのゲートウェイを使用して VPN コミュニティ NPN ストアをセットアップしました。1 つのリモート ゲートウェイ (I .1.1.1) とローカル ゲートウェイにいくつかの問題があります。両方のゲートウェイの IKE フェーズ 2 で合意されたネットワークのみを表示する最適なログ フィルターは何ですか。
A. アクション: 「キーのインストール」および 1.1.1.1 およびクイック モード
B. ブレード: 「VPN」AND VPN ストア AND メイン モード
C. アクション: 「キーのインストール」 AND 1.1.1.1 AND メイン モード
D. ブレード: 「VPN」AND VPN ストア AND クイック モード
Answer: A (メーッセージを残す**)**
説明
このログ フィルタは、「キーのインストール」アクションを持つログのみを表示します。これは、Security Gateway が VPN トンネル 1 に新しい暗号化キーをインストールしたことを意味します。また、IP アドレス 1.1.1.1 を持つログのみも表示されます。これは、問題のあるリモート ゲートウェイです。最後に、クイック モードを持つログのみが表示されます。これは、両方のゲートウェイで合意されたネットワークを確立する IKE フェーズ 2 ネゴシエーションです2。
他のログ フィルターは、ゲートウェイ 2 間に安全なチャネルを確立する IKE フェーズ 1 ネゴシエーションであるメイン モードが含まれているか、リモート ゲートウェイの IP アドレスを指定していないため、正しくありません。
* ロギングとモニタリング R81.20 管理ガイド
* リモート アクセス VPN R81.20 管理ガイド
* リモート アクセス VPN R81 管理ガイド

最新問題**: 176**
Application Control の機能や利点ではないものは次のうちどれですか?

A. ネットワーク内の不明なアプリケーションや不要なアプリケーションを排除して、IT の複雑さとアプリケーションのリスクを軽減します。
B. IT 環境内にあるアプリケーションと IT 環境に追加するアプリケーションを識別して制御します。
C. ポリシーを決定するために、ユーザーがダウンロードしているファイルの内容をスキャンします。
D. 実行権限を持つ信頼できるソフトウェアを自動的に識別します
Answer: C (メーッセージを残す**)**
説明
Application Control は、管理者がアプリケーションや Web サイトへのアクセスをユーザー、グループ、マシン、時間ごとに制御できるようにするブレードです。Application Control は、ネットワーク内の未知の不要なアプリケーションを排除して IT の複雑さとアプリケーションのリスクを軽減し、IT 環境内にあるアプリケーションと IT 環境に追加するアプリケーションを識別して制御し、実行権限のある信頼できるソフトウェアを自動的に識別します1。ただし、Application Control は、ポリシーを決定するためにユーザーがダウンロードしているファイルの内容をスキャンできません。これは、コンテンツ認識と呼ばれる別のブレードの機能であり、タイプ、サイズ、名前、データに基づいてファイルを検査できます2。参考資料: Check Point R81 アプリケーション コントロール管理ガイド、Check Point R81 コンテンツ アウェアネス管理ガイド

最新問題**: 177**
Security Gateway で SNX を構成しました。クライアントは Security Gateway に接続し、ユーザーは認証資格情報を入力します。
クライアントが Security Gateway の VPN ドメインに接続できるようにする認証の後は、何が起こる必要がありますか?
A. SNX クライアント アプリケーションがクライアントにインストールされている必要があります。
B. オフィス モード アドレスはクライアントによって取得される必要があります。
C. SNX はルーティング テーブルを変更して、VPN トラフィックを Security Gateway に転送します。
D. Active-X がクライアントで許可されている必要があります。
Answer: C (メーッセージを残す**)**

最新問題**: 178**
以下のルールをご覧ください。左の列のペンのマークは何を意味しますか?

3	HR can access to social network applications	HR	Internet
4	All employees can access YouTube for work purposes	Corporate LANs Branch Office LAN Data Center LAN	Internet

A. 現在、別のユーザーがルールの編集をロックしています。
B. 構成ロックが存在します。ロックを取得するには、ペンのシンボルをクリックします。
C. ログインした管理者によってルールが編集されましたが、ポリシーはまだ公開されていません。
D. これらのルールは現在のセッションで公開されています。
Answer: C (メーッセージを残す**)**

最新問題: **179**
空白を埋めてください: ライセンスをインストールするには、まずライセンスを _____ 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. ライセンスおよび契約リポジトリ
Answer: D (メーッセージを残す)
説明
ライセンスをインストールするには、まずライセンスと契約リポジトリにライセンスを追加する必要があります。ライセンスおよび契約リポジトリは、Check Point 製品のすべてのライセンスと契約を保存する集中データベースです。
これにより、Check Point 製品のライセンスを管理、アクティベート、およびアタッチできます。
参考資料: Check Point Security Management 管理ガイド R81、p.10 19-20

最新問題: **180**
アクセス ロールにより、ファイアウォール管理者は次に従ってネットワーク アクセスを構成できます。
A. リモート アクセス クライアント。
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. ユーザーとユーザー グループ。
D. 上記のすべて。
Answer: (解答を表示する)
説明
アクセス ロールを使用すると、ファイアウォール管理者は、リモート アクセス クライアント、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、およびユーザーとユーザー グループに従ってネットワーク アクセスを構成できます12。したがって、正解は D です。

最新問題: **181**
セキュリティを強化するために、管理者はコア保護の 「ホスト ポート スキャン」の事前定義感度を 「中」から 「高」に変更しました。変更を公開した後、管理者はどのポリシーをインストールする必要がありますか?
A. アクセス制御および脅威防止ポリシー。
B. アクセス制御ポリシー。
C. アクセス制御および HTTPS 検査ポリシー。
D. 脅威防御ポリシー。
Answer: D (メーッセージを残す)
https://supportcenter.checkpoint.com/supportcenter/portal?action=portlets.SearchResultMainAction&eventSubmit_doGoviewsolutiondetails=&solutionid=sk110873

最新問題: **182**
Wade がユーザー、グループ、マシンの可視性を提供しながら、ID ベースのポリシーによるアクセス制御も提供する Check Point ソフトウェアはどれですか?
A. ファイアウォール
B. URL フィルタリング
C. アイデンティティの認識
D. アプリケーション制御
Answer: (解答を表示する**)**

最新問題: **183**
_____ NAT では、_____ が変換されます。
A. シンプル。ソース
B. 非表示; 行き先
C. 静的。ソース
D. 非表示; ソース
Answer: D (メーッセージを残す**)**

最新問題: **184**
セキュリティを強化するために、管理者はコア保護の 「ホスト ポート スキャン」を 「中」から 「中」に変更しました。
「高」の事前定義された感度。変更を公開した後、管理者はどのポリシーをインストールする必要がありますか?
A. アクセス制御および脅威防止ポリシー。
B. アクセス制御ポリシー。
C. アクセス制御および HTTPS 検査ポリシー。
D. 脅威防御ポリシー。
Answer: (解答を表示する**)**
説明
セキュリティを強化するために、管理者はコア保護の 「ホスト ポート スキャン」を 「中」から 「中」に変更しました。
「高」の事前定義された感度。管理者は、変更を公開した後、脅威対策ポリシーをインストールする必要があります3。脅威防御ポリシーは、Security Gateway がポート スキャン、ボット攻撃、ゼロデイ エクスプロイトなどの脅威を検査して保護する方法を定義します4。参考資料: Check Point R81 ファイアウォール管理ガイド、Check Point R81 脅威対策管理ガイド

最新問題: **185**
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. 尊重されます
C. cpm
D. cpd

Answer: A (メーッセージを残す)
説明
fwd デーモンが FW CLI コマンドを担当するため、正解は A です3。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、Security Management サーバーと SmartConsole 間の通信を処理します。cpd デーモンは、Security Gateway 上の重要なプロセスのステータスを監視します。参考資料: Check Point ファイアウォールのプロセスとデーモン

最新問題**: 186**
WebUI のどのアイコンが読み取り/書き込みアクセスが有効であることを示していますか?
A. 鉛筆
B. 南京錠
C. 本
D. 眼鏡
Answer: A (メーッセージを残す)
説明
読み取り/書き込みアクセスが有効であることを示す WebUI のアイコンは、鉛筆アイコン です。デバイスが読み取り/書き込みモードの場合、デバイス名の横に鉛筆アイコンが表示され、設定を変更できます。南京錠アイコンは、読み取り専用アクセスが有効になっていて、構成を変更できないことを示します。ブック アイコンは、WebUI の使用に関する情報とガイダンスを提供するオンライン ヘルプが利用可能であることを示します。眼鏡アイコンは、ログインせずに設定を表示できる表示専用モードが有効になっていることを示します。
参考資料: Gaia R81.10 管理ガイド、WebUI の概要

最新問題**: 187**
スタンドアロン インストールを実行する場合、他の Check Point アーキテクチャ コンポーネントと一緒に Security Management Server を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. セキュアクライアント
D. スマートイベント
Answer: (解答を表示する)

最新問題**: 188**
ルールを見直してください。ドメイン UDP が暗黙のルールで有効になっていると仮定します。

No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	User Auth	Log	Policy Targets
2	0		Any	Any	Any Traffic	Any	accept	None	Policy Targets

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参照しようとするとどうなりますか? ユーザー :
A. 認証を求められずにインターネットに接続できます。
B. インターネットに正常に接続する前に、プロンプトが 3 回表示されます。
C. 認証後、インターネットに正常に接続できます。
D. クライアント認証デーモンのポート 259 に Telnet 接続した後、インターネットに接続できます。

Answer: (解答を表示する)

最新問題: **189**
ログとモニタリングでは、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どれですか?
A. 会計
B. 抑制
C. アカウンティング/抑制
D. アカウンティング/拡張
Answer: C (メーッセージを残す)

最新問題: **190**
Check Point Capsule のコンポーネントではないものは次のうちどれですか?
A. カプセルワークスペース
B. カプセルエンタープライズ
C. カプセル ドキュメント
D. カプセルクラウド
Answer: B (メーッセージを残す)

最新問題: **191**
サイト間 VPN にとって重要な属性は次のうちどれですか?
A. 強力なデータ暗号化
B. 一元管理
C. ユーザー グループに対応する拡張性
D. 強力な認証
Answer: A (メーッセージを残す)

最新問題: **192**
ログのクエリが非常に高速になった理由を最もよく説明するものを選択してください。
A. SmartConsole は Security Gateway から直接結果をクエリするようになりました。
B. 保存されるログの量は、古いバージョンの通常よりも少ないです
C. 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
D. 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。
Answer: D (メーッセージを残す)

最新問題: **193**
セントラル ライセンスが推奨されるライセンス方法であるのはなぜですか?
A. セントラル ライセンスは実際には Gaia ではサポートされていません。
B. Gaia を導入する場合は、集中ライセンスが唯一のオプションです
C. 集中ライセンスはゲートウェイの IP アドレスに関連付けられており、必要に応じて任意のゲートウェイに変更できます。

D. セントラル ライセンスは管理サーバーの IP アドレスに関連付けられており、ゲートウェイの IP アドレスが変更された場合でも依存しません。
Answer: (解答を表示する**)**
説明
中央ライセンスは、管理サーバーの IP アドレスに関連付けられ、変更された場合でもゲートウェイの IP に依存しないため、優先および推奨されるライセンス付与方法です。中央ライセンスを使用すると、管理者はすべての Security Gateway のライセンスを 1 つの中央の場所から管理できます。ゲートウェイの IP アドレスが変更されても、同じ管理サーバーに接続されている限りライセンスは有効です。
セントラル ライセンスは Gaia でサポートされていますが、Gaia を導入する際の唯一のオプションではありません。集中ライセンスはゲートウェイの IP アドレスに関連付けられていないため、必要に応じてゲートウェイを変更することはできません。
参考資料: 1: Rugged Appliances 2: SmartUpdate 3: Check Point ソフトウェア導入オプション:
[ウイルス対策] : [Check Point Software Blade] : [セントラル ライセンス]

最新問題**: 194**
安全なネットワークを構築するための 3 つの考慮事項は何ですか?
A. リモート、スタンドアロン、分散
B. スタンドアロン、分散、ブリッジ モード
C. 分散、ブリッジ モード、およびリモート
D. ブリッジ モード、リモート、スタンドアロン
Answer: C (メーッセージを残す**)**

最新問題**: 195**
現在の CPView ページをファイル名形式 cpview_"cpview process ID" で保存するために使用されるキー。キャップ 𠮟キャプチャ数」?
A. S
B. C
C. W
D. スペースバー
Answer: B (メーッセージを残す**)**

最新問題**: 196**
Secure Network Distributor (SND) はどのような点で Security Gateway に関連する機能ですか?
A. 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。
B. SND は複数の SSL VPN 接続を高速化する機能です
C. 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。
D. 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
Answer: A (メーッセージを残す**)**

最新問題: **197**
ID 認識では、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: B (メーッセージを残す**)**
説明
Identity Aware は、管理者が IP アドレスだけではなく、ユーザーとマシンの ID に基づいてアクセス ルールを定義できるようにするブレードです。ID 認識を使用すると、ネットワークの場所、ユーザーの ID、マシンの ID 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。
ネットワークの場所とは、トラフィックの送信元または宛先のネットワーク セグメントを指します。ユーザーの ID 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 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。参考文献:
[Check Point R81 ID 認識管理ガイド]

最新問題: **198**
R80 の有効な展開オプションではないものは次のうちどれですか?
A. ログサーバー
B. マルチドメイン管理サーバー
C. オールインワン (スタンドアロン)
D. スマートイベント
Answer: B (メーッセージを残す**)**

最新問題: **199**
IPS ブレードについての真実は何ですか?
A. R81 では、IPS レイヤーで可能なアクションは、Basic、Optimized、Strict の 3 つだけです
B. R81 では、IPS 例外を 「すべてのルール」に付加することはできません。
C. R81 では、GeoPolicy 例外と脅威対策例外は同じです
D. R81 では、IPS は脅威防御ポリシーによって管理されます。
Answer: D (メーッセージを残す**)**

最新問題: **200**
SSL VPN と IPSec VPN の違いは何ですか?

A. IPSec VPN には常駐 VPN クライアントのインストールは必要ありません
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 には常駐 VPN クライアントのインストールが必要ですが、SSL VPN に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)
説明
SSL VPN と IPSec VPN の違いは、IPSec VPN では常駐 VPN クライアントのインストールが必要であるのに対し、SSL VPN ではブラウザのインストールのみが必要であるという点です5。IPSec VPN は、事前共有キー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。参考資料: Check Point リモート アクセス VPN 管理ガイド R81、[Check Point CCSA の無料サンプル質問および学習ガイド]

最新問題**: 201**
MegaCorp のセキュリティ インフラストラクチャは、セキュリティ ゲートウェイを地理的に分離します。1 つのリモート Security Gateway に対して中央ライセンスをリクエストする必要があります。
ライセンスはどのように適用しますか?
A. Security Management Server の IP アドレスを使用し、SmartUpdate 経由でライセンスをリモート ゲートウェイにアタッチします。
B. リモート ゲートウェイの 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。
C. リモート ゲートウェイの IP アドレスを使用し、SmartUpdate 経由でライセンスをリモート ゲートウェイにアタッチします。
D. ゲートウェイの各 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。
Answer: A (メーッセージを残す)

最新問題**: 202**
空白を埋めてください: 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. 特定のサテライト ゲートウェイから中央ゲートウェイ トンネルへ
B. すべての衛星ゲートウェイから衛星ゲートウェイへのトンネル上
C. 特定のゲートウェイの特定のトンネル上
D. コミュニティ内の特定のトンネル上
Answer: D (メーッセージを残す)

最新問題**: 203**
WebUI には、CPUSE 経由でホットフィックスをダウンロードするための 3 つの方法が用意されています。その 1 つは自動メソッドです。
CPUSE エージェントは 1 日に何回ホットフィックスをチェックし、自動的にダウンロードしますか?
A. 3 時間ごと
B. 1 日あたり 6 回
C. 1 日 7 回
D. 2 時間ごと
Answer: (解答を表示する)

最新問題: **204**
メッシュとスターの 2 種類の VPN トポロジです。
この種のコミュニティに関し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、すべてのメンバーが他のメンバーとトンネルを作成できます。
B. スター コミュニティには、Check Point 独自のテクノロジーである Check Point ゲートウェイが必要です。
C. メッシュ コミュニティでは、メンバー ゲートウェイは相互に直接通信できません。
D. スター コミュニティでは、衛星ゲートウェイは相互に通信できません。
Answer: A (メーッセージを残す**)**

最新問題: **205**
SmartEvent では、相関ユニット (CU) は何を行うために使用されますか?
A. セキュリティ ゲートウェイ ログを収集し、ログにインデックスを付けて、ログを圧縮します。
B. リージョン内のファイアウォールおよびその他のソフトウェア ブレードのログを受信し、プライマリ ログ サーバーに転送します。
C. ログ エントリを分析し、イベントを特定します。
D. DOS 攻撃中に SAM ブロック ルールをファイアウォールに送信します。
Answer: (解答を表示する**)**
説明
相関ユニット (CU) は、ログ サーバー上のログ エントリを分析し、事前定義またはカスタム ルール 1 に基づいてイベントを識別する SmartEvent のコンポーネントです。CU は 1 つ以上のログ サーバーからログを受信し、それらを SmartEvent サーバーに転送し、そこでイベント データベースに保存されます。

最新問題: **206**
スプーフ トラッキングを構成する場合、管理者はスプーフされたパケットが検出されたときに実行するトラッキング アクションを選択できますか?
A. ログ、SNMP トラップ、電子メールの送信
B. パケットのドロップ、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、メール送信
Answer: C (メーッセージを残す**)**
説明
スプーフ トラッキングを構成するとき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 トラッキングは、スプーフィングされた送信元 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ときに、ログのみを記録するか、ログを記録して警告するか、何もしないかを選択できます。他のオプションは、利用できないか、この機能に関連していないため、スプーフ トラッキングの有効なトラッキング アクションではありません。
参考文献: [スプーフィング追跡]、[ファイアウォール管理ガイド]

最新問題: **207**

管理者がネットワーク リソースへのアクセスを制限し、特定のユーザーが特定のネットワーク上にいる場合にのみアクセスを許可したい場合、これを実現する最善の方法は何でしょうか?
A. 宛先がターゲット ネットワーク リソースであるインライン レイヤーを作成します。特定のソースのみがターゲット リソースにアクセスできるようにするサブルールを定義します。
B. 「場所の新しいレガシー ユーザー」を使用し、目的の場所でユーザーが属する LDAP ユーザー グループを指定します。
C. 特定の送信元 IP アドレスのみがターゲット ネットワーク リソースにアクセスできるようにするルールを作成します。
D. 特定のユーザーまたはユーザー グループを指定し、特定のネットワークを定義して、アクセス ロール オブジェクトを作成します。このアクセス ロールをアクセス コントロール ルールの「ソース」として使用します。
Answer: D (メーッセージを残す)
説明
ネットワーク リソースへのアクセスを制限し、特定のユーザーが特定のネットワーク上にいる場合にのみアクセスを許可する最善の方法は、特定のユーザーまたはユーザー グループを指定し、特定のネットワークを定義してアクセス ロール オブジェクトを作成することです。次に、このアクセス ロールをアクセス コントロール ルールの「ソース」として使用します。これにより、ユーザー ID と場所に基づいてネットワーク トラフィックをきめ細かく制御できるようになります3。
参考資料: 3: Check Point R81 Security Gateway 管理ガイド、13 ページ。

最新問題**: 208**
アクセス ロールにより、ファイアウォール管理者は次に従ってネットワーク アクセスを構成できます。
A. 上記のすべて
B. ユーザーとユーザー グループ
C. リモート アクセス クライアント
D. コンピュータ グループとネットワークの組み合わせ
Answer: A (メーッセージを残す)

最新問題**: 209**
Gaia Web インターフェイスから、セキュリティ管理サーバーで実行できない操作は次のうちどれですか?
A. 静的ルートを追加します
B. セキュリティ ポリシーを確認する
C. ターミナル シェルを開きます
D. セキュリティ管理 GUI クライアントの表示
Answer: C (メーッセージを残す)

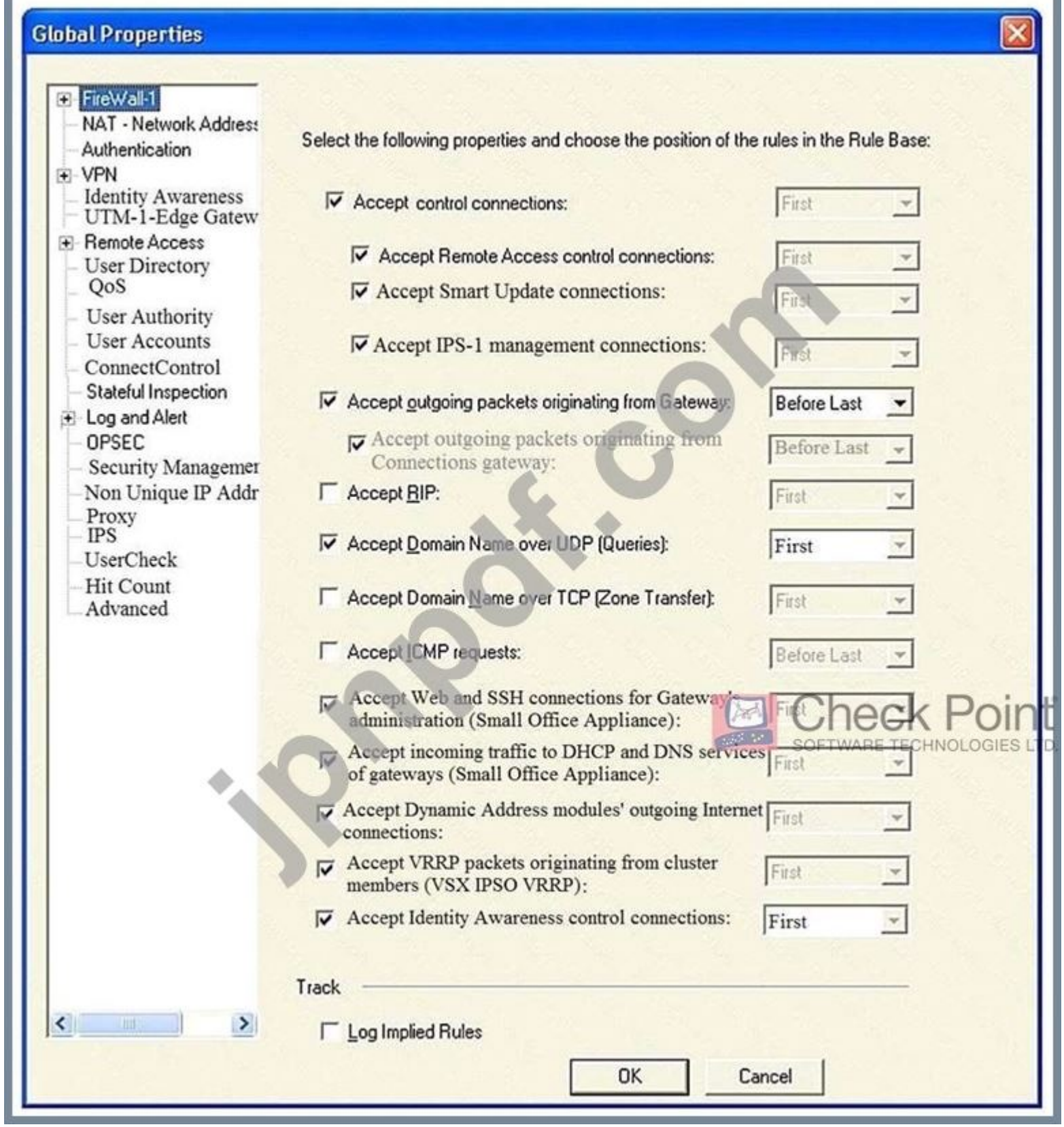
最新問題**: 210**
セキュリティ ポリシーを変更するために、管理者は次のどのツールを使用できますか? 最良の回答を選択してください。
A. Security Gateway 上の mgmt_cli または WebUI、および Security Management Server 上の SmartConsole。
B. Security Management Server 上の SmartConsole と WebUI。
C. SmartConsole がインストールされているコンピューター上の SmartConsole または mgmt_cli。
D. Security Management Server のコマンド ライン、または Windows コンピュータ上の mgmt_cli.exe。
Answer: C (メーッセージを残す)

最新問題: **211**
クラスタ メンバー間の完全な同期は、ファイアウォール カーネルによって処理されます。これにはどのポートが使用されますか?
A. UDP ポート 256
B. UDP ポート 265
C. TCP ポート 256
D. TCP ポート 265
Answer: (解答を表示する**)**

最新問題: **212**
「ヒット カウント」機能を使用すると、各ルールに一致する接続の数を追跡できます。
追跡オプションが「なし」に設定されている場合でも、ヒット カウント機能はロギングとは独立して動作し、ヒットを追跡しますか?
A. はい、ヒット カウントを有効にすると、SMS がサポートされているセキュリティ ゲートウェイからデータを収集するため、独立して機能します。
B. はい、Security Gateway で「すべてのルールを分析」チェックボックスが有効になっている限り、独立して機能します。
C. いいえ、ヒット カウントではすべてのルールをログに記録する必要があるため、単独では機能しません。
D. いいえ、単独では動作しません。ヒット数は、追跡オプションがログまたはアラートとして設定されているルールに対してのみ表示されます。
Answer: (解答を表示する**)**

最新問題: **213**
Application Control の機能や利点ではないものは次のうちどれですか?
A. IT 環境内にあるアプリケーションと IT 環境に追加するアプリケーションを識別して制御します。
B. 実行権限を持つ信頼できるソフトウェアを自動的に識別します
C. ネットワーク内の不明なアプリケーションや不要なアプリケーションを排除して、IT の複雑さとアプリケーションのリスクを軽減します。
D. ポリシーを決定するために、ユーザーがダウンロードしているファイルのコンテンツをスキャンします。
Answer: D (メーッセージを残す**)**

最新問題: **214**
グローバル プロパティの次の設定を考慮してください。



選択したオプション "UDP 経由の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、外部スプーフィング防止トポロジ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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。

B. すべての UDP クエリは、すべてのインターフェイスを介して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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。

C. すべてのインターフェイスを介して許可されるトラフィックでは 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 ポリシーに最初に記述する明示的なルールの前に行われます。
D. すべての UDP クエリは、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: A (メーッセージを残す**)**
説明
選択したオプション「UDP 経由のドメイン名を受け入れる (クエリ)」は、外部スプーフィング防止トポロジ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 UDP クエリが受け入れられることを意味します。これは、管理者がセキュリティ ポリシーに最初の明示的なルールを書き込む前に行われます。このオプションを使用すると、Security Gateway が外部ホストからの 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 ポリシーの明示的なルールの前に適用される暗黙的なルールによって受け入れられます。暗黙のルールでは、外部のスプーフィング防止グループが定義されているインターフェイスからのクエリのみが許可されます。参考文献: Check Point R81 Quantum Security Gateway ガイド、暗黙のルール

最新問題**: 215**
新しいライセンスをいつ生成する必要がありますか?
A. ライセンスがアップグレードされた場合のみ。
B. 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場合の RMA 手順後。
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、ライセンスが関連付けられている IP アドレスが変更されます。
D. 契約ファイルをインストールする前。
Answer: B (メーッセージを残す**)**

最新問題**: 216**
ゲートウェイと Security Management Server の間で最初に信頼を作成するために使用されるのは次のうちどれですか?
A. 内部認証局
B. トークン
C. ワンタイムパスワード
D. 証明書
Answer: (解答を表示する**)**
説明
ワンタイム パスワードは、最初にゲートウェイと Security Management Server の間に信頼を確立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 コマンド ライン インターフェイスに入力します。これにより、ゲートウェイとサーバーの間に安全な内部通信 (SIC) が確立されます。他のオプションはこの目的には使用されません。参考文献: [セキュア内部通信 (SIC) の構成]、[Check Point CCSA - R81: 模擬テストと解説]

最新問題**: 217**
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ない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. ThreatWiki
B. ホワイトリスト ファイル

C. AppWiki
D. IPS 保護
Answer: A (メーッセージを残す**)**
説明
ThreatWiki は、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で、管理者は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脅威対策ブレードに指定できます3。ThreatWiki は、Check Point の顧客、パートナー、研究者などの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表示し、分析のためにファイルをアップロードし、侵害の指標をダウンロードできます3。ホワイトリスト ファイル、AppWiki、および 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。参考資料: 脅威対策 R80.40 管理ガイド

最新問題**: 218**
新しいポリシー レイヤを作成する場合、どのようなデフォルト レイヤが含まれますか?
A. ファイアウォール、アプリケーション制御、および IPS
B. ファイアウォール、アプリケーション コントロール、および IPSec VPN
C. アクセス制御、脅威防止、および HTTPS 検査
D. アプリケーション制御、URL フィルタリング、および脅威防御
Answer: C (メーッセージを残す**)**

最新問題**: 219**
Capsule Connect と Capsule Workspace の違いは何ですか?
A. Capsule Connect はレイヤー3 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. Capsule Workspace は任意のアプリケーションへのアクセスを提供できます
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: A (メーッセージを残す**)**
説明
Capsule Connect は、ユーザーがモバイル デバイスから企業リソースに安全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、ビジネス データおよびアプリケーションを個人データおよびアプリケーションから分離する安全なコンテナをモバイル デバイス上に提供します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。参考資料: Check Point Capsule Connect、Check Point Capsule Workspace

最新問題**: 220**
セキュリティ ゾーンは、どの種類の定義されたルールでは機能しませんか?
A. アプリケーション制御ルール
B. 手動 NAT ルール
C. IPS バイパス ルール
D. ファイアウォール ルール
Answer: B (メーッセージを残す**)**

https://community.checkpoint.com/t5/Management/Workaround-for-manual-NAT-when-security-zones-are-used/td-p/9915

最新問題**: 221**
パケット アクセラレーション (SecureXL) は、いくつかの属性によって接続を識別します。
接続の識別に使用されない属性はどれですか?
A. 宛先アドレス
B. TCP 確認番号
C. 送信元ポート
D. 送信元アドレス
Answer: B (メーッセージを残す**)**

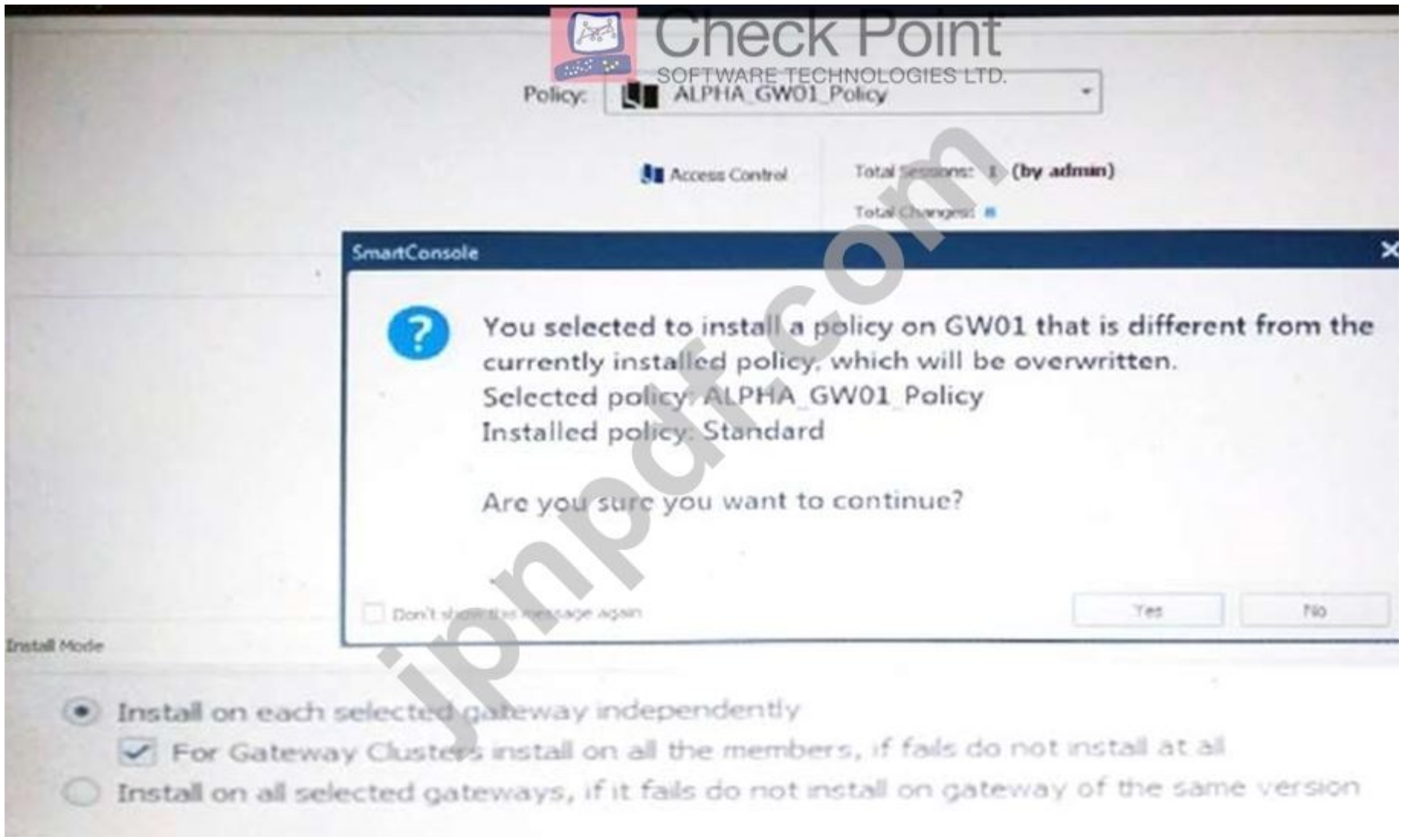
最新問題**: 222**
HTTPS 検査ポリシーを構成するにはどのような手順を実行しますか?
A. SmartDashboard で [管理と設定] > [ブレード] > [HTTPS 検査] > [構成] に移動します。
B. [アプリケーションと URL フィルタリング] ブレード > [詳細設定] > [HTTPS 検査] > [ポリシー] に移動します。
C. [管理と設定] > [ブレード] > [HTTPS 検査] > [ポリシー] に移動します。
D. [アプリケーションと URL フィルタリング] ブレード > [HTTPS 検査] > [ポリシー] に移動します。
Answer: C (メーッセージを残す**)**
説明
HTTPS 検査ポリシーを設定する手順は次のとおりです34:
管理と設定」に移動 >
[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。
ルールのソースと宛先を定義します。アクションは、検査、バイパス、または確認のいずれかです。
[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。参考文献: HTTPS インスペクション R81 管理ガイド、Check Point CCSA - R81: 実践テストと解説

最新問題**: 223**
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ぐ Check Point 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. スパム対策と電子メールのセキュリティ
D. ウイルス対策
Answer: D (メーッセージを残す**)**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_ThreatPrevention_AdminGuide/Topics-TPG/The_Check_Point_ThreatCloud.htm

最新問題**: 224**
GAiA 管理 CLI を使用して IP アドレス 10.50.23.90 の「emailserver1」ホストを追加するには、正しいコマンド構文を選択してください。

A. ホスト名 emailserver1 ip-address 10.50.23.90 を追加します。
B. 管理はホスト名を追加します emailserver1 ip-address 10.50.23.90
C. 管理はホスト名 IP アドレス 10.50.23.90 を追加します
D. ホスト名 myHost12 IP アドレス 10.50.23.90
Answer: B (メーッセージを残す**)**

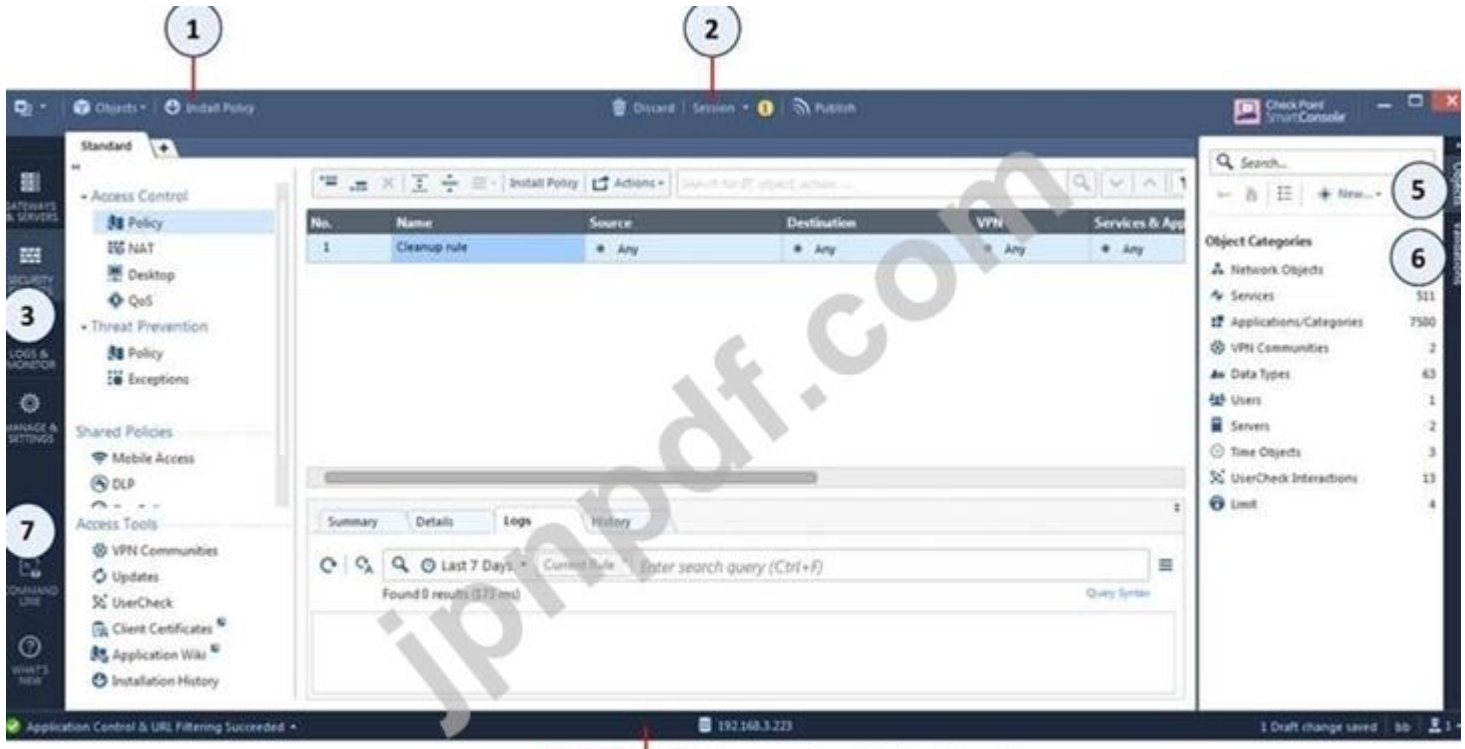
最新問題**: 225**
管理者に以下のメッセージが表示されるのはなぜですか?



A. ゲートウェイで作成された新しいポリシー パッケージは、既存の管理にインストールされます。
B. 管理上で作成された新しいポリシー パッケージは、既存のゲートウェイにインストールされます。
C. ゲートウェイ上で作成され、管理に転送された新しいポリシー パッケージは、現在ゲートウェイ上にあるポリシー パッケージによって上書きされますが、ゲートウェイ上の定期的なバックアップから復元できます。
D. 管理とゲートウェイの両方で作成された新しいポリシー パッケージは削除されるため、続行する前に最初にパッケージ化する必要があります。
Answer: B (メーッセージを残す**)**

最新問題**: 226**
R80 SmartConsole の有効なアプリケーション ナビゲーション タブではないものは次のうちどれですか?

A. 管理およびコマンドライン
B. ログとモニター
C. セキュリティ ポリシー
D. ゲートウェイとサーバー
Answer: (解答を表示する**)**
説明
管理とコマンド ライン」はインターフェイスに存在しないため、R80 SmartConsole の有効なアプリケーション ナビゲーション タブではありません。この画像は、R80 SmartConsole のナビゲーション ツールバーを示しています。これには 4 つのタブがあります。セキュリティ ポリシー、ログと監視、ゲートウェイとサーバー、管理と設定1。コマンド ライン インターフェイス ボタンは、ナビゲーション ツールバーではなく、システム情報領域にあります1。
参考資料: アプリケーション制御と URL フィルタリング - Check Point Software



Item	Description
1	Global Toolbar
2	Session Management Toolbar
3	Navigation Toolbar
4	System Information Area

Item	Description
5	Objects Bar (F11)
6	Validations pane
7	Command line interface button

最新問題: **227**
完了したステートメントのうち、真実でないものはどれですか? WebUI は、ユーザー アカウントの管理と次の目的に使用できます。
A. ユーザーに権限を割り当てます。
B. ユーザーのホーム ディレクトリを編集します。
C. ユーザーを Gaia システムに追加します。
D. Security Management Server のホーム ディレクトリにユーザー権限を割り当てます。
Answer: D (メーッセージを残す**)**
ユーザー
WebUI と CLI を使用してユーザー アカウントを管理します。あなたはできる：

最新問題: **228**
R80 では、異なる Check Point コンポーネント間の通信はどのように保護されますか? 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. ICA を使用する
B. IPSEC を使用する
C. 3DES を使用する
D. SIC を使用する
Answer: (解答を表示する**)**

最新問題: **229**
空白を埋めてください: _____情報は 「完全なログ」追跡オプションに含まれていますが、 「ログ」追跡オプションには含まれていませんか?
A. ファイル属性
B. アプリケーション
C. 宛先ポート
D. データ型
Answer: (解答を表示する**)**
追跡オプション

最新問題: **230**
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、同じセキュリティ管理サーバー (SMS) 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入力するボックスを見つけませんでした。なぜ事前共有秘密を指定できないのでしょうか?

A. 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。
B. 事前共有秘密はグローバル プロパティですでに構成されています
C. [すべての外部メンバーに対して共有シークレットのみを使用する] チェックボックスがオフになっています
D. ゲートウェイは SMB デバイスです
Answer: (解答を表示する**)**

最新問題**: 231**
Check Point ライセンスを表示および適用するにはどの GUI ツールを使用できますか?
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: (解答を表示する**)**
ライセンスを管理するには、SmartUpdate GUI が推奨される方法です。

最新問題**: 232**
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: (解答を表示する**)**
説明
Security Management Server と Security Gateway は、Check Point Security Management Architecture にログを保存できるコンポーネントです。Security Management Server はログをデータベースに保存し、外部のログ サーバーに転送することもできます。Security Gateway は、ログをローカルのバッファまたはローカル ログ ファイルに保存したり、Security Management Server やログ サーバーに送信したりできます。
参考資料: Check Point Security Management 管理ガイド R81、p.10 11-12

最新問題**: 233**
空白を埋めてください: デフォルトでは、R81 Management Server によって発行される SIC 証明書は _____ アルゴリズムに基づいています。
A. SHA-256
B. SHA-200
C. SHA-128
D. MD5
Answer: A (メーッセージを残す**)**

最新問題**: 234**

管理者は、ポリシーのルールでアプリケーション オブジェクトを使用したいと考えていますが、ルールの [サービスとアプリケーション] 列に新しい項目を追加するために [+] をクリックするときに、追加するオプションとしてアプリケーション オブジェクトがリストされていません。これを修正するにはどうすればよいでしょうか?
A. 管理者は、必要なアプリケーション オブジェクトをオブジェクト エクスプローラーから新しいルールにドラッグ アンド ドロップする必要があります。
B. 「アプリケーション コントロール」ブレードはゲートウェイで有効にする必要があります
C. まず、ルールが作成されているポリシー層で 「アプリケーションと URL フィルタリング」を有効にする必要があります。
D. 管理者はまず、ルールに追加するアプリケーションをいくつか作成する必要があります。
Answer: C (メーッセージを残す)
説明
ルールでアプリケーション オブジェクトを使用するには、ルールが作成されているポリシー レイヤーで [アプリケーションと URL フィルタリング] ブレードを有効にする必要があります。ゲートウェイ上で 「Application Control」ブレードを有効にするだけでは十分ではありません3.
参考資料: 3: Check Point R81 セキュリティ管理管理ガイド、102 ページ。

最新問題**: 235**
CLI からソフトウェアのバージョンを確認するにはどうすればよいでしょうか?
A. FW 統計
B. cpinfo
C. FW バージョン
D. FW モニター
Answer: (解答を表示する)

最新問題**: 236**
空白を埋めてください。LDAP が Check Point Security Management と統合されると、_____ と呼ばれます。
A. ユーザー センター
B. ユーザー管理
C. ユーザーディレクトリ
D. ユーザーチェック
Answer: C (メーッセージを残す)
説明
LDAP が Check Point Security Management と統合されると、それはユーザー ディレクトリと呼ばれます。ユーザー ディレクトリは、管理者が Active Directory2 などの外部 LDAP サーバーからユーザーとユーザー グループを管理できるようにする機能です。
参考資料: 2: Check Point R81 Identity Awareness 管理ガイド、9 ページ。

最新問題**: 237**
あなたは、会社のビジネス パートナーの 1 つとサイト間 VPN を構成しようとしているときに、フェーズ 2 の交渉が失敗したと考えています。
疑わしいもの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 ステータス

B. SmartView トラッカー
C. スマートダッシュボード
D. スマートアップデート
Answer: B (メーッセージを残す)

最新問題**: 238**
グローバル プロパティの次の設定を考慮してください。
選択したオプション "UDP 経由の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、外部スプーフィング防止トポロジ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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。
B. すべての UDP クエリは、すべてのインターフェイスを介して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、管理者によってセキュリティ ポリシーに最初の明示的なルールが書き込まれる前に行われます。
C. すべてのインターフェイスを介して許可されるトラフィックでは 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 ポリシーに最初に記述する明示的なルールの前に行われます。
D. すべての UDP クエリは、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: A (メーッセージを残す)
説明
選択したオプション "UDP 経由のドメイン名を受け入れる (クエリ)"は、外部スプーフィング防止トポロジ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 UDP クエリが受け入れられることを意味します。これは、管理者がセキュリティ ポリシーに最初の明示的なルールを書き込む前に行われます。このオプションを使用すると、Security Gateway が外部ホストからの 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 ポリシーの明示的なルールの前に適用される暗黙的なルールによって受け入れられます。暗黙のルールでは、外部のスプーフィング防止グループが定義されているインターフェイスからのクエリのみが許可されます。参考文献: Check Point R81 Quantum Security Gateway ガイド、暗黙のルール

最新問題**: 239**
CDT ユーティリティは次の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. すべてのアップグレード
C. R77.30 へのメジャー バージョン 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: B (メーッセージを残す)

最新問題**: 240**
SmartConsole のゲートウェイ ステータス ビューには、セキュリティ ゲートウェイとソフトウェア ブレードの全体的なステータスが表示されます。ステータス アテンションとは何を意味しますか?
A. Security Gateway に到達できません。
B. ゲートウェイとそのすべての Software Blade は正常に動作しています。
C. 少なくとも 1 つの Software Blade に軽微な問題がありますが、ゲートウェイは機能します。
D. Security Management Server と Security Gateway の間で SIC を作成できません

Answer: C (メーッセージを残す)
説明
ステータス アテンションは、少なくとも 1 つの Software Blade に軽微な問題があるが、ゲートウェイは動作していることを意味します1。たとえば、これは、ライセンスの有効期限切れの警告、ポリシーのインストールの失敗、ブレードのアクティベーションの問題などを示している可能性があります2。参考資料: Check Point R81 SmartConsole ガイド、Check Point R81 セキュリティ管理管理ガイド

最新問題**: 241**
URL フィルタリングは次の目的には使用できません。
A. 組織のセキュリティを向上させる
B. 制御帯域幅の問題
C. 法的責任の軽減
D. データ セキュリティの制御
Answer: B (メーッセージを残す)

最新問題**: 242**
暗黙のポリシーを受け入れる」が 最初」に設定されている場合、Jorge がログを表示できない理由は何ですか?
A. ログ暗黙ルールがルール ベースのトラック列に正しく設定されていませんでした。
B. 追跡ログ列が完全なログではなくログに設定されます。
C. 追跡ログ列はなしに設定されます。
D. グローバル プロパティで暗黙のルールのログが選択されていませんでした。
Answer: D (メーッセージを残す)
説明
暗黙のポリシーを受け入れる」が 最初」に設定されている場合、グローバル プロパティで暗黙のルールをログが選択されていないため、Jorge はログを表示できません。[暗黙のルールをログに記録する] オプションでは、DHCP、スプーフィング対策、クリーンアップ ルールなど、すべての暗黙のルールのログを有効にします。
参考資料: Check Point R81 セキュリティ管理管理ガイド、103 ページ。

最新問題**: 243**
ID 共有をサポートするために使用される 2 つの ID 認識デーモンはどれですか?
A. ポリシー起動ポイント (PAP) とポリシー決定ポイント (PDP)
B. ポリシー操作ポイント (PMP) およびポリシー起動ポイント (PAP)
C. ポリシー施行ポイント (PEP) およびポリシー操作ポイント (PMP)
D. ポリシー決定ポイント (PDP) とポリシー施行ポイント (PEP)

Answer: D (メーッセージを残す)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk88520

最新問題**: 244**
リアルタイム イベント監視用の SmartEvent R81 Web アプリケーションは次のように呼ばれます。
A. スマートイベントウェブ
B. SmartView モニター
C. SmartView
D. SmartEvent 用の Web アプリケーションはありません
Answer: (解答を表示する**)**

最新問題**: 245**
SmartConsole のどの部分で管理者はオブジェクトの追加、編集、削除、複製を行うことができますか?
A. オブジェクト エクスプローラー
B. オブジェクトエディタ
C. オブジェクト ブラウザ
D. オブジェクトナビゲータ
Answer: A (メーッセージを残す)

最新問題**: 246**
セッションを最もよく表すものを選択してください
A. セッションは編集のためにポリシー パッケージをロックします。
B. 管理者が SmartConsole で行われたすべての変更を公開すると開始します。
C. ポリシーが Security Gateway にプッシュされると、セッションが終了します。
D. 管理者が SmartConsole 経由でログインすると開始され、管理者がログアウトすると終了します。
Answer: D (メーッセージを残す)

最新問題**: 247**
パケットから詳細情報を抽出し、その情報を状態テーブルに保存するテクノロジーは次のうちどれですか?
A. 検査エンジン
B. 次世代ファイアウォール
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: B (メーッセージを残す)
説明
INSPECT エンジンは、パケットから詳細情報を抽出し、その情報を状態テーブルに保存するテクノロジーです。ステートフル インスペクションとアプリケーション層フィルタリングを有効にします12 参考資料: INSPECT エンジン、ステートフル インスペクション

最新問題**: 248**
暗号化時と同じキーを復号化に使用するのは次のうちどれですか?

A. 対称暗号化
B. 証明書ベースの暗号化
C. 非対称暗号化
D. 動的暗号化
Answer: A (メーッセージを残す**)**

最新問題**: 249**
ID 認識に使用される認証方法は次のうちどれですか?
A. SSL
B. PKI
C. RSA
D. キャプティブ ポータル
Answer: D (メーッセージを残す**)**

最新問題**: 250**
安全なネットワークを構築するための 3 つの考慮事項は何ですか?
A. 分散、ブリッジ モード、およびリモート
B. ブリッジ モード、リモート、スタンドアロン
C. リモート、スタンドアロン、分散
D. スタンドアロン、分散、ブリッジ モード
Answer: C (メーッセージを残す**)**
説明
安全なネットワークを構築するための 3 つの考慮事項は、リモート、スタンドアロン、分散です3。リモート展開とは、Security Management Server と Security Gateway が異なるマシンにインストールされることを意味します。スタンドアロン展開とは、Security Management Server と Security Gateway が同じマシンにインストールされることを意味します。分散展開とは、1 つ以上の Security Management Server によって管理される複数の Security Gateway が存在することを意味します3。したがって、正解は C. リモート、スタンドアロン、および分散です。

最新問題**: 251**
Check Point ライセンスには 2 つの形式があります。それらの形式は何ですか?
A. セキュリティ ゲートウェイとセキュリティ管理。
B. オンプレミスおよびパブリック クラウド。
C. アクセス制御と脅威防止。
D. 中央とローカル。
Answer: D (メーッセージを残す**)**

最新問題**: 252**
空白を埋めてください: ブラウザベースの認証は、ユーザーを Web ページに送信し、次を使用して ID を取得します。
_____。
A. キャプティブ ポータルと透過的な 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**)**
説明
ブラウザベースの認証では、ユーザーが Web ページに送信され、キャプティブ ポータルと透過的 Kerberos 認証を使用して ID を取得します。Captive Portal は、ユーザーに資格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 コントローラー 2 からの有効な Kerberos チケットを持つ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、認証用の Web ページではなく、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す。キャプティブ ポータルだけでは、ブラウザベースの認証で使用される方法の 1 つにすぎないため、空白を埋めるのに十分ではありません。

最新問題**: 253**
VPN ゲートウェイは、情報を交換する前に相互に認証する必要があります。認証に使用される 2 種類の資格情報は何ですか?
A. 3DES および MD5
B. 証明書と IPsec
C. IPsec および VPN ドメイン
D. 証明書と事前共有秘密
Answer: (解答を表示する**)**

最新問題**: 254**
空白を埋めてください: 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リクエストから _____ データを取得します
A. 宛先
B. アイデンティティ
C. ペイロード
D. 場所
Answer: (解答を表示する**)**
RADIUS アカウンティングと ID 認識の連携方法
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。

最新問題**: 255**
R77 Windows CD からインストールできる利用可能な SmartConsole クライアントは次のうちどれですか? すべての回答を読んで、最も完全で有効なリストを選択してください。
A. SmartView トラッカー、CPINFO、SmartUpdate
B. SmartView トラッカー、SmartDashboard、CPINFO、SmartUpdate、SmartView ステータス
C. SmartView トラッカー、SmartDashboard、SmartLSM、SmartView モニター
D. セキュリティ ポリシー エディター、ログ ビューアー、リアルタイム モニター GUI
Answer: A (メーッセージを残す**)**

最新問題: **256**
R80 Management の新しい API 統合を使用してオブジェクトを操作できる方法は次のうちどれですか?
A. Microsoft パブリッシャー
B. JSON
C. Microsoft Word
D. RC4 暗号化
Answer: (解答を表示する**)**
説明
R80 Management の新しい API 統合を使用してオブジェクトを操作できる方法は、JSON です。
JSON (JavaScript Object Notation) は、人間やマシンが簡単に読み書きできる軽量のデータ交換形式です。R80 Management API は、リクエストと応答の主要なデータ形式として JSON を使用します。したがって、正解は B.JSON です。

最新問題: **257**
推奨されるライセンス モデルは次のうちどれですか? 最良の回答を選択してください
A. 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 アドレスに結び付け、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 Security Management Server の IP アドレスに結び付け、ゲートウェイに依存しないため、集中ライセンス。
C. パッケージ ライセンスを Security Management Server の管理インターフェイスの MAC アドレスに結び付け、ゲートウェイに依存しないため、集中ライセンス。
D. パッケージ ライセンスをゲートウェイの IP アドレスに結び付け、セキュリティ管理サーバーに依存しないため、ローカル ライセンス。
Answer: B (メーッセージを残す**)**

最新問題: **258**
帯域幅とトラフィック制御ルールを適用するためにどのポリシー タイプが使用されますか?
A. アクセス制御
B. 脅威エミュレーション
C. 脅威の防止
D. QoS
Answer: D (メーッセージを残す**)**

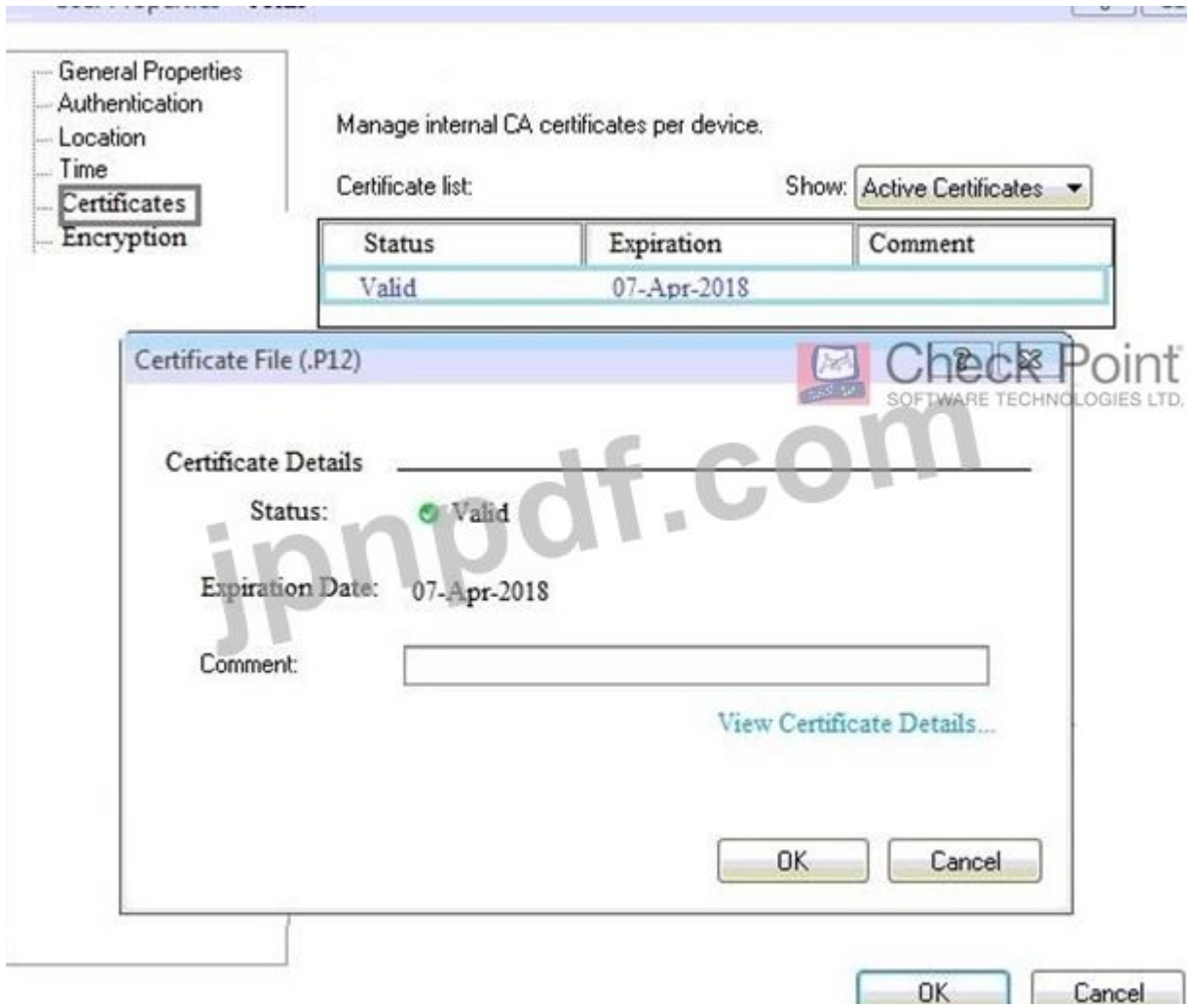
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_QoS_AdminGuide/127573

最新問題: **259**
R77 から R80 にアップグレードします。アップグレードする前に、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の状態で古いバージョンに簡単に復元できるようにする必要があります。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. エクスポートの移行
Answer: C (メーッセージを残す**)**
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、Check Point 製品、構成、オペレーティング システムが含まれます。
R77.10 以降、あるマシンからイメージをエクスポートし、そのイメージを同じタイプの別のマシンにインポートすること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は含まれません。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: **260**
空白を埋めてください: LDAP サーバーのデフォルトのポート番号は、標準接続の場合は _____ で、SSL 接続の場合は _____ です。
A. 389、636
B. 290、675
C. 636、290
D. 675、389
Answer: A (メーッセージを残す**)**

最新問題: **261**
ローミング ユーザーに ID 認識を導入する最良の方法は何ですか?
A. オフィス モードを使用する
B. アイデンティティ エージェントを使用する
C. ゲートウェイ間でユーザー ID を共有します
D. キャプティブ ポータルを使用する
Answer: B (メーッセージを残す**)**
Endpoint Identity Agent を使用すると、次のことが可能になります。

最新問題: **262**
次の図が表示されます。



そこには何が提示されているのでしょうか？
A. ユーザー John の .p12 証明書プロパティが期限切れです。
B. John のゲートウェイの VPN 証明書プロパティ。
C. 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。
D. John のパスワードの共有秘密プロパティ。
Answer: C (メーッセージを残す)

最新問題: **263**
Application Control の機能や利点ではないものは次のうちどれですか?
A. ネットワーク内の不明なアプリケーションや不要なアプリケーションを排除して、IT の複雑さとアプリケーションのリスクを軽減します。
B. ポリシーを決定するために、ユーザーがダウンロードしているファイルのコンテンツをスキャンします。
C. 実行権限を持つ信頼できるソフトウェアを自動的に識別します
D. IT 環境内にあるアプリケーションと IT 環境に追加するアプリケーションを識別して制御します。
Answer: B (メーッセージを残す)
ファイル スキャンは ThreatCloud のジョブであり、ファイルをサンドボックス化/スクラブします。

最新問題: **264**

あなたの上司は、企業秘密を競合他社に譲渡した疑いのある従業員を注意深く監視するようあなたに求めています。IT 部門は、容疑者が暗号化通信を使用するために 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。このタスクを達成するには次の方法のうちどれが最適ですか?
A. 容疑者にキーロギング型トロイの木馬を添付した電子メールを送信し、容疑者の悪行に関する直接情報を入手します。
B. SmartDashboard を使用して、自分の IP アドレス、および潜在的なターゲットおよび疑わしいプロトコルの IP アドレスと一致するルールをファイアウォール ルール ベースに追加します。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。
C. SmartView Tracker を使用して、WinSCP 宛先ポートを特徴とするログ 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。次に、対応するエントリを文書化するために別のログ ファイルにエクスポートします。
D. ルール ベースと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。
Answer: (解答を表示する**)**

最新問題**: 265**
パケットのタグ付けとコンピュータ認証を含む Endpoint Identity Agent のタイプはどれですか?
A. フル
B. カスタム
C. 完了
D. ライト
Answer: A (メーッセージを残す**)**
説明
パケットのタグ付けとコンピュータ認証を含む Endpoint Identity Agent のタイプは 「フル」です。Full Identity Agent は、ユーザー認証、コンピュータ認証、パケットのタグ付け、ID キャッシュ、ID 共有などの完全な ID 認識機能を提供するクライアント側のソフトウェアです。他のタイプの Endpoint Identity Agent にはカスタム、完全、およびライトがあり、それぞれに異なる特徴と機能があります。

最新問題**: 266**
HTTPS 検査ポリシーを構成するにはどのような手順を実行しますか?
A. SmartDashboard で [管理と設定] > [ブレード] > [HTTPS 検査] > [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 > [詳細設定] > [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: C (メーッセージを残す**)**
説明
HTTPS 検査ポリシーを設定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、および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です。
* [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。参考文献: HTTPS インスペクション R81 管理ガイド、Check Point CCSA - R81: 実践テストと解説

最新問題**: 267**

証明書を使用して VPN を確立したいと考えています。VPN は外部パートナーと証明書を交換します。次のアクティビティのうち、最初に行うのはどれですか?
A. パートナーの証明書失効リストを手動でインポートします。
B. エクスポートされた CA キーを交換し、それらを使用してパートナーの認証局 (CA) を表す新しいサーバー オブジェクトを作成します。
C. パートナーの CA を表す新しい論理サーバー オブジェクトを作成します。
D. パートナーのアクセス制御リストを手動でインポートします。
Answer: (解答を表示する**)**

最新問題**: 268**
アクセス コントロール ポリシー層を構成する 2 つの順序付けされた層はどれですか?
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**)**
説明
アクセス コントロール ポリシー層を構成する 2 つの順序付けされた層は、ネットワークと脅威防止です。
ネットワーク層には、Security Gateway によるトラフィックの検査および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 2 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。
参考資料: Check Point R81 セキュリティ管理管理ガイド

最新問題**: 269**
「拡張ログ」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. 宛先ポート
B. ファイル属性
C. データ型情報
D. アプリケーション情報
Answer: (解答を表示する**)**

最新問題**: 270**
John は、R77.30 Check Point Security Gateway を管理する R81 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. セッションからのログアウト
B. データベースをインストールします
C. セッションを公開します
D. ファイル > 保存
Answer: C (メーッセージを残す**)**

最新問題: **271**
ネットワーク管理者は、ネットワーク上で悪意のあるホストを特定したことを通知し、それをブロックするように指示しました。企業ポリシーにより、現時点ではファイアウォール ポリシーの変更は行えません。
このトラフィックをブロックするにはどのようなツールを使用できますか?
A. ボット対策保護
B. マルウェア対策保護
C. ポリシーベースのルーティング
D. 不審なアクティビティの監視 (SAM) ルール
Answer: (解答を表示する**)**
説明
ネットワーク管理者がネットワーク上の悪意のあるホストを特定し、それをブロックするように指示したが、現時点ではファイアウォール ポリシーを変更できない場合は、不審なアクティビティの監視 (SAM) ルールを使用してこのトラフィックをブロックできます。SAM ルールは、セキュリティ ポリシーを変更せずに、特定の送信元または宛先からのトラフィックをブロックまたは制限できる一時的なルールです。SAM ルールは SmartView Monitor によって作成および管理され、指定された期間セキュリティ ゲートウェイによって適用されます。ボット対策、マルウェア対策保護、およびポリシーベースのルーティングは、ファイアウォール ポリシーを変更せずにトラフィックをブロックするために使用できるツールではありません。参考文献: [Check Point R81 SmartView モニター管理ガイド]

最新問題: **272**
SmartConsole を通じて作成されたアカウントに使用される認証スキームではないものは次のうちどれですか?
A. 半径
B. チェックポイントのパスワード
C. 秘密の質問
D. SecurID
Answer: C (メーッセージを残す**)**
説明
セキュリティの質問は、SmartConsole4 を通じて作成されたアカウントに使用される認証スキームではありません。使用可能な認証スキームは、Check Point パスワード、RADIUS、TACACS、SecurID、LDAP、および証明書です。参考資料: Check Point R81 セキュリティ管理管理ガイド

最新問題: **273**

セキュリティ ルールの追跡オプションとして 拡張ログ」を有効にしました。ただし、データ型情報はまだ表示されません。最も考えられる理由は何ですか?
A. ID 認識が有効になっていません。
B. ログにディスク容量の問題があります
C. コンテンツ認識が有効になっていません。
D. ログのトリミングが有効になっています。
Answer: (解答を表示する**)**

最新問題**: 274**
ユーザーチェックとは何ですか?
A. ユーザーの資格情報を検証するためのメッセージング ツール ユーザー
B. アクセスしようとしている Web サイトまたは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: D (メーッセージを残す**)**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/UserCheck.htm

最新問題**: 275**
SmartView Monitor で Security Gateway 統計のリアルタイムおよび履歴グラフ ビューを表示するには、Security Gateway でどの機能を有効にする必要がありますか?
A. ロギングとモニタリング
B. なし - データはデフォルトで利用可能です
C. 監視ブレード
D. SNMP
Answer: (解答を表示する**)**
https://sc1.checkpoint.com/documents/R81/WebAdminGuides/EN/CP_R81_NextGenSecurityGateway_Guide/Topics-FWG/Monitoring-Blade.htm

最新問題**: 276**
内部ルーターは、GRE でカプセル化され、R77 Security Gateway 経由でパートナー サイトに送信される UDP キープアライブ パケットを送信します。GRE トラフィックのルールが ACCEPT/LOG 用に設定されています。キープアライブ パケットは 1 分ごとに送信されますが、SmartView Tracker ログで GRE トラフィックを検索すると、1 日中 (ポリシー インストール後の早朝) のエントリが 1 つしか表示されません。
パートナー サイトは、GRE カプセル化されたキープアライブ 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。
ルーター上で 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 1 分ごとに表示します。
この動作に最適なのは次のうちどれですか?

A. ログ統合プロセスで使用されている LUUID (Log Unification Unique Identification) は破損しています。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. VPN トラフィックであるため、ログ サーバーは GRE トラフィックを適切にログに記録できません。適切なログを有効にするには、パートナー サイトへのすべての VPN 構成を無効にします。
C. ログ設定では、GRE のこのレベルの詳細はキャプチャされません。特定のタイプのトラフィックはこの方法でのみ追跡できるため、ルール追跡アクションを 監査」に設定します。
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 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 分のセッション タイムアウトがあるため、各キープアライブ パケットは、その日の初めにログに記録された元の接続の一部とみなされます。
Answer: D (メーッセージを残す)

最新問題**: 277**
企業のシステム管理者は、トラフィックの高速化が機能しない理由を調べようとしています。トラフィックはルールベースに従って許可され、ウイルスがチェックされます。しかしそれは加速されない。トラフィックが加速されない最も考えられる理由は何ですか?
A. 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
B. 接続にはセキュリティ サーバーが必要でした
C. 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
D. アクセラレーションが有効になっていません
Answer: (解答を表示する)

最新問題**: 278**
帯域幅とトラフィック制御ルールを適用するためにどのポリシー タイプが使用されますか?
A. アクセス制御
B. 脅威エミュレーション
C. 脅威の防止
D. QoS
Answer: (解答を表示する)
説明
帯域幅とトラフィック制御ルールを強制するために使用されるポリシー タイプは QoS です。QoS は、Quality of Service の略で、管理者が送信元、宛先、サービス、アプリケーション、ユーザーなどのさまざまな基準に従ってネットワーク トラフィックの優先順位を設定できるようにするソフトウェア ブレードです。QoS は、特定のトラフィック タイプの帯域幅消費を制限したり、トラフィックの帯域幅消費を保証したりすることもできます。クリティカルなアプリケーションの最小帯域幅。参考文献:
[Check Point R81 QoS 管理ガイド]

最新問題**: 279**
セッションを公開する前に管理者が行った変更は、スーパーユーザー管理者にはどのように表示されるのでしょうか?
A. ログイン名...」オプションを使用して管理者になりすます。
B. 見えません
C. SmartView Tracker 監査ログから

D. [管理と設定] > [セッション] から、セッションを右クリックし、[変更の表示...] をクリックします。
Answer: D (メーッセージを残す)
説明
セッションを公開する前に管理者が行った変更は、スーパーユーザー管理者が 管理と設定」> セッション」から確認でき、セッションを右クリックして 変更の表示...」をクリックします。このオプションを使用すると、スーパーユーザーは保留中のセッションで別の管理者が行った変更を確認できます1。
参考資料: Check Point R81 セキュリティ管理管理ガイド

最新問題**: 280**
空白を埋めてください: デフォルトでは、R80 Management Server によって発行される SIC 証明書は _____ アルゴリズムに基づいています。
A. MD5
B. SHA-200
C. SHA-256
D. SHA-128
Answer: C (メーッセージを残す)

最新問題**: 281**
QUESTION NO: 238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. ターミナル サーバー エンドポイント ID エージェント
B. RADIUS とアカウント ログオン
C. エンドポイント ID エージェントとブラウザベースの認証
D. AD クエリ
Answer: C (メーッセージを残す)

最新問題**: 282**
拡張ログ」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: B (メーッセージを残す)
説明
アプリケーション情報は 拡張ログ」追跡オプションには含まれますが、ログ」追跡オプションには含まれません4。 拡張ログ」オプションは、名前、カテゴリ、リスク、テクノロジーなど、アプリケーションに関する追加情報を提供します4。参考資料: ロギングとモニタリング R80

最新問題**: 283**

空白を埋めてください: SmartConsole、SmartEvent GUI クライアント、および _____ では、数十億の統合ログを表示でき、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. 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. SmartReporter
Answer: (解答を表示する**)**
SmartEvent ソフトウェア ブレードは、リアルタイムのグラフィカルな脅威管理情報を提供する、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、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。セキュリティ インシデントに直ちに対応します」https://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/html_frameset.htm?topic=documents/R80/%20CP_R80_LoggingAndMonitoring/131915

最新問題**: 284**
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。管理サーバーがインターネットに接続されていない場合の最良のアップグレード方法は何ですか?
A. CPUSE オンライン 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. CPUSE オフライン アップグレード
D. SmartUpdate のアップグレード
Answer: C (メーッセージを残す**)**

最新問題**: 285**
SmartConsole を通じてセキュリティ管理サーバーに初めてログインすると、フィンガープリントは次の場所に保存されます。
A. Windows レジストリは、将来の Security Management Server 認証に使用できます。
B. とにかく、指紋の保存に使用されるメモリがありません。
C. Security Management Server の /home/.fgpt ファイル。将来の SmartConsole 認証に使用できます。
D. SmartConsole キャッシュは、将来の Security Management Server 認証に使用できます。
Answer: (解答を表示する**)**

最新問題**: 286**
正誤問題: Security Gateway ログの宛先サーバーは、Security Management Server 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構成されます。
B. True、すべての Security Gateway は SmartCenter Server 構成のログのみを転送します。
C. True、すべての Security Gateway はログを Security Management Server に自動的に転送します。
D. False、ログ サーバーは Security Gateway 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**)**
説明
Security Gateway ログの宛先サーバーは、Security Management Server の構成によって異なります。

Security Management Server は Security Gateway からログを受信するログ サーバーを定義しているため、これは当てはまります。ログ サーバーは、Security Management Server 自体または専用の Log Server12 のいずれかになります。参考資料: Check Point R81 ログおよびモニタリング管理ガイド、Check Point R81 Quantum Security Gateway ガイド

最新問題**: 287**
R80.x SmartConsole の主な機能の 1 つは同時管理です。AdminA、AdminB、AdminC が同じセキュリティ ポリシーを編集していることを考慮すると、不可能なのは次のうちどれですか?
A. AdminA、AdminB、AdminC は 3 つの異なるルールを同時に編集しています。
B. AdminA と AdminB は同じルールを同時に編集しています。
C. AdminB には、現在編集中のルールの横に鉛筆アイコンが表示されます。
D. AdminC には、ルールが別の管理者による編集のためにロックされていることを示す鍵アイコンが表示されます。
Answer: (解答を表示する**)**

最新問題**: 288**
UserCheck メッセージには 3 種類ありますか?
A. 通知、質問、ブロック
B. ブロック、アクション、警告
C. アクション、通知、および質問
D. 質問、ブロック、通知
Answer: A (メーッセージを残す**)**
説明
UserCheck メッセージには、inform、ask、block の 3 種類があります。通知メッセージはセキュリティ イベントについてユーザーに通知します。ユーザーのアクションは必要ありません。Ask メッセージでは、アクションを許可するかブロックするかをユーザーに選択させます。メッセージをブロックすると、ユーザーはアクションを実行できなくなり、理由が表示されます1。
参考資料: Check Point R81 ログおよびモニタリング管理ガイド

最新問題**: 289**
ファイアウォール カーネルは複数回レプリケートされるため、次のようになります。
A. ファイアウォールはコアごとに異なるポリシーを実行できます
B. ファイアウォール カーネルは新しい接続がある場合にのみ複製され、接続がタイムアウトすると自身を削除します。
C. ファイアウォール カーネルは、接続が高速化されている場合にのみパケットにアクセスします。
D. ファイアウォールはすべてのコアで同じポリシーを実行できます。
Answer: D (メーッセージを残す**)**

最新問題: **290**
SmartConsole では、オブジェクトは物理ネットワーク コンポーネントと仮想ネットワーク コンポーネント、および一部の論理コンポーネントを表すために使用されます。これらのオブジェクトはいくつかのカテゴリに分類されます。オブジェクト カテゴリではないものは次のうちどれですか?
A. 制限
B. リソース
C. カスタム アプリケーション/サイト
D. ネットワーク オブジェクト
Answer: (解答を表示する**)**
説明
リソースは、SmartConsole1 のオブジェクト カテゴリではありません。18. SmartConsole のオブジェクト カテゴリは、ネットワーク オブジェクト、ホスト、ネットワーク、グループ、ゲートウェイ、クラスター、VPN コミュニティ、サービス、時間オブジェクト、アクセス ロール、カスタム アプリケーション/サイト、データ センター オブジェクト、制限です。参考資料: Check Point CCSA - R81: 実践テストと説明、[Check Point SmartConsole R81 ヘルプ]

最新問題: **291**
VPN コミュニティとの関連付けに関係なく、接続に一致するオプションはどれですか?
A. すべてのサイト間 VPN コミュニティ
B. すべての暗号化されたトラフィックを受け入れます
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: B (メーッセージを残す**)**
説明
[すべての暗号化トラフィックを受け入れる] は、VPN コミュニティとの関連付けに関係なく、接続を照合するオプションです2。このオプションを使用すると、VPN コミュニティで定義されていない場合でも、任意の VPN ピアからの暗号化されたトラフィックが許可されます2。参考資料: R80.x のサイト間 VPN - 初心者向けチュートリアル

最新問題: **292**
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. セキュリティ ゲートウェイ
B. ポリシー サーバー
C. 管理サーバー
D. SmartLSM
Answer: C (メーッセージを残す**)**

最新問題: **293**
ヴァネッサは非常に重要なセキュリティ レポートを待っています。文書は電子メールに添付して送信する必要があります。Security_report.pdf ファイルを含む電子メールが彼女の電子メールの受信箱に配信されました。PDF ファイルを開いたとき、ファ

イルは基本的に空であり、テキストが数行しか含まれていないことに気づきました。レポートには一部のグラフ、表、リンクがありません。彼女の会社は、SandBlast 保護のどのコンポーネントをゲートウェイで使用していますか?
A. SandBlast 脅威エミュレーション
B. SandBlast 脅威の抽出
C. サンドブラスト エージェント
D. チェックポイント保護
Answer: B (メーッセージを残す)

最新問題**: 294**
Application Control/URL フィルタリング データベース ライブラリは次のように知られています。
A. アプリケーション データベース
B. AppWiki
C. アプリケーション フォレンジック データベース
D. アプリケーション ライブラリ
Answer: (解答を表示する)
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk113795

最新問題**: 295**
WebUI には、CPUSE 経由でホットフィックスをダウンロードするための 3 つの方法が用意されています。その 1 つは自動メソッドです。CPUSE エージェントは 1 日に何回ホットフィックスをチェックし、自動的にダウンロードしますか?
A. 1 日あたり 6 回
B. 1 日 7 回
C. 3 時間ごと
D. 2 時間ごと
Answer: C (メーッセージを残す)

最新問題**: 296**
SOLR データベースは何のためにありますか?
A. DLE サーバーにリクエストを転送する役割を担う GUI を提供します。
B. 強力なマッチング機能を有効にし、データベースにデータを書き込みます。
C. データベースと全文検索にデータを書き込みます
D. 全文検索に使用され、強力なマッチング機能が有効になります。
Answer: (解答を表示する)

最新問題**: 297**
管理者は R81 の信頼できる SmartConsole クライアントのリストをどこで編集できますか?
A. SmartConsole のみを使用します: [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]。
B. Security Management Server の cpconfig、Security Management Server にログインした WebUI、SmartConsole: [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 にログオンした WebUI クライアント。SmartDashboard: Security Gateway の cpconfig 経由で、[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]。
D. Security Management Server にログインした WebUI 内の Security Management Server 上の cpconfig。
Answer: B (メーッセージを残す)

最新問題: **298**
CLI でクラスター メンバーを監視するために使用されるコマンドは次のどれですか?
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)
説明
コマンド showclusterstate は、CLI でクラスターメンバーを監視するために使用されます。クラスタ モード、クラスタ メンバー、ステータス、優先順位、インターフェイスなどの情報が表示されます。参考資料: [ClusterXL Administration Guide]、[Check Point CLI Reference Card]

最新問題: **299**
セキュリティ ポリシーを変更するために、管理者は次のどのツールを使用できますか? （最良の答えを選択する。）
A. Security Gateway 上の mgmt_cli (API) または WebUI、および Security Management Server 上の SmartConsole。
B. Security Management Server 上の SmartConsole と WebUI。
C. SmartConsole がインストールされているコンピューター上の SmartConsole または mgmt_cli (API)。
D. Security Management Server のコマンド ライン、または Windows コンピュータ上の mgmt_cli.exe。
Answer: C (メーッセージを残す)

最新問題: **300**
あなたは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すると、ログが POP3 トラフィックを受け入れていることがわかりますが、ルール ベースに POP3 トラフィックを許可するルールが表示されません。最も考えられる原因は次のうちどれですか?
A. POP3 ルールが無効になっています。
B. POP3 はグローバル プロパティで受け入れられます。
C. POP3 は、R77 のデフォルトのメール オブジェクトによって受け入れられる 3 つのサービス (POP3、IMAP、および SMTP) の 1 つです。
D. POP3 ルールは非表示になります。
Answer: D (メーッセージを残す)

最新問題: **301**
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ポリシーの最後にあるルール。
Answer: (解答を表示する**)**
説明
ステルス ルールの目的は、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ドロップすることです1、p. 32. ステルス ルールは、通常、セキュリティ ゲートウェイ 2 へのトラフィックを許可する他のルールの前に、ルール ベースの先頭に配置されます。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ドロップしたりするためには使用されません。
参考資料: Check Point CCSA - R81: 模擬テストと説明、156-315.81 チェックポイント試験情報および無料模擬テスト

最新問題: **302**
ローミング ユーザーに ID 認識を導入する最良の方法は何ですか?
A. オフィス モードを使用する
B. アイデンティティ エージェントを使用する
C. ゲートウェイ間でユーザー ID を共有します
D. キャプティブ ポータルを使用する
Answer: B (メーッセージを残す**)**
説明
ローミング ユーザーに ID 認識を展開する最良の方法は、ID エージェントを使用することです。ID エージェントは、ユーザーとマシンの ID 情報を Security Gateway45 に提供するエンドポイントにインストールされるソフトウェア コンポーネントです。ID エージェントは、ネットワークの変更やユーザーの操作を必要としないため、他の方法よりも安全で信頼性が高くなります4。オフィス モード、ゲートウェイ間でのユーザー ID の共有、およびキャプティブ ポータルの使用は、Identity Awareness を展開する方法ではなく、Identity Awareness で使用できる機能またはオプションです46。
参考資料: ID 認識リファレンス アーキテクチャとベスト プラクティス、ID 認識 PDP ブローカー、ID 認識データシート

最新問題: **303**
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. 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
B. SmartConsole およびセキュリティ管理サーバー
C. セキュリティ管理サーバー
D. スマートコンソール
Answer: A (メーッセージを残す**)**

最新問題: **304**

空白を埋めてください: _____ は、ネットワーク ユーザーに関する識別情報とセキュリティ情報を取得するために使用されます。
A. ユーザーインデックス
B. ユーザーチェック
C. ユーザーディレクトリ
D. ユーザーサーバー
Answer: (解答を表示する**)**
説明
ユーザー ディレクトリは、ネットワーク ユーザーに関する識別情報とセキュリティ情報を取得するために使用されます。LDAP、RADIUS、TACACS+ などの外部ユーザー データベースと統合できます。参考資料: Certified Security Administrator (CCSA) R81.20 コースの概要、9 ページ。

最新問題**: 305**
パケットから状態関連情報を抽出し、その情報を状態テーブルに保存するために使用されるのは次のうちどれですか?
A. 状態エンジン
B. TRACK エンジン
C. レコード エンジン
D. 検査エンジン
Answer: D (メーッセージを残す**)**
ステートフル インスペクションでは、パケットはネットワーク層で傍受されますが、その後 INSPECT エンジンが引き継ぎます。すべてのアプリケーション層からセキュリティの決定に必要な状態関連情報を抽出し、後続の接続試行を評価するためにこの情報を動的状態テーブルに保持します。

最新問題**: 306**
R81.10 では、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、デフォルトのログ サーバーは次のポートを使用します。
A. 18210
B. 18191
C. 257
D. 18184
Answer: D (メーッセージを残す**)**

最新問題**: 307**
デフォルトで SmartLog インデックス ファイルを保持するディレクトリはどれですか?
A. $FWDIR/スマートログ
B. $FWDIR/ログ
C. $SMARTLOG/ディレクトリ
D. $SMARTLOGDIR/データ
Answer: D (メーッセージを残す**)**

最新問題**: 308**

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、完了までに 3 分以上かかります
B. 脅威の抽出は常にファイルを配信し、完了までに 1 秒もかかりません
C. 脅威エミュレーションは、完了までに 1 秒未満かかるファイルを配信することはありません
D. 脅威の抽出ではファイルが配信されず、完了までに 3 分以上かかります
Answer: (解答を表示する**)**
説明
脅威の抽出は常にファイルを配信し、完了までに 1 秒もかからないため、正解は B です2。脅威の抽出は、悪用可能なコンテンツをファイルから削除し、クリーンで安全なファイルをユーザー 2 に配信します。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、悪意があるか無害であるかを判定します2。ファイルのサイズと複雑さによっては、脅威エミュレーションが完了するまでに 3 分以上かかる場合があります2。参考資料: Check Point R81 脅威対策管理ガイド

最新問題**: 309**
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。この構成用にデータベース 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。
どうすればこんなことができるのでしょうか？
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 -1 ファイル名を実行します。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。
D. 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。 「データベースの改訂」画面でデータベース全体の復元を選択します。次に、fwm_dbimport を実行します。
Answer: (解答を表示する**)**

最新問題**: 310**
SmartConsole に同時に 2 人の管理者がログインしており、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? 最良の答えを選択する
A. セッションを元に戻します。
B. ポリシーを保存してインストールします
C. セッションを公開または破棄します
D. 古いバージョンのデータベースを削除します
Answer: C (メーッセージを残す**)**

最新問題**: 311**
DLP と地域ポリシーは、どのような種類のポリシーの例ですか?
A. 検査ポリシー
B. 共有ポリシー

C. 統合ポリシー
D. 標準ポリシー
Answer: B (メーッセージを残す**)**
https://sc1.checkpoint.com/documents/R80.30/WebAdminGuides/EN/CP_R80.30_NextGenSecurityGateway_Guide/html_frameset.htm?topic=documents/R80.30/WebAdminGuides/EN/CP_R80.30_NextGenSecurityGateway_Guide/137006

最新問題**: 312**
ポリシーに加えられた変更が Security Gateway によって適用されるようにするには、管理者はどのようなアクションを実行する必要がありますか?
A. 変更を公開する
B. 変更を保存
C. ポリシーのインストール
D. データベースをインストールします
Answer: C (メーッセージを残す**)**
説明
ポリシーに加えられた変更が Security Gateway によって適用されるようにするには、管理者はポリシーのインストール 3 を実行する必要があります。このアクションにより、ポリシー パッケージが Security Management Server から Security Gateway に転送され、アクティブ化されます。参考資料: Check Point R81 セキュリティ管理管理ガイド

最新問題**: 313**
空白を埋めてください: LDAP が Check Point Security Management と統合されると、LDAP は次のように呼ばれます。
____。
A. ユーザー センター
B. ユーザー管理
C. ユーザーディレクトリ
D. ユーザーチェック
Answer: (解答を表示する**)**
説明
LDAP が Check Point Security Management と統合されると、それはユーザー ディレクトリと呼ばれます。
ユーザー ディレクトリは、外部 LDAP サーバーからユーザーとグループをインポートし、セキュリティ ポリシーで使用できるようにする機能です。ユーザー センター、ユーザー管理、および UserCheck は、LDAP 統合とは関係のない別の機能です。参照: [ユーザーディレクトリ]、[LDAP 統合]

最新問題**: 314**
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 2 とレイヤ 3 の設定が正しいことを考慮すると、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. ネットワークごとに自動 NAT を定義し、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.3 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。ポリシーを公開してインストールします。

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、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。
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。Security Gateway を定義して、ゲートウェイの外部 IP.3 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。ポリシーを公開します。
Answer: (解答を表示する**)**

最新問題**: 315**
Management API を使用した通信方法の 1 つではない方法は次のうちどれですか?
A. 「mgmt_cli」コマンドを使用した API コマンドの入力
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 コマンドを入力します。
C. Gaia のセキュア シェル (クラッシュ) を使用した API コマンドの入力19+
D. Web サービスを使用した http 接続経由の API コマンドの送信
Answer: D (メーッセージを残す**)**
説明
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の 1 つではないため、正解は D です3。Management API は HTTPS プロトコルのみをサポートし、HTTP3 はサポートしません。他のメソッドは、Management API を使用して通信する有効な方法です3。
参考資料: Check Point の学習とトレーニングに関するよくある質問 (FAQ)

最新問題**: 316**
TCP/IP モデルのトランスポート層は何を担当しますか?
A. 2 つのホスト間のデータ フローを管理し、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. ネットワーク接続の物理コンポーネントのあらゆる側面を扱い、さまざまな種類のネットワークに接続します。
D. 宛先に到達するために、さまざまなルートに沿ってパケットをデータグラムとして転送します。
Answer: (解答を表示する**)**

最新問題**: 317**
ステルス ルールの目的は何ですか?
A. 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ポリシーの最後にあるルール。
B. 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。

C. 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。
D. 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ドロップします。
Answer: D (メーッセージを残す**)**

最新問題**: 318**
空白を埋めてください: ____ は、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 VPN ゲートウェイによって使用されます。
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**)**
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 インターフェイス) を使用して、物理インターフェイ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、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**: 319**
マルチキューを使用することで克服される (軽減される) CoreXL の制限はどれですか?
A. 各 NIC には、1 つの CPU によって処理される 1 つのトラフィック キューがあります。
B. 複数の NIC が 1 つの CPU で 1 つのトラフィック キューを使用できます
C. 処理するトラフィック キューがありません
D. 各 NIC には、複数の CPU コアによって処理される複数のトラフィック キューがあります。
Answer: D (メーッセージを残す**)**

最新問題**: 320**
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 2 とレイヤ 3 の設定が正しいことを考慮すると、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.3 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。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、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。
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、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。Security Gateway を定義して、ゲートウェイの外部 IP.3 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。ポリシーを公開します。
Answer: C (メーッセージを残す**)**
説明

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 ポリシーで受け入れ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 Security Gateway を通過できるようになります。
ネットワークごとに自動 NAT を定義し、パブリック IP の背後にあるネットワークを NAT 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。この手順では、Security Gateway に加えた変更を適用し、セキュリティ ルールと NAT ルールをアクティブにします。
参考資料: Check Point R81 Quantum Security Gateway ガイド

最新問題**: 321**
Secure Network Distributor (SND) はどのような点で Security Gateway に関連する機能ですか?
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: (解答を表示する**)**
説明
Secure Network Distributor (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る Security Gateway の機能です。複数の CPU コアを利用することで、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が向上します。他のオプションは SND とは関係ありません。参考文献: [Check Point Security Gateway のアーキテクチャとパケット フロー]、[Check Point CCSA の無料サンプル質問と学習ガイド]

最新問題**: 322**
空白を埋めてください: サービス ブレードは _____ に取り付けられる必要があります。
A. セキュリティ ゲートウェイ
B. 管理コンテナ
C. 管理サーバー
D. Security Gateway コンテナ
Answer: A (メーッセージを残す**)**
説明
サービス ブレードは Security Gateway に接続する必要があります。セキュリティ ゲートウェイは、通過するトラフィックにセキュリティ ポリシーを適用するデバイスです。サービス ブレードは、ファイアウォール、VPN、IPS などの特定のセキュリティ機能を提供するソフトウェア モジュールです。ライセンスとハードウェア機能に応じて、Security Gateway に 1 つ以上のサービス ブレードを接続できます。他のオプションは正しくありません。管理コンテナは、Security Management Server または Log Server をホストする仮想化環境です。管理サーバーは、セキュリティ ポリシーを管理し、Security Gateway に配布するデバイスです。Security Gateway コンテナは、Check Point の用語では有効な用語ではありません。参考資料: 『Check Point R81 Security Management 管理ガイド』、『Check Point R81 CloudGuard 管理ガイド』

Valid 156-215.81 Dumps shared by GoShiken.com for Helping Passing 156-215.81 Exam! GoShiken.com now offer the **newest 156-215.81 exam dumps**, the GoShiken.com 156-215.81 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com 156-215.81 dumps with Test Engine here: https://www.goshiken.com/CheckPoint/156-215.81-mondaishu.html (**414** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)