CheckPoint.156-215.80.v2022-08-14.q187

試験コード:	156-215.80
試験名称:	Check Point Certified Security Administrator R80
認定資格:	CheckPoint
無料問題数:	187
バージョン:	v2022-08-14
アクセス数:	2667
ページビュー数:	1870
https://www.jpnpdf.com/CheckPoint.156-215.80.v2022-08-14.q187-mondaishu.html	

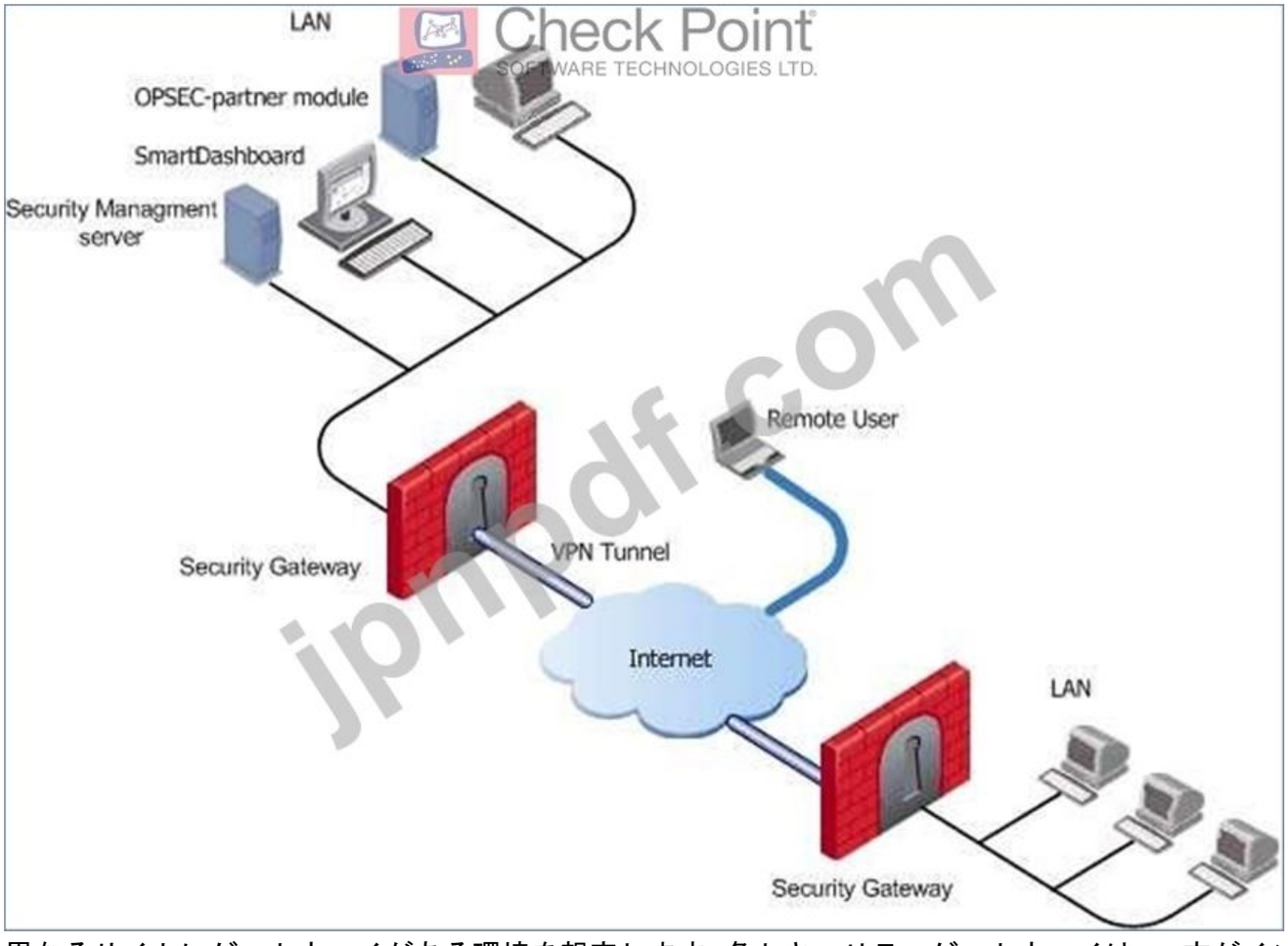
最新問題: **1**
次のうち、推奨されるライセンスモデルはどれですか？
A. パッケージライセンスをゲートウェイのIPアドレスに関連付け、セキュリティ管理サーバーに依存しないため、ローカルライセンス。
B. パッケージライセンスをセキュリティ管理サーバーのIPアドレスに関連付け、ゲートウェイの依存関係がないため、中央ライセンス。
C. ローカルライセンス。パッケージライセンスをゲートウェイ管理インターフェイスのMACアドレスに関連付け、セキュリティ管理サーバーに依存しないためです。
D. パッケージライセンスをセキュリティ管理サーバー管理インターフェイスのMACアドレスに関連付け、ゲートウェイの依存関係がないため、中央ライセンス。
Answer: B (メーッセージを残す**)**
説明
セントラルライセンス
セントラルライセンスは、ゲートウェイIPアドレスではなく、セキュリティ管理サーバーのIPアドレスに付加されるライセンスです。セントラルライセンスの利点は次のとおりです。
*すべてのライセンスに必要なIPアドレスは1つだけです。
*ライセンスは、あるゲートウェイから取得して別のゲートウェイに付与できます。
*ゲートウェイのIPアドレスを変更しても、新しいライセンスは引き続き有効です。新しいライセンスを作成してインストールする必要はありません。

最新問題: **2**
完成したステートメントのうち、正しく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で使用できます。
A. ユーザーに特権を割り当てます。
B. ユーザーのホームディレクトリを編集します。
C. Gaiaシステムにユーザーを追加します。

D. セキュリティ管理サーバー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**: 3**
ネットワークとセキュリティのパフォーマンスを監視するために使用されるSmartConsoleタブはどれですか？
A. 管理と設定
B. セキュリティポリシー
C. ゲートウェイとサーバー
D. ログとモニター
Answer: D (メーッセージを残す**)**
説明/参照：

最新問題**: 4**
チェック・ポイントのセキュリティ管理アーキテクチャの3つの重要なコンポーネントは何ですか？
A. SmartConsole、セキュリティ管理サーバー、セキュリティゲートウェイ
B. SmartConsole、SmartUpdate、Security Gateway
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、コマンドラインインターフェイス
D. WebUI、SmartConsole、セキュリティゲートウェイ
Answer: A (メーッセージを残す**)**
展開
基本的な展開：
*スタンドアロン展開-SecurityGatewayとSecurityManagementサーバーが同じマシンにインストールされます。
*分散展開-SecurityGatewayとSecurityManagementサーバーは異なるマシンにインストールされます。



異なるサイトにゲートウェイがある環境を想定します。各セキュリティゲートウェイは、一方がインターネットに接続し、もう一方がLANに接続します。
2つのセキュリティゲートウェイ間に仮想プライベートネットワーク（VPN）を作成して、それらの間のすべての通信を保護できます。
セキュリティ管理サーバーはLANにインストールされ、セキュリティゲートウェイによって保護されています。セキュリティ管理サーバーはセキュリティゲートウェイを管理し、リモートユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboardは、セキュリティ管理サーバーまたは別のコンピューターにインストールできます。
セキュリティ管理サーバーとそのセキュリティゲートウェイを使用してネットワークセキュリティを完了するために、他のOPSECパートナーモジュール（たとえば、アンチウイルスサーバー）が存在する場合があります。
参照：https ://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm？topic = document / R77 / CP_R77_SecurityManagement_WebAdminGuide / 118037

最新問題: **5**
多数のルールを適用する複数のセキュリティゲートウェイを使用しています。
セキュリティ管理を簡素化するために、どのアクションを選択しますか？
A. 個別のSmartConsoleインスタンスを実行して、各セキュリティゲートウェイに直接ログインして構成します。
B. 適用可能なすべてのルールを特定のネットワークのみに制限するネットワークオブジェクトを作成します。

C. ステルスルールやクリーンアップルールなど、考えられるすべての矛盾するルールを排除します。
D. リモートセキュリティゲートウェイごとに個別のセキュリティポリシーパッケージを作成します。
Answer: D (メーッセージを残す**)**

最新問題**: 6**
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次の手順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. コンピューターまたはコンピューターグループとネットワークの組み合わせ
D. リモートアクセスクライアント
Answer: (解答を表示する**)**

最新問題**: 7**
IT管理チームは、チェックポイントR80管理の新機能に関心があり、アップグレードしたいと考えていますが、既存のR77.30 Gaiaゲートウェイは非常に異なるため、R80で管理できないことを懸念しています。ファイアウォールを担当する管理者として、これらの懸念にどのように答えたり確認したりできますか？
A. R80 Managementには、R80より前のバージョンのCheckPointGatewayを管理するための互換性パッケージが含まれています。詳細については、R80リリースノートを参照してください。
B. R80管理では、R80より前のバージョンのCheck Point Gatewayを管理するために、互換性修正プログラムパッケージを個別にインストールする必要があります。詳細については、R80リリースノートを参照してください。
C. R80管理は、完全に異なる管理システムとして設計されているため、R80より前のチェックポイントゲートウェイのみを監視できます。
D. R80 Managementは、R80より前のバージョンのCheckPointGatewayを管理できません。R80以降のゲートウェイのみを管理できます。詳細については、R80リリースノートを参照してください。
Answer: (解答を表示する**)**
説明/参照：
Explanation:

参照 :http ://dl3.checkpoint.com/paid/1f/1f7e21da67aa992954aa12a0a84e53a8/ CP_R80_ReleaseNotes.pdf？HashKey = 1479838085_d6ffcb36c6a3128708b3f6d7bcc4f94e &xtn = .pdf

最新問題**: 8**

チェック ポイントのセキュリティ管理アーキテクチャの3つの重要なコンポーネントは何ですか？

A. SmartConsole、セキュリティ管理サーバー、セキュリティゲートウェイ

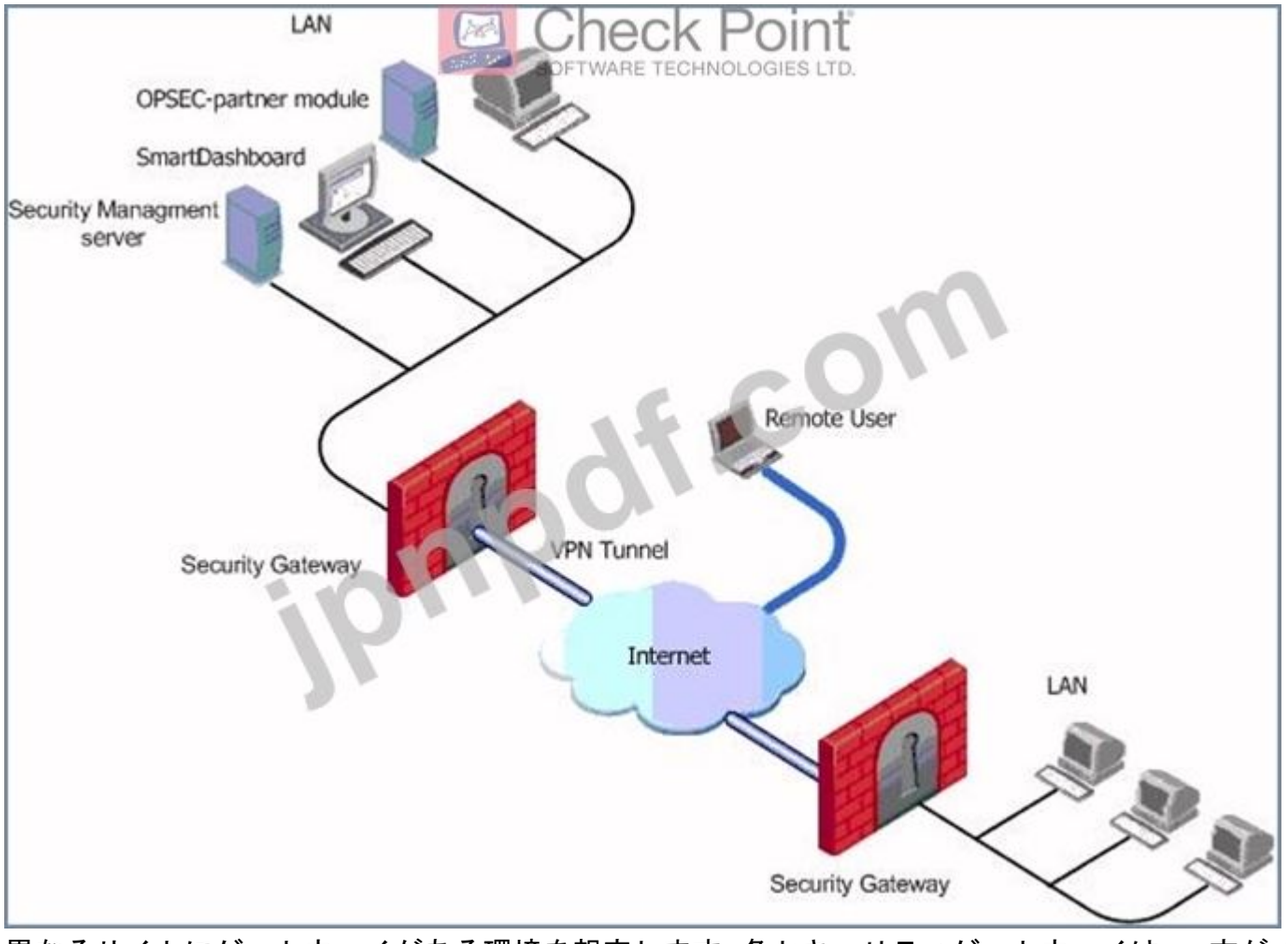
B. SmartConsole、SmartUpdate、Security Gateway

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、コマンドラインインターフェイス

D. WebUI、SmartConsole、セキュリティゲートウェイ

Answer: A (メーッセージを残す**)**

展開基本的な展開：



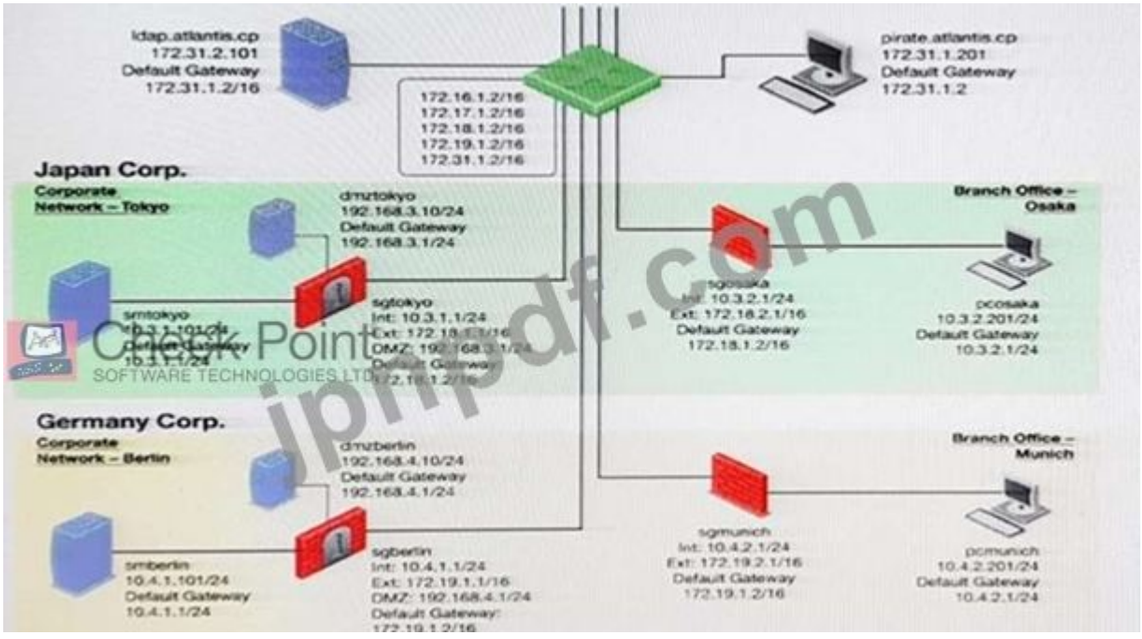
異なるサイトにゲートウェイがある環境を想定します。各セキュリティゲートウェイは、一方がインターネットに接続し、もう一方がLANに接続します。
2つのセキュリティゲートウェイ間に仮想プライベートネットワーク（VPN）を作成して、それらの間のすべての通信を保護できます。
セキュリティ管理サーバーはLANにインストールされ、セキュリティゲートウェイによって保護されています。セキュリティ管理サーバーはセキュリティゲートウェイを管理し、リモートユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboardは、セキュリティ管理サーバーまたは別のコンピューターにインストールできます。
セキュリティ管理サーバーとそのセキュリティゲートウェイを使用してネットワークセキュリティを完了するために、他のOPSECパートナーモジュール（たとえば、アンチウイルスサーバー）が存在する場合があります。

最新問題: **9**
ヴァネッサは彼女の会社のファイアウォール管理者です。彼女の会社は、R80 SecurityManagementServerによって一元管理されている中央およびリモートの場所でCheckPointファイアウォールを使用しています。中央の1つの場所には、OpenサーバーにR77.30ゲートウェイがインストールされています。リモートロケーションは、R71を備えたCheck PointUTM-1570シリーズアプライアンスを使用しています。各場所の中央管理とファイアウォール間のセキュア内部通信（SIC）で使用される暗号化はどれですか？
A. 中央ファイアウォールではAES128暗号化がSICに使用され、リモートファイアウォールでは3DES暗号化がSICに使用されます。

B. 両方のファイアウォールで、同じ暗号化がSICに使用されます。これはAES-GCM-256です。
C. ファイアウォール管理者は、SICが使用する暗号化スイートを選択できます。
D. 中央ファイアウォールではAES256暗号化がSICに使用され、リモートファイアウォールではAES128暗号化がSICに使用されます。
Answer: A (メーッセージを残す**)**
説明
R71より上のゲートウェイは、SICにAES128を使用します。ゲートウェイの1つがR71以下の場合、ゲートウェイは3DESを使用します。

最新問題**: 10**
管理者は、脅威ツールの[更新]タブにある[今すぐ更新]オプションをクリックして、SmartConsoleからIPS保護を更新したいと考えています。アップデートが機能するためにインターネットアクセスが必要なデバイスはどれですか？
A. セキュリティゲートウェイのみ
B. SmartConsoleがインストールされているデバイスのみ
C. セキュリティ管理サーバーのみ
D. セキュリティ管理サーバーまたはSmartConsoleがインストールされているデバイス
Answer: B (メーッセージを残す**)**
説明
IPSを手動で更新する
IPS Webサイトから、攻撃に関するリアルタイムの情報とすべての最新の保護を使用してIPSをすぐに更新できます。Internet Explorerの設定でプロキシが定義されている場合にのみ、IPSを手動で更新できます。
IPS Webサイトからすべての最新の保護の更新を取得するには、次のようにします。
*InternetExplorerでプロキシサーバーの設定を構成します。
* Microsoft Internet Explorerで、[ツール]>[インターネットオプション]>[接続]タブ>[LAN設定]を開きます。
[LAN設定]ウィンドウが開きます。
*[LANにプロキシサーバーを使用する]を選択します。
*プロキシサーバーのIPアドレスとポート番号を構成します。
*[OK]をクリックします。
InternetExplorerプロキシサーバーの設定が構成されます。
* [IPS]タブで、[アップデートのダウンロード]を選択し、[今すぐアップデート]をクリックします。
フォローアップの新しい保護を自動的にマークすることを選択した場合は、フォローアップページを直接開いて新しい保護を表示するオプションがあります。

最新問題**: 11**
smberlinとsgosakaの間でSICをリセットしたいとします。



SmartDashboardでは、sgosaka、Communication、Resetを選択します。sgosakaで、cpconfigを起動し、Secure Internal Communication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が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、機能している接続ではなく、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. まだcpconfigユーティリティを使用しているため、ゲートウェイ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。
B. 最初にSmartDashboardでゲートウェイ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て、[基本設定]> [初期化]を選択します）。
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さまざまな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. ゲートウェイが再起動されませんでした。これはSICキーを変更するために必要です。
Answer: A (メーッセージを残す**)**

最新問題**: 12**
GAiAを使用する場合、インターフェースeth0のMACアドレスを一時的に変更する必要がある場合があります。

00 :0C :29 :12 :34 :56。ネットワークを再起動した後、古いMACアドレスがアクティブになっているはずです。この変更をどのように構成しますか？

A. 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リンクセットeth0ダウン
#IPリンクセットeth0 addr 00 :0C :29 :12 :34 :56
#IPリンクセットeth0 up

B. WebUIを開き、[ネットワーク]>[接続]>[eth0]を選択します。[物理アドレス]フィールドに新しいMACアドレスを入力し、[適用]を押して設定を保存します。

C. 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に入力します ¢onf
:(conns
：c¢nn
:hwaddr（"00 :0C :29 :12 :34 :56"）

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リンクセットeth0 addr 00 :0C :29 :12 :34 :56

Answer: (解答を表示する**)**

最新問題**: 13**
ルールを確認します。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	Ac
1	0	Authentication	Customers@Any	Any	Any Traffic	http ftp	
2	0		Any	Any	Any Traffic	Any	

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

A. インターネットに正常に接続する前に3回プロンプトが表示されます。

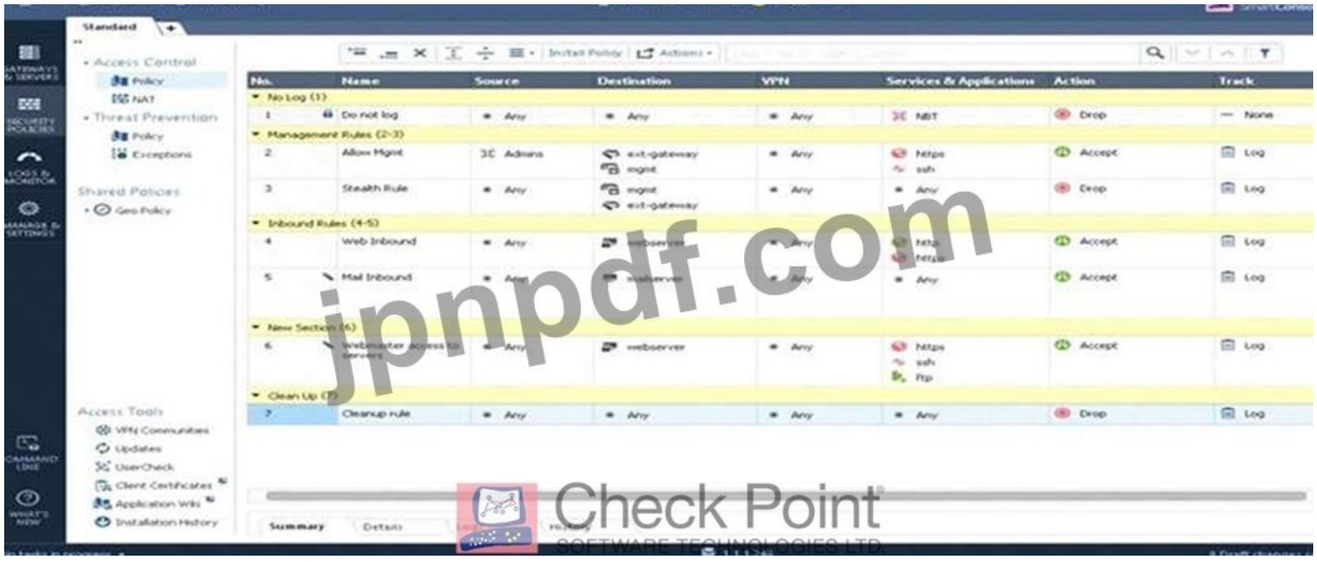
B. 認証を求められることなくインターネットにアクセスできます。

C. クライアント認証デーモンポート259にTelnetを実行した後、インターネットに接続できます。

D. 認証後、インターネットに正常に接続できます。

Answer: B (メーッセージを残す**)**

最新問題**: 14**
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7（クリーンアップルール）は、暗黙のクリーンアップルールを非表示にします

D. 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

Answer: (解答を表示する**)**

最新問題**: 15**

ブラウザベースの認証は、ユーザーをWebページに送信し、_____を使用してIDを取得します。

A. ユーザーディレクトリ

B. キャプティブポータルと透過的なKerberos認証

C. キャプティブポータル

D. UserCheck

Answer: B (メーッセージを残す**)**

Identity Awarenessを有効にするには：

1.SmartDashboardにログインします。

2. [ネットワークオブジェクト]ツリーから、[チェックポイント]ブランチを展開します。

3.IdentityAwarenessを有効にするSecurityGatewayをダブルクリックします。

4. [ソフトウェアブレード]セクションで、[ネットワークセキュリティ]タブの[ID認識]を選択します。

IdentityAwarenessConfigurationウィザードが開きます。

5.1つ以上のオプションを選択します。これらのオプションは、管理対象資産と管理対象外資産のIDを取得するための方法を設定します。

*ADクエリ-SecurityGatewayがActiveDirectoryユーザーとコンピューターをシームレスに識別できるようにします。

*ブラウザベースの認証-ユーザーをWebページに送信して、身元不明のユーザーからIDを取得します。

透過的なKerberos認証が構成されている場合、ADユーザーは透過的に識別される可能性があります。

参照：https ://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62050.htm

最新問題: **16**
mgmt_cliを使用して、CLIからServer_1というホストオブジェクトをインポートするための正しい構文は何ですか？
A. mgmt_cli add-host "Server_1" ip_address "10.15.123.10" --format txt
B. mgmt_cli add host name "Server_1" ip_address "10.15.123.10" --format json
C. mgmt_cli add object-host "Server_1" ip_address "10.15.123.10" --format json
D. mgmt_cli add object "Server_1" ip_address "10.15.123.10" --format json
Answer: A (メーッセージを残す**)**
説明/参照：
参照 :https ://sc1.checkpoint.com/documents/latest/APIs/index.html#cli/add-host~v1.1

最新問題: **17**
ルールベースの上部にルールを作成して、ゲストワイヤレスアクセスをインターネットに許可しました。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すると、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. 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]をオンにします
B. ルールで[同意する]を右クリックし、[その他]を選択して、[IDキャプティブポータルを有効にする]をオンにします。
C. セキュリティ管理サーバーオブジェクトで、[IDログ]チェックボックスをオンにします
D. ファイアウォールオブジェクトの[レガシー認証]画面で、[IDキャプティブポータルを有効にする]をオンにします
Answer: (解答を表示する**)**

最新問題: **18**
次の図には、ポリシーのレイヤーがあります。

定義されたポリシーのトラフィック検査の優先順位は何ですか？

A. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。暗黙のドロップルールがパケットをドロップすると、IPSレイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。。

B. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。パケットを受け入れるルールがある場合は、IPSレイヤーの隣に来て、パケットを受け入れた後、脅威に渡されます。防止層

C. パケットはゲートウェイに到着し、ネットワークポリシー層のルールと照合されます。パケットを受け入れるルールがある場合は、脅威防止層の隣に来て、パケットを受け入れた後、次の宛先に渡されます。IPSレイヤー。

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

Answer: B (メーッセージを残す)

説明

ポリシー管理を簡素化するために、R80はポリシーをポリシーレイヤーに編成します。レイヤーは、ルールのセット、またはルールベースです。

たとえば、以前のバージョンからR80にアップグレードする場合：

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

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

IPSおよび脅威エミュレーションソフトウェアブレードが有効になっているゲートウェイでは、脅威防止ポリシーがIPSと脅威防止の2つの並列レイヤーに分割されます。

すべてのレイヤーが並行して評価されます

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

すべてのレイヤーが並行して評価されます

参照：

最新問題**: 19**

ソフトウェアコンテナには_____種類があります_____。

A. 3; セキュリティ管理、セキュリティゲートウェイ、およびエンドポイントセキュリティ

B. 3; セキュリティゲートウェイ、エンドポイントセキュリティ、およびゲートウェイ管理

C. 2つ; セキュリティ管理とエンドポイントセキュリティ

D. 2つ; エンドポイントセキュリティとセキュリティゲートウェイ

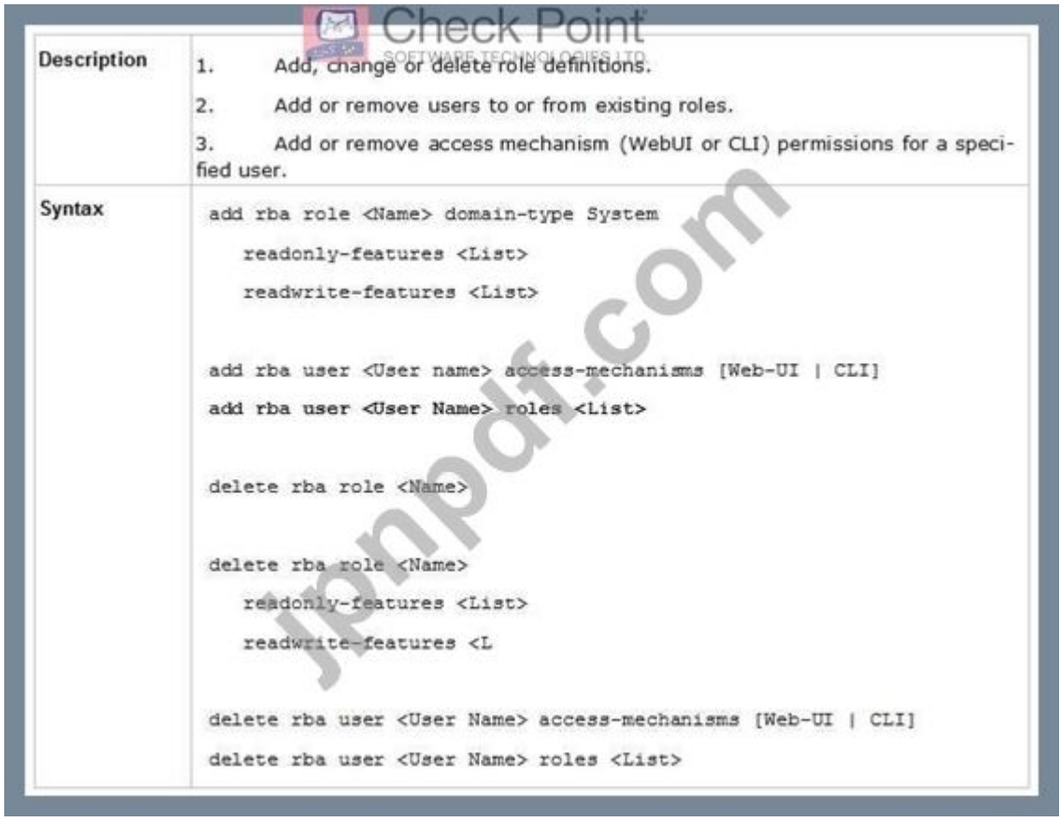
Answer: A (メーッセージを残す)

説明
ソフトウェアコンテナには、セキュリティ管理、セキュリティゲートウェイ、エンドポイントセキュリティの3種類があります。

最新問題: **20**
IDベースのポリシーを通じてアクセス制御を提供しながら、ユーザー、グループ、およびマシンの可視性を提供する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. アイデンティティの認識
C. アプリケーション制御
D. URLフィルタリング
Answer: B (メッセージを残す**)**
Check Point Identity Awareness Software Bladeは、ユーザー、グループ、およびマシンの詳細な可視性を提供し、正確なIDベースのポリシーの作成を通じて比類のないアプリケーションとアクセス制御を提供します。一元化された管理と監視により、ポリシーを単一の統合されたコンソールから管理できます。
参照 :https ://www.checkpoint.com/products/identity-awareness-software-blade/

最新問題: **21**
アクティブな同時接続の数を確認するために使用できるコマンドはどれですか？
A. fw conn all
B. fw ctl pst pstat
C. すべての接続を表示
D. 接続を表示
Answer: B (メッセージを残す**)**
説明/参照：
参照 :https ://supportcenter.checkpoint.com/supportcenter/portal？
eventSubmit_doGoviewsolutiondetails =＆solutionid = sk103496

最新問題: **22**
既存のロールにユーザーを追加したり、既存のロールからユーザーを追加したりするために使用されるコマンドはどれですか？
A. rbaユーザー<ユーザー名>ロール<リスト>を追加します
B. rbaユーザーを追加<ユーザー名>
C. ユーザー<ユーザー名>の役割を追加<リスト>
D. ユーザーを追加<ユーザー名>
Answer: A (メッセージを残す**)**
説明
Explanation:
役割の構成-CLI rba）



Description	1. Add, change or delete role definitions. 2. Add or remove users to or from existing roles. 3. Add or remove access mechanism (WebUI or CLI) permissions for a specified user.
Syntax	add rba role <Name> domain-type System readonly-features <List> readwrite-features <List> add rba user <User name> access-mechanisms [Web-UI | CLI] add rba user <User Name> roles <List> delete rba role <Name> delete rba role <Name> readonly-features <List> readwrite-features <L delete rba user <User Name> access-mechanisms [Web-UI | CLI] delete rba user <User Name> roles <List>

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

最新問題**: 23**
IT管理チームは、チェックポイントR80管理の新機能に関心があり、アップグレードしたいと考えていますが、既存のR77.30 Gaiaゲートウェイは非常に異なるため、R80で管理できないことを懸念しています。ファイアウォールを担当する管理者として、これらの懸念にどのように答えたり確認したりできますか？
A. R80 Managementには、R80より前のバージョンのCheckPointGatewayを管理するための互換性パッケージが含まれています。詳細については、R80リリースノートを参照してください。
B. R80管理では、R80より前のバージョンのCheck Point Gatewayを管理するために、互換性修正プログラムパッケージを個別にインストールする必要があります。詳細については、R80リリースノートを参照してください。
C. R80管理は、完全に異なる管理システムとして設計されているため、R80より前のチェックポイントゲートウェイのみを監視できます。
D. R80 Managementは、R80より前のバージョンのCheckPointGatewayを管理できません。R80以降のゲートウェイのみを管理できます。詳細については、R80リリースノートを参照してください。
Answer: A (メーッセージを残す**)**
説明/参照：
Explanation:

Compatibility with Gateways

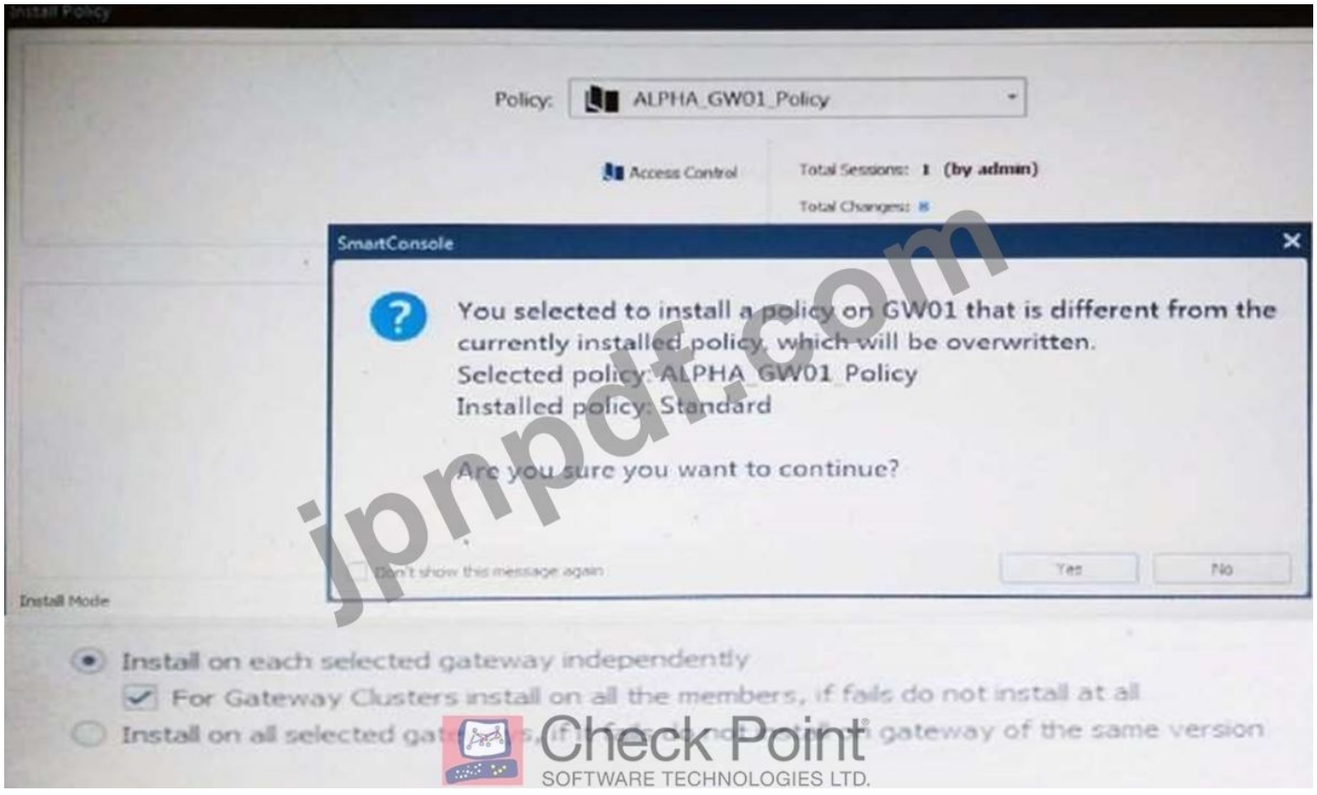
R80 Management Servers can manage gateways of these versions:

Release	Version
Security Gateway	R75.20, R75.30, R75.40, R75.45, R75.40VS, R75.46, R75.47, R76 R77, R77.10, R77.20, R77.30
Security Gateway 80	R71.45, R75.20.x
1100 Appliance	R75.20.x, R77.20.x
1200R Appliance	R77.20.x
UTM-1 Edge	7.5.x and higher (Edge-X and Edge-W are not supported)

参照 :http ://dl3.checkpoint.com/paid/1f/1f7e21da67aa992954aa12a0a84e53a8/ CP_R80_ReleaseNotes.pdf？HashKey = 1479838085_d6ffcb36c6a3128708b3f6d7bcc4f94e＆xtn = .pdf

最新問題: **24**
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つ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、バージョン1にロールバックしてルールベースを使用することにしましたが、ユーザーデータベースを保持したいと考えています。
どうすればこれを行うことができますか？
A. ユーザーデータベースを除くデータベース全体を復元します。
B. ユーザーデータベースを除くデータベース全体を復元してから、新しいユーザーとユーザーグループを作成します。
C. fwm_dbexportを実行して、ユーザーデータベースをエクスポートします。[データベースリビジョン]画面で[データベース全体を復元する]を選択します。次に、fwm_dbimportを実行します。
D. fwmdbexport-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-1filenameを実行してユーザーをインポートします。
Answer: A (メーッセージを残す**)**

最新問題: **25**
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クする必要があります。
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が既存の管理にインストールされます。
C. 管理で作成された新しいポリシーパッケージが既存のゲートウェイにインストールされます。
D. ゲートウェイで作成され、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、ゲートウェイの定期的なバックアップから復元できます。
Answer: (解答を表示する**)**

最新問題**: 26**
空欄に記入してください :LDAPがCheck Point Security Managementと統合されている場合、LDAPは次のように呼ばれます。

_____
A. UserCheck
B. ユーザーディレクトリ
C. ユーザー管理
D. ユーザーセンター
Answer: (解答を表示する**)**
説明/参照：
Explanation:
チェックポイントユーザーディレクトリは、LDAPおよびその他の外部ユーザー管理テクノロジーをチェックポイントソリューションと統合します。ユーザー数が多い場合は、セキュリティ管理サーバーのパフォーマンスを向上させるために、LDAPなどの外部ユーザー管理データベースを使用することをお勧めします。

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

最新問題: **27**
次の図には、ポリシーのレイヤーがあります。

定義されたポリシーのトラフィック検査の優先順位は何ですか？
A. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。暗黙のドロップルールがパケットをドロップすると、IPSレイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。。
B. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。パケットを受け入れるルールがある場合は、IPSレイヤーの隣に来て、パケットを受け入れた後、脅威に渡されます。防止層
C. パケットはゲートウェイに到着し、ネットワークポリシー層のルールと照合されます。パケットを受け入れるルールがある場合は、脅威防止層の隣に来て、パケットを受け入れた後、次の宛先に渡されます。IPSレイヤー。
D. パケットはゲートウェイに到着し、IPSポリシーレイヤーのルールと照合され、ネットワークポリシーレイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。
Answer: (解答を表示する**)**
説明/参照：
Explanation:ポリシー管理を簡素化するために、R80はポリシーをポリシーレイヤーに編成します。レイヤーは、ルールのセット、またはルールベースです。
たとえば、以前のバージョンからR80にアップグレードする場合：
ファイアウォールとアプリケーション制御ソフトウェアブレードが有効になっているゲートウェイでは、
▪
アクセス制御ポリシーは、ネットワークとアプリケーションの2つの順序付けられたレイヤーに分割されます。ゲートウェイがレイヤー内のルールと一致すると、ゲートウェイは次のレイヤー内のルールの評価を開始します。
IPSおよび脅威エミュレーションソフトウェアブレードが有効になっているゲートウェイでは、脅威が発生します
▪
防止ポリシーは、IPSと脅威防止の2つの並列レイヤーに分割されます。

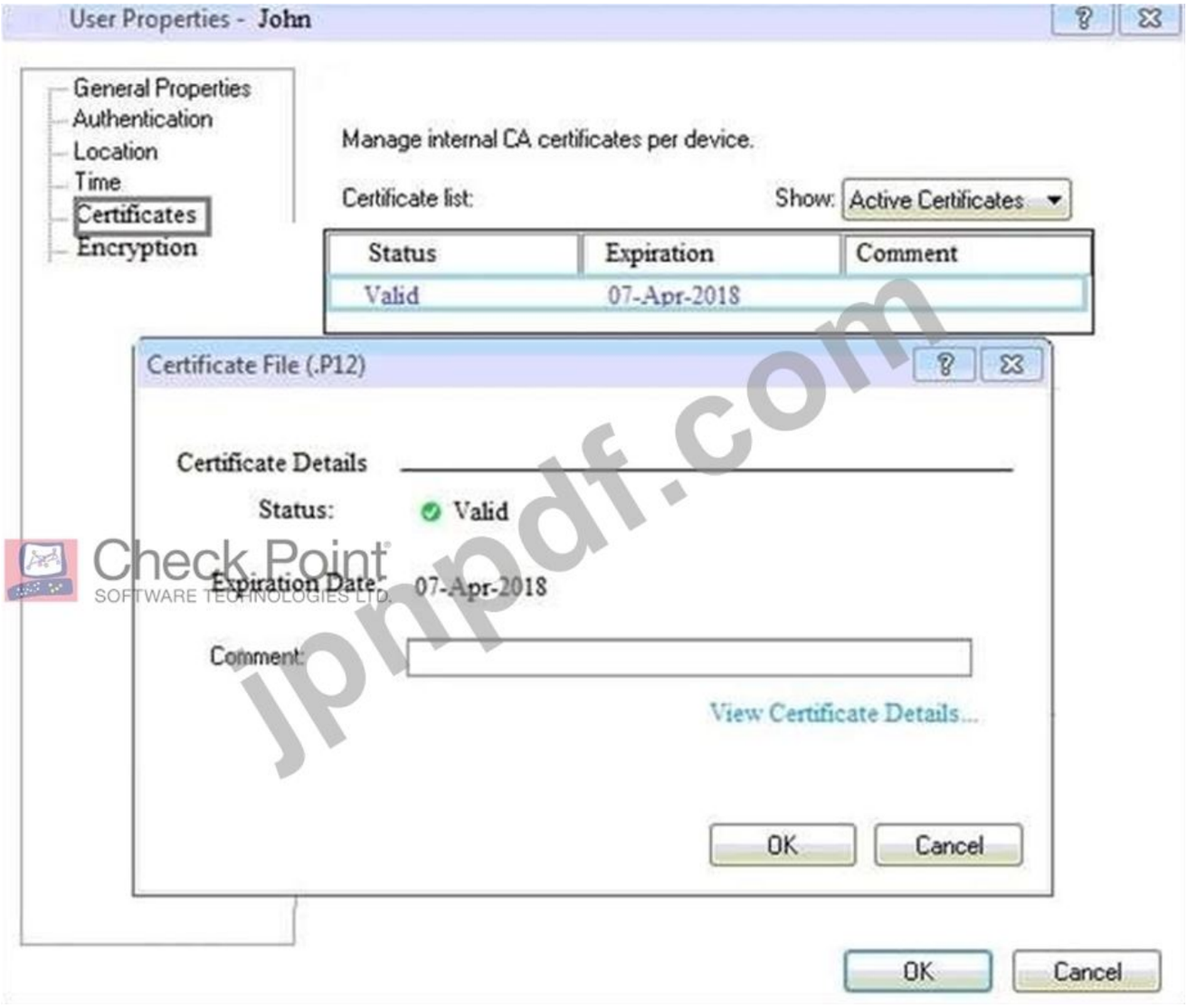
すべてのレイヤーが並行して評価されます
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 126197

最新問題: **28**
どのSmartEventコンポーネントがイベントを作成しますか？
A. SmartEvent GUI
B. 統合ポリシー
C. SmartEventポリシー
D. 相関ユニット
Answer: D (メーッセージを残す**)**

最新問題: **29**
次のうち、パッカーアクセラレーションの属性ではないものはどれですか？
A. 宛先ポート
B. アプリケーションの認識
C. 送信元アドレス
D. プロトコル
Answer: B (メーッセージを残す**)**

最新問題: **30**
IDベースのポリシーを通じてアクセス制御を提供しながら、ユーザー、グループ、およびマシンの可視性を提供する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/参照：
Explanation:Check Point Identity Awareness Software Bladeは、ユーザー、グループ、およびマシンの詳細な可視性を提供し、正確なIDベースのポリシーの作成を通じて比類のないアプリケーションとアクセス制御を提供します。一元化された管理と監視により、ポリシーを単一の統合されたコンソールから管理できます。
参照 :https ://www.checkpoint.com/products/identity-awareness-software-blade/

最新問題: **31**
次の図を見ることができます。



その上に何が表示されますか？

A. ユーザーJohnの.p12証明書のプロパティが期限切れになりました。

B. ジョンのゲートウェイのVPN証明書のプロパティ。

C. Johnのパスワードの共有秘密プロパティ。

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

Answer: D (メーッセージを残す)

最新問題: **32**

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に、IdentityAwarenessでどのIDソースを選択する必要がありますか？
A. ADクエリ
B. ターミナルサーバーエンドポイントIDエージェント
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. RADIUSとアカウントログオン
Answer: (解答を表示する**)**
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高レベルのセキュリティが必要な場合。
キャプティブポータルは、EndpointIdentityAgentを配布するために使用されます。IPスプーフィング保護は、パケットがIPスプーフィングされるのを防ぐために設定できます。
参照：
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide / html_frameset.htm？topic = document / R80.10 / WebAdminGuides / EN / CP_R80.10_IdentityAwareness_AdminGuide / 101858

最新問題**: 33**
UserCheckとは何ですか？
A. 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コミュニケーションツール。
B. ユーザーが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. ユーザーの資格情報を確認するために使用されるメッセージングツール。
Answer: B (メーッセージを残す**)**

最新問題**: 34**
ネットワークコンピュータに感染する可能性のある悪意のあるソフトウェアからの保護を提供する脅威防止ソフトウェアブレードはどれですか？
A. マルウェア対策
B. IPS
C. アンチボット
D. スパム対策
Answer: C (メーッセージを残す**)**
説明
アンチボット
アンチボットの必要性
今日の脅威の状況には、次の2つの新しい傾向があります。
*さまざまなツールを使用して目標を達成する、利益重視のサイバー犯罪業界。この業界には、サイバー犯罪者、マルウェアオペレーター、ツールプロバイダー、コーダー、およびアフィリエイトプログラムが含まれます。彼らの 製品」は、多数のサイト たとえば、日曜大工のマルウェアキット、スパム送信、データの盗難、サービス拒否攻撃）からオンラインで簡単に注文でき、組織はこれらの攻撃に対抗するのが難しいと感じています。

*政治的目的を促進したり、サイバー戦争キャンペーンを実行したりするために人々や組織を標的とするイデオロギー的および国家主導の攻撃。
これらの傾向は両方とも、ボット攻撃によって引き起こされています。
ボットは、コンピュータに侵入する可能性のある悪意のあるソフトウェアです。多くの感染方法があります。これには、脆弱性を悪用する添付ファイルを開くことや、悪意のあるダウンロードをもたらすWebサイトにアクセスすることが含まれます。

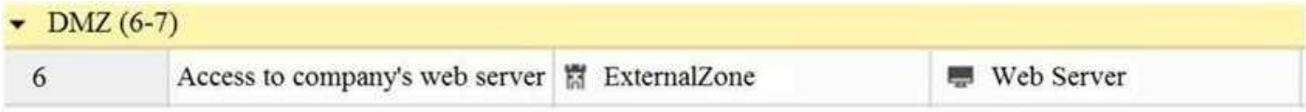
最新問題: **35**
VPNコミュニティの種類は次のうちどれですか？
A. ペンタゴン、スター、および組み合わせ
B. 星、八角形、および組み合わせ
C. 組み合わせてスター
D. メッシュ、スター、および組み合わせ
Answer: D (メーッセージを残す**)**
説明/参照 :https ://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm？トピック=ドキュメント/R77/ CP_R77_VPN_AdminGuide / 13894

最新問題: **36**
空欄に記入してください :_____ VPN展開は、インターネットブラウザを介してユーザーを認証することにより、リモートユーザーに内部の企業リソースへの安全なアクセスを提供するために使用されます。
A. クライアントレスリモートアクセス
B. クライアントレス直接アクセス
C. クライアントベースのリモートアクセス
D. 直接アクセス
Answer: (解答を表示する**)**
説明/参照：
Explanation:
クライアントレスユーザーはWebブラウザーを介して接続し、HTTPS接続を使用します。クライアントレスソリューションは通常、Webベースの企業リソースへのアクセスを提供します。
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80BC_Firewall/html_frameset.htm？topic = document / R80 / CP_R80BC_Firewall / 92704

最新問題: **37**
R80では、異なるチェックポイントコンポーネント間の通信はどのように保護されていますか？すべての質問と同様に、最良の回答を選択してください。
A. IPSECを使用する
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/参照：
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 125443

最新問題**: 38**
提示されたルールでExternalZoneは何を表していますか？



A. インターネット。
B. 管理者が外部セキュリティゾーンの一部として定義したインターフェイス。
C. すべてのセキュリティゲートウェイの外部インターフェイス。
D. 特定のゲートウェイの外部インターフェース。
Answer: B (メーッセージを残す**)**
インターフェイスの構成
[セキュリティゲートウェイ]ウィンドウの[インターフェイス]タブで、セキュリティゲートウェイ80のインターフェイスを設定します。
インターフェイスを設定するには：
1. [デバイス]ウィンドウで、SecurityGateway80をダブルクリックします。
[セキュリティゲートウェイ]ウィンドウが開きます。
2.[インターフェイス]タブを選択します。
3.[次の設定を使用する]を選択します。インターフェイス設定が開きます。
4.インターフェイスを選択し、[編集]をクリックします。
編集ウィンドウが開きます。
5. [IP割り当て]セクションから、インターフェイスのIPアドレスを構成します。
1.静的IPを選択します。
2.インターフェイスのIPアドレスとサブネットマスクを入力します。
6. [セキュリティゾーン]で、[ワイヤレス]、[DMS]、[外部]、または[内部]を選択します。セキュリティゾーンは、IPアドレスとルーター構成を維持しながら、セグメントを簡単に作成するためにブリッジによって作成されるゾーンの一種です。セキュリティゾーンでは、セグメント間のファイアウォールを有効にするかどうかを選択できます。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_SmartProvisioning_WebAdmin/16741.htm

最新問題**: 39**
チェックポイントホストオブジェクトについて正しいのは次のうちどれですか？
A. チェックポイントホストには、複数のインターフェイスがインストールされている場合でもルーティング機能はありません。
B. チェックポイントホストはIP転送メカニズムを持つことができます。
C. CheckPointHostはファイアウォールとして機能できます。

D. R77.30以前のバージョンからR80にアップグレードすると、チェックポイントホストオブジェクトがゲートウェイオブジェクトに変換されます。
Answer: A (メーッセージを残す**)**

最新問題**: 40**
ボブとジョーはどちらも、Gaiaプラットフォームで管理者の役割を持っています。ボブはWebUIにログインし、ジョーはCLIを介してログインします。ボブとジョーの両方がログインしている次のシナリオを最もよく表すものを選択してください。
A. Joeがログインすると、Bobは自動的にログアウトされます。
B. ボブは、ジョーがログインしたというプロンプトを受け取ります。
C. データベースはBobによってロックされ、Joeは変更を加えることができなくなります。
D. 両方とも異なるインターフェースにログインしているため、両方とも変更を加えることができます。
Answer: (解答を表示する**)**

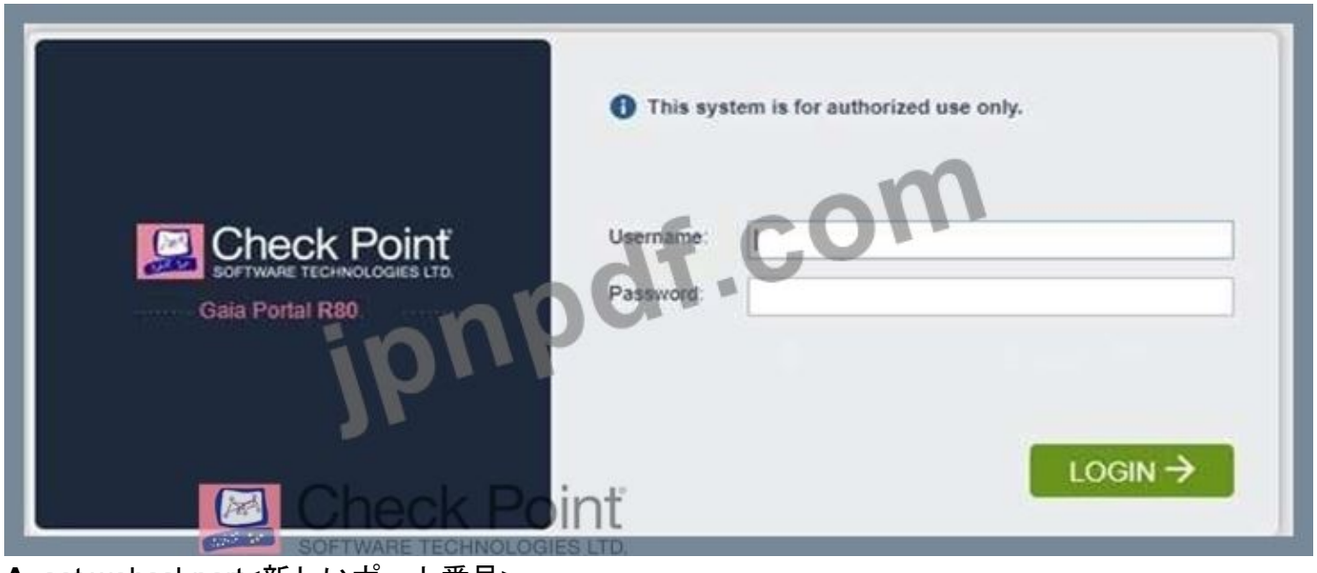
最新問題**: 41**
管理者は、本社と支社の間にIPsecサイト間VPNを作成しています。両方のオフィスは、同じセキュリティ管理サーバーによって管理されるCheck PointSecurityGatewayによって保護されています。事前共有シークレットを指定するようにVPNコミュニティを構成しているときに、管理者は事前共有シークレットを有効にするチェックボックスが共有されており、有効にできないことに気付きました。なぜ彼は事前共有秘密を指定できないのですか？
A. セキュリティゲートウェイはR75.40より前のものです。
B. 両方のセキュリティゲートウェイでIPsecVPNブレードを有効にする必要があります。
C. 証明書ベースの認証は、同じSMSによって管理される2つのセキュリティゲートウェイ間で使用できる唯一の認証方法です。
D. 事前共有は、サードパーティベンダーと
チェック・ポイント・セキュリティ・ゲートウェイ。
Answer: B (メーッセージを残す**)**

最新問題**: 42**
SmartConsoleに同時にログインしている2人の管理者がいて、オブジェクトがロックされている場合編集中、他の管理者が利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. セッションを公開または破棄します。
B. セッションを元に戻します。
C. ポリシーを保存してインストールします。
D. 古いバージョンのデータベースを削除します。
Answer: A (メーッセージを残す**)**
説明
すべての管理者が変更を利用できるようにし、編集中のオブジェクトとルール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。

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、セッションを公開する必要があります。セッションを公開すると、新しいデータベースバージョンが作成されます。
[ポリシーのインストール]を選択すると、未公開の変更をすべて公開するように求められます。をインストールすることはできません
含まれている変更が公開されていない場合のポリシー。

最新問題: **43**
次のうち、識別名の構成要素ではないものはどれですか？
A. 組織単位
B. 国
C. 一般名
D. ユーザーコンテナ
Answer: D (メーッセージを残す)
説明
識別名コンポーネント
CN =一般名、OU =組織単位、O =組織、L =地域、ST =州または県、C =国名参照：

最新問題: **44**
ALPHA Corpネットワークの管理者であるKofiは、デフォルトのHTTPSポートに現在設定されているデフォルトのGaiaWebUIポータルポート番号を変更したいと考えています。このTCPポートを変更するには、どのCLISHコマンドが必要ですか？



A. set webssl-port<新しいポート番号>
B. ガイアポータルポートを設定<新しいポート番号>
C. Gaia-portalhttps-port<新しいポート番号>を設定します
D. ウェブhttps-port<新しいポート番号>を設定します
Answer: A (メーッセージを残す)
クリッシュで

A.セキュリティゲートウェイ/各クラスタメンバーのコマンドラインに接続します。
B.Clishにログインします。
C.目的のポートを設定します（例ポート4434）：
HostName> set web ssl-port <Port_Number>
D.変更を保存します：
ホスト名>設定の保存
E.構成が保存されたことを確認します。
[Expert @ HostName]#grep'httpd :ssl_port' / config / db / initial
参照 :https ://supportcenter.checkpoint.com/supportcenter/portal？
eventSubmit_doGoviewsolutiondetails =＆solutionid = sk83482

最新問題**: 45**
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に次のものが必要です。
A. 非武装地帯
B. 各セキュリティゲートウェイが少なくとも1つのルールを適用すること
C. ルーティングテーブル
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**)**

最新問題**: 46**
パケットフィルタリングの利点ではないものは何ですか？
A. セキュリティが低く、ネットワーク層の上にスクリーニングがない
B. アプリケーションの独立性
C. 高性能
D. スケーラビリティ
Answer: A (メーッセージを残す**)**
説明
パケットフィルターの長所と短所

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

参照：

最新問題: **47**
ルールベースの効率を最適化するには、最もヒットするルールはどこにあるべきですか？
A. ルールベースから削除されました。
B. ルールベースの中央に向かって。
C. ルールベースの上部に向かって。
D. ルールベースの下部に向かって。
Answer: C (メーッセージを残す**)**
一致するルールが見つかるかどうか、より少ないルールがチェックされた場合、デバイスが使用しているCPUサイクルがより少なくなることは論理的です。チェックポイントは、上の最初のルールから下の最後のルールまでのセッションと一致します。

最新問題: **48**
上司は、新しいビジネスパートナーサイトへのVPNを設定するように要求します。パートナーサイトの管理者がVPN設定を提供すると、彼がIKEフェーズ1用にAES 128をセットアップし、IKEフェーズ2用にAES256をセットアップしていることに気付きます。これが問題のあるセットアップである理由は何ですか。
A. 2つのアルゴリズムのキー長は同じではないため、連携しません。エラーが発生します
...提案は選択されていません...
B. データの暗号化には最長のキー長が選択され、トンネルのセットアップのパフォーマンスが向上するために短いキー長が選択されているため、すべて問題ありません。
C. フェーズ2を保護するフェーズ1キーには128ビットキーのみが使用されるため、フェーズ2でキーの長さが長くなるとパフォーマンスが低下するだけで、フェーズ1ではキーが短くなるためセキュリティが向上しません。
D. すべて問題なく、そのまま使用できます。
Answer: C (メーッセージを残す**)**
説明/参照：

最新問題: **49**
空欄に記入してください。ソフトウェアコンテナには_____種類があります_____
A. 3; セキュリティ管理。セキュリティゲートウェイとエンドポイントのセキュリティ。
B. 3; セキュリティゲートウェイ、エンドポイントセキュリティ、およびゲートウェイ管理。
C. 2つ; エンドポイントセキュリティとセキュリティゲートウェイ
D. 2つ; セキュリティ管理とエンドポイントセキュリティ
Answer: A (メーッセージを残す**)**

最新問題: **50**
Tinaは、現在新しいCheckPointR80をレビューしている新しい管理者です。

管理コンソールインターフェイス。[ゲートウェイ]ビューで、彼女は下のスクリーンショットのように[概要]画面を確認しています。 オープンサーバー」とは何ですか？

A. OpenSSLを使用するCheckPointManagementServerソフトウェア。
B. OpenServerConsortiumが承認したサーバーハードウェア
セキュリティと可用性。
C. OpenSystemsInterconnectionを使用してデプロイされたCheckPointManagement Server
（OSI）サーバーとセキュリティの展開モデル。
D. CheckPoint以外のアプライアンスにデプロイされたCheckPointソフトウェア。
Answer: D (メーッセージを残す**)**

最新問題**: 51**
以下のルールをご覧ください。左の列のロック記号はどういう意味ですか？最良の答えを選択してください。
A. 現在の管理者には、脅威防止ポリシーに対する読み取り専用のアクセス許可があります。
B. 別のユーザーが編集のためにルールをロックしました。
C. 構成ロックが存在します。ロック記号をクリックして、読み取り/書き込みアクセスを取得します。
D. 他の誰かがポリシーを編集しているため、現在の管理者は読み取り専用としてログインしています。
Answer: B (メーッセージを残す**)**
説明
管理者のコラボレーション
複数の管理者が同時にセキュリティ管理サーバーに接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。
管理者がSmartConsoleを介してセキュリティ管理サーバーにログインすると、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、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールに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。

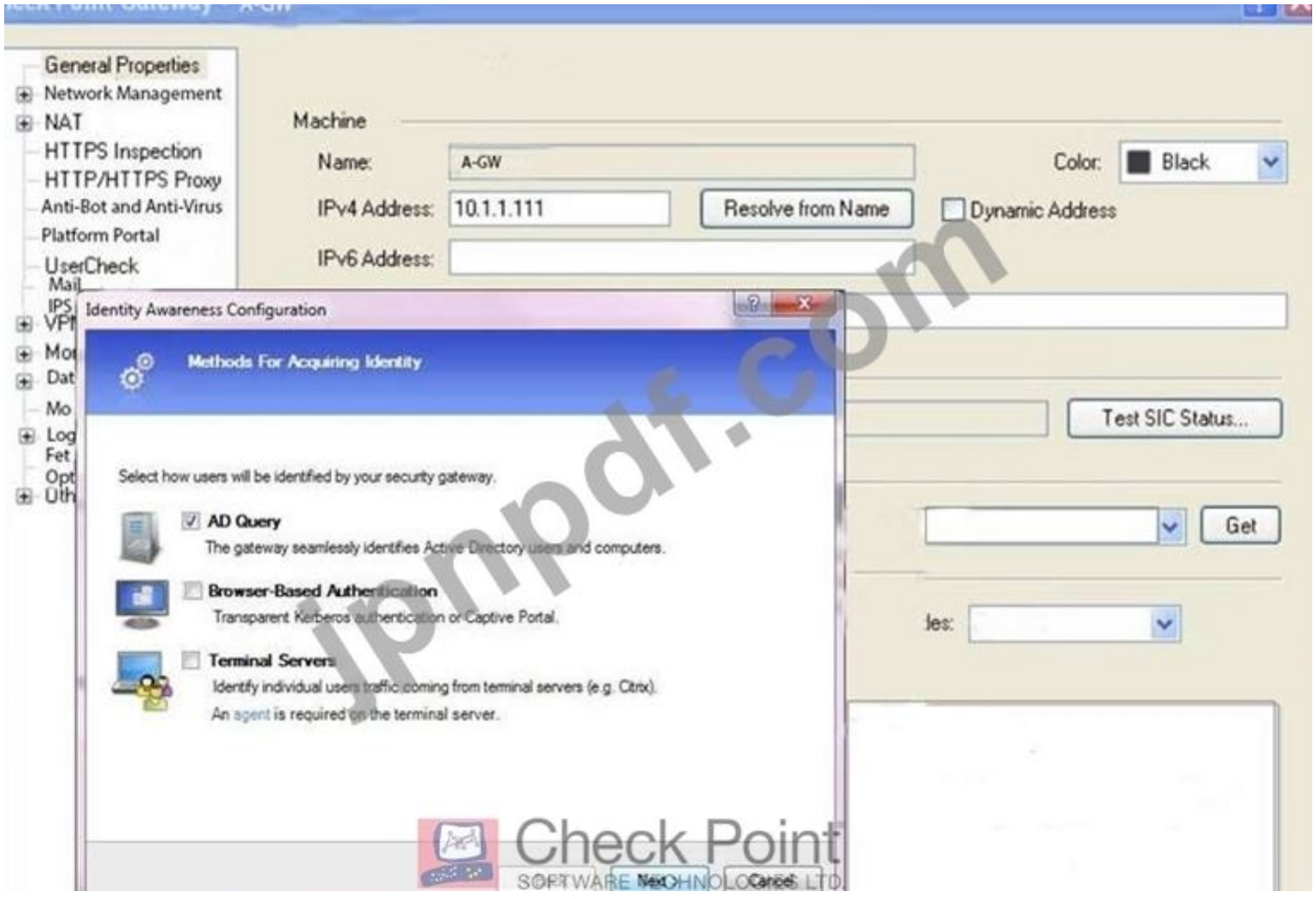
最新問題**: 52**

次のうち、Endpoint Identity Agentのタイプではないものはどれですか？
A. ターミナル
B. 軽い
C. フル
D. カスタム
Answer: A (メーッセージを残す**)**
説明/参照 :https ://supportcenter.checkpoint.com/supportcenter/portal？
eventSubmit_doGoviewsolutiondetails =&solutionid = sk107415

最新問題**: 53**
以下のルールをご覧ください。左の列のロック記号はどういう意味ですか？最良の答えを選択してください。

A. 現在の管理者には、脅威防止ポリシーに対する読み取り専用のアクセス許可があります。
B. 別のユーザーが編集のためにルールをロックしました。
C. 構成ロックが存在します。ロック記号をクリックして、読み取り/書き込みアクセスを取得します。
D. 他の誰かがポリシーを編集しているため、現在の管理者は読み取り専用としてログインしています。
Answer: B (メーッセージを残す**)**
説明/参照：
Explanation:管理者コラボレーション
複数の管理者が同時にセキュリティ管理サーバーに接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。
管理者がSmartConsoleを介してセキュリティ管理サーバーにログインすると、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、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールに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。
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 124265

最新問題**: 54**
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、上記の構成がサポートされます。

A. ActiveDirectory統合で機能するKerberosSSO

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

C. キャプティブポータルの義務的な使用

D. ブラウザベースの構成済み認証で使用されるポート443または80

Answer: B (メーッセージを残す)

説明

Identity Awarenessを有効にするには：

IdentityAwarenessConfigurationウィザードが開きます。

最新問題: **55**

ビジターモードに関して正しい説明は何ですか？

A. ESPトラフィックのみがポートTCP443を介してトンネリングされます。

B. すべてのVPNトラフィックはUDPポート4500を介してトンネリングされます。

C. VPN認証と暗号化されたトラフィックは、ポートTCP443を介してトンネリングされます。

D. メインモードとクイックモードのトラフィックのみがTCPポート443でトンネリングされます。

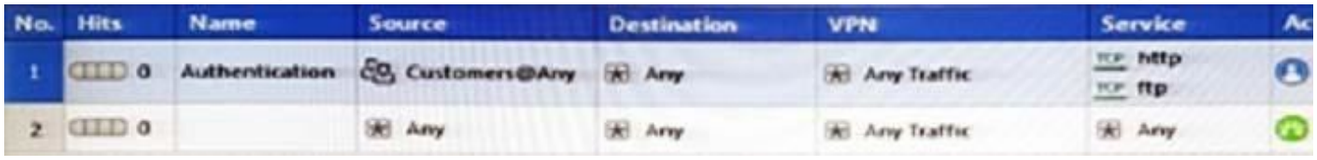
Answer: C (メーッセージを残す)

最新問題: **56**

以下のルールをご覧ください。左の列のロック記号はどういう意味ですか？最良の答えを選択してください。

A. 現在の管理者には、脅威防止ポリシーに対する読み取り専用のアクセス許可があります。
B. 別のユーザーが編集のためにルールをロックしました。
C. 構成ロックが存在します。ロック記号をクリックして、読み取り/書き込みアクセスを取得します。
D. 他の誰かがポリシーを編集しているため、現在の管理者は読み取り専用としてログインしています。
Answer: B (メーッセージを残す**)**
管理者のコラボレーション
複数の管理者が同時にセキュリティ管理サーバーに接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。
管理者がSmartConsoleを介してセキュリティ管理サーバーにログインすると、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、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールに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。
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 124265

最新問題**: 57**
ルールを確認します。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。



内部ネットワークのユーザーがHTTPを使用してインターネットを閲覧しようとするとどうなりますか？ユーザー：
A. 認証を求められることなくインターネットにアクセスできます。
B. クライアント認証デーモンポート259にTelnetを実行した後、インターネットに接続できます。
C. インターネットに正常に接続する前に3回プロンプトが表示されます。
D. 認証後、インターネットに正常に接続できます。
Answer: A (メーッセージを残す**)**

最新問題**: 58**
R80ユーティリティのfwモニターは、_____のトラブルシューティングに使用されます
A. ユーザーデータベースの破損
B. LDAPの競合
C. 交通問題
D. フェーズ2のキーネゴシエーション
Answer: C (メーッセージを残す**)**
説明

チェックポイントのFWモニターは、パケットレベルでネットワークトラフィックをキャプチャするための強力な組み込みツールです。FW Monitorユーティリティは、FireWallインスペクションチェーンに沿った複数のキャプチャポイントでネットワークパケットをキャプチャします。
これらのキャプチャされたパケットは、後でWireSharkを使用して検査できます。

最新問題: **59**
あなたはAlphaCorpの管理者です。R80管理サーバーにログインしました。ルールベースにいくつかの変更を加えていますが、ルールNo.6の横に鉛筆アイコンがあることに注意してください。

これは何を意味するのでしょうか？
A. ルールNo.6は、別の管理セッションで削除対象としてマークされています。
B. ルールNo.6は、管理セッションで削除対象としてマークされています。
C. ルールNo.6は、管理セッションで編集するためにマークされています。
D. ルールNo.6は、別の管理セッションで編集するためにマークされています。
Answer: C (メーッセージを残す**)**

最新問題: **60**
ネットワークでアクティビティを発見しました。取るべき最善の即時行動は何ですか？
A. トラフィックをブロックするポリシールールを作成します。
B. 疑わしいアクションルールを作成して、そのトラフィックをブロックします。
C. 変更を加える前に、トラフィックが識別されるまで待ちます。
D. ISPに連絡してトラフィックをブロックします。
Answer: B (メーッセージを残す**)**
説明/参照：
参照：https ://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_LoggingAndMonitoring_AdminGuide / html_frameset.htm？topic = document / R80.10 / WebAdminGuides / EN / CP_R80.10_LoggingAndMonitoring_AdminGuide / 118300

最新問題: **61**
SmartViewTrackerを使用してNATエントリのトラブルシューティングを行っています。ソースNATを使用している場合、NATされたソースポートを表示するためにどの列をチェックしますか？

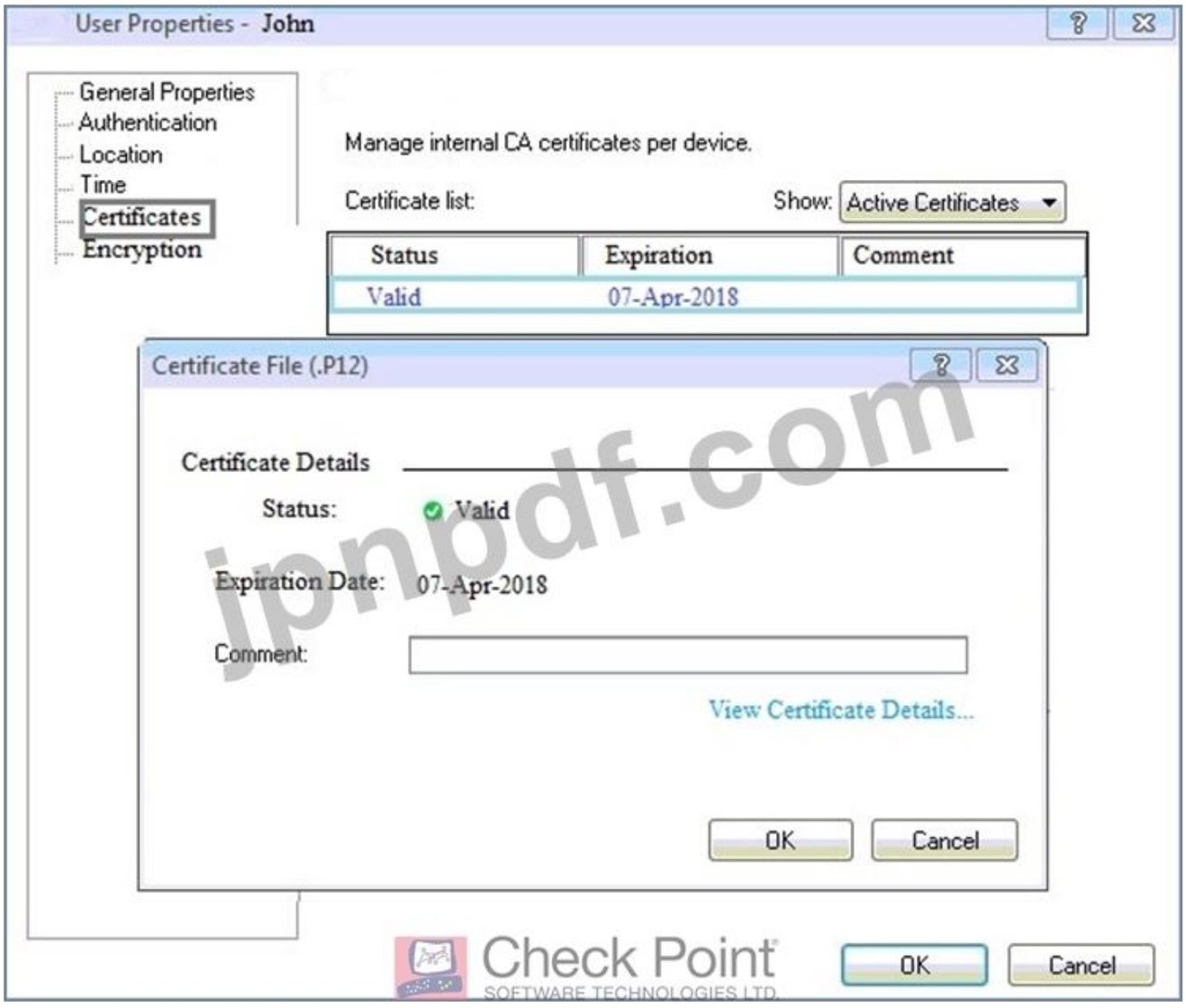
URL List Version	☐	100
Unreachable directories	☐	100
Update Service	☐	100
Update Source	☐	100
Update Status	☐	100
User Action Comment	☐	100
User Additional Information	☐	100
User Check	☐	100
User DN	☐	100
User Directory	☐	100
User Display Name	☐	100
User Group	☐	100
User Reported Wrong Category	☐	100
User Response	☐	100
User SID	☐	100
User UID	☐	100
User's IP	☐	100
UserCheck ID	☐	100
UserCheck Interaction Name	☐	100
UserCheck Message to User	☐	100
UserCheck Scope	☐	100
UserCheck User Input	☐	100
VLAN ID	☐	100
VPN Feature	☐	100
VPN Peer Gateway	☐	100
Version	☐	100
Virtual Link	☐	100
Virus Name	☐	100
VoIP Duration	☐	100
VoIP Log Type	☐	100
VoIP Reject Reason	☐	100
VoIP Reject Reason Information	☐	100

Web Filtering Categories	☐	100
Wire Byte/Sec Out	☐	100
Wire Byte/Sec in	☐	100
Wire Packet/Sec Out	☐	100
Wire Packet/Sec in	☐	100
Write Access	☐	100
XlateDPort	☐	100
XlateDst	☐	100
XlateSPort	☐	100
XlateSrc	☐	100
Special properties	☐	100

A. XlateSPort
B. XlateDst
C. XlateSrc
D. XlateDPort
Answer: A (メーッセージを残す**)**

最新問題**: 62**
空欄に記入してください :LDAPサーバーは1つ以上の_____を保持しています。
A. サーバーユニット
B. 管理者ユニット
C. アカウント単位
D. アカウントサーバー
Answer: C (メーッセージを残す**)**
説明
参照：

最新問題**: 63**
次の図を見ることができます。



その上に何が表示されますか？

A. ユーザーJohnの.p12証明書のプロパティが期限切れになりました。

B. 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。

C. ジョンのゲートウェイのVPN証明書のプロパティ。

D. ジョンのパスワードの共有秘密プロパティ。

Answer: B (メーッセージを残す**)**

最新問題**: 64**

SmartView Trackerで、スプーフィング防止のためにパケットがドロップされたときに表示されるルールはどれですか。

A. クリーンアップルール

B. ルール番号の下の空白のフィールド

C. ルール1

D. ルール0

Answer: D (メーッセージを残す**)**

最新問題**: 65**

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

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

B. /var/log/Cpbackup/backups/backup/backup_fw.tar

C. /var/log/Cpbackup/backups/backups/backup_fw.tar

D. /var/log/Cpbackup/backups/backup_fw.tgz

Answer: D (メーッセージを残す)

Gaiaのバックアップ機能を使用すると、Gaia OSとセキュリティ管理サーバーデータベースの構成をバックアップしたり、以前に保存した構成を復元したりできます。

構成は、次のディレクトリの.tgzファイルに保存されます。

Gaia OS Version	Hardware	Local Directory
R75.40 - R77.20	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	/var/CPbackup/backups/
R77.30	Check Point appliances	/var/log/CPbackup/backups/
	Open Server	

参照：https ://supportcenter.checkpoint.com/supportcenter/portal？action = portals.SearchResultMainAction＆eventSubmit_doGoviewsolutiondetails =＆solutionid = sk91400

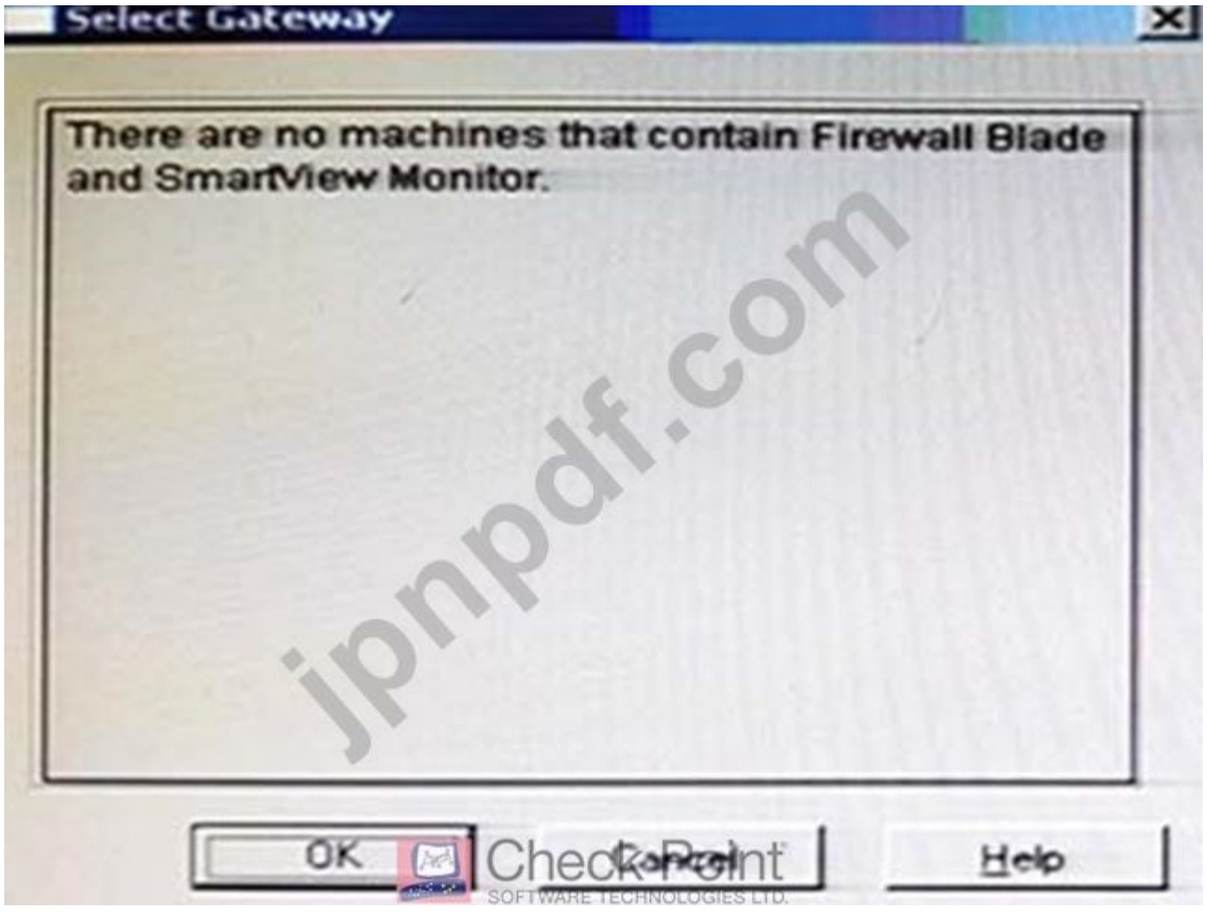
最新問題**: 66**

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

残念ながら、次のメッセージが表示されます。

「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どうすればよいですか？最良の答えを与えてください。



A. セキュリティゲートウェイのSmartViewMonitorライセンスを購入します。
B. セキュリティゲートウェイで監視を有効にします。
C. セキュリティ管理サーバーで監視を有効にします。
D. セキュリティ管理サーバーのSmartViewMonitorライセンスを購入します。
Answer: B (メーッセージを残す**)**

最新問題**: 67**
脅威防止ポリシーレイヤーの3つの競合解決ルールは何ですか？
A. アクションの競合、宛先の競合、設定の競合
B. スコープでの競合、設定での競合、および例外での競合
C. 設定の競合、アドレスの競合、例外の競合
D. アクションでの競合、例外での競合、および設定での競合
Answer: (解答を表示する**)**

最新問題**: 68**
キャプティブポータルの目的は何ですか？
A. SmartConsoleへのリモートアクセスを提供します
B. SmartConsoleでユーザー権限を管理します
C. ユーザーを認証し、インターネットや企業リソースへのアクセスを許可します
D. ユーザーを認証し、GaiaOSへのアクセスを許可します

Answer: C (メッセージを残す)
説明
参照 :https ://www.checkpoint.com/products/identity-awareness-software-blade/

最新問題: **69**
空欄に記入してください :トンネルテストパケットが応答を呼び出さなくなると、SmartViewモニターは次のように表示します
特定のVPNトンネルの_____。
A. ダウン
B. 無応答
C. 非アクティブ
D. 失敗
Answer: (解答を表示する)
説明/参照 :https ://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm？トピック=ドキュメント/R77/ CP_R77_VPN_AdminGuide / 14018

最新問題: **70**
IKEによって実行される2フェーズネゴシエーションプロセスのフェーズ1は、_____モードで動作します。
A. メイン
B. 認証
C. クイック
D. 高アラート
Answer: A (メッセージを残す)
説明/参照：
Explanation:
フェーズIモード
セキュリティゲートウェイの間には、IKEフェーズIの2つのモードがあります。
これらのモードはIKEv1にのみ適用されます。
メインモード
▪
アグレッシブモード
▪
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_VPN_AdminGuide/13847.htm

最新問題: **71**
空欄に記入してください。RADIUSプロトコルは_____を使用してゲートウェイと通信します。
A. UDP
B. TDP
C. CCP
D. HTTP
Answer: A (メッセージを残す)
パラメーター：

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

参照 :https ://sc1.checkpoint.com/documents/R76SP/CP_R76SP_Security_System_WebAdminGuide / 105209.htm

最新問題**: 72**

次のルールベースを調べます。

ルールベースに加えられた最近の変更について何を推測できますか？

A. ルール7は、現在のセッションで「admin」管理者によって作成されました

B. 前回のポリシーのインストール以降、管理者によって8つの変更が加えられました

C. ルール1、5、および6は「admin」管理者が編集できません

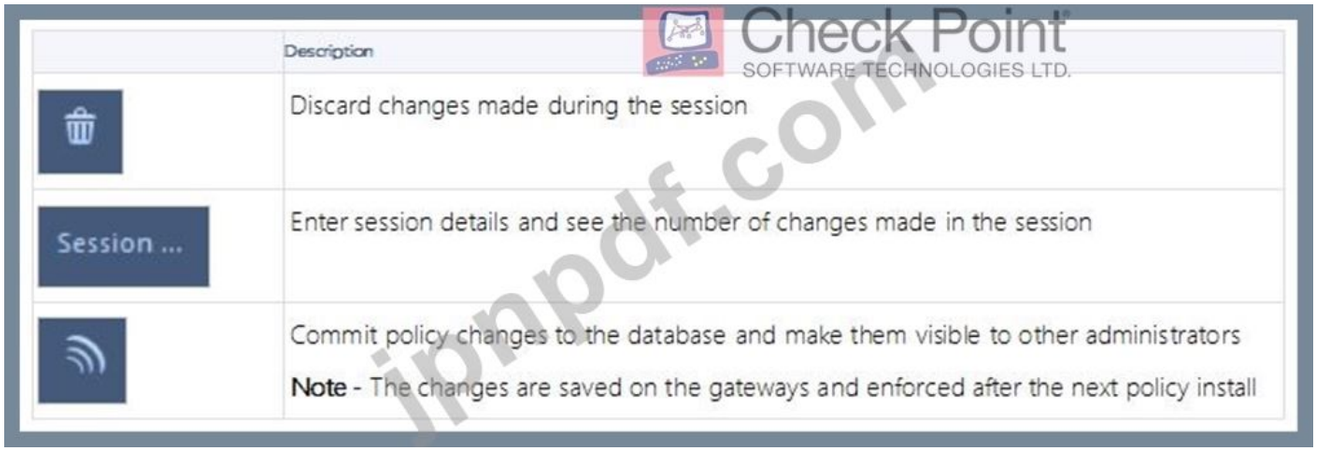
D. ルール1とオブジェクトWebサーバーが別の管理者によってロックされています

Answer: D (メーッセージを残す**)**

説明

印刷画面の上部には、行われた変更と保存されなかった変更の数を表す番号「8」があります。

セッション管理ツールバー（SmartConsoleの上部）



参照：

最新問題: **73**
SmartConsoleを介し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. セキュリティの質問
B. チェックポイントパスワード
C. SecurID
D. RADIUS
Answer: (解答を表示する**)**
認証スキーム：
-チェックポイントパスワード
-オペレーティングシステムのパスワード
-RADIUS
-SecurID
-TACAS
-未定義未定義の認証スキームを持つユーザーが何らかの形式の認証を持つセキュリティルールと一致する場合、アクセスは常に拒否されます。

最新問題: **74**
fwモニターユーティリティは、次の問題のどれをトラブルシューティングするために使用されますか？
A. ユーザーデータベースの破損
B. ログ統合エンジン
C. アドレス変換
D. フェーズ2のキーネゴシエーション
Answer: (解答を表示する**)**

最新問題: **75**
空欄に記入してください：各クラスターには_____インターフェースがあります。
A. 5
B. 2つ

C. 3つ
D. 4つ
Answer: (解答を表示する**)**
各クラスターメンバーには、3つのインターフェイスがあります。1つは外部インターフェイス、1つは内部インターフェイス、もう1つは同期用です。各方向を向いているクラスタメンバーインターフェイスは、スイッチ、ルーター、またはVLANスイッチを介して接続されます。

最新問題**: 76**
空欄に記入してください：高可用性デプロイメントは、_____クラスターおよび負荷分散と呼ばれます
デプロイメントは_____クラスターと呼ばれます。
A. スタンバイ/スタンバイ; アクティブ/アクティブ
B. アクティブ/アクティブ; スタンバイ/スタンバイ
C. アクティブ/アクティブ; アクティブ/スタンバイ;
D. アクティブ/スタンバイ; アクティブ/アクティブ
Answer: (解答を表示する**)**
説明
高可用性クラスターでは、1つのメンバーのみがアクティブになります（アクティブ/スタンバイ操作）。
ClusterXLロードシェアリングは、複数のメンバーの合計スループットが
増加しました。負荷分散構成では、クラスター内で機能しているすべてのメンバーがアクティブであり、
ネットワークトラフィック（アクティブ/アクティブ操作）。

最新問題**: 77**
空欄に記入してください。ネットワークポリシーレイヤーでは、暗黙の最後のルールのデフォルトのアクションは_____すべてのトラフィックです。ただし、アプリケーション制御ポリシーレイヤーでは、デフォルトのアクションは_____すべてのトラフィックです。
A. リダイレクト; 落とす
B. ドロップ; 受け入れる
C. 受け入れる; リダイレクト
D. 受け入れる; 落とす
Answer: B (メーッセージを残す**)**

最新問題**: 78**

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

A. ルール4の[ソース]列または[宛先]列を変更します
B. ルール4の[サービス]列からサービスHTTPを削除します。
C. 何もありません
D. ルール2の列VPNを変更して、特定のトラフィックへのアクセスを制限します。
Answer: (解答を表示する**)**

最新問題**: 79**
Gaiaで一度に読み取り/書き込みアクセスできるユーザーは何人ですか？
A. 1つ
B. 3つ
C. 2つ
D. 無限
Answer: A (メーッセージを残す**)**

最新問題**: 80**
UserCheckとは何ですか？
A. 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
B. 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コミュニケーションツール
C. ユーザーの資格情報を確認するためのメッセージングツールユーザー
D. ユーザーが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
Answer: D (メーッセージを残す**)**

最新問題**: 81**
Gaiaオペレーティングシステムはどのルーティングプロトコルをサポートしていますか？
A. BGP、OSPF、RIP
B. BGP、OSPF、EIGRP、PIM、IGMP
C. BGP、OSPF、RIP、PIM、IGMP
D. BGP、OSPF、RIP、EIGRP

Answer: A (メーッセージを残す)
説明
Advanced Routing Suite
Advanced Routing Suite CLIは、Advanced NetworkingSoftwareBladeの一部として利用できます。
スケーラブルでフォールトトレラントで安全なネットワークの実装を検討している組織向けの
AdvancedNetworking
ブレードを使用すると、BGP、OSPF、RIPv1、および
セキュリティゲートウェイ上のRIPv2。OSPF、RIPv1、およびRIPv2は、単一の自律型での動的ルーティングを可能にします
ネットワーク障害を回避するためのシステム（単一の部門、会社、またはサービスプロバイダーなど）。BGPは提供します
複数の自律システムを含むより複雑なネットワーク全体での動的ルーティングのサポート-
会社が2つのサービスプロバイダーを使用する場合、またはネットワークを異なる複数のエリアに分割する場合
それぞれのパフォーマンスを担当する管理者。

最新問題: **82**
コマンドラインからGAIAでDHCPサービスを構成できるユーティリティはどれですか。
A. ifconfig
B. dhcp_cfg
C. sysconfig
D. cpconfig
Answer: C (メーッセージを残す)
Sysconfig構成オプション

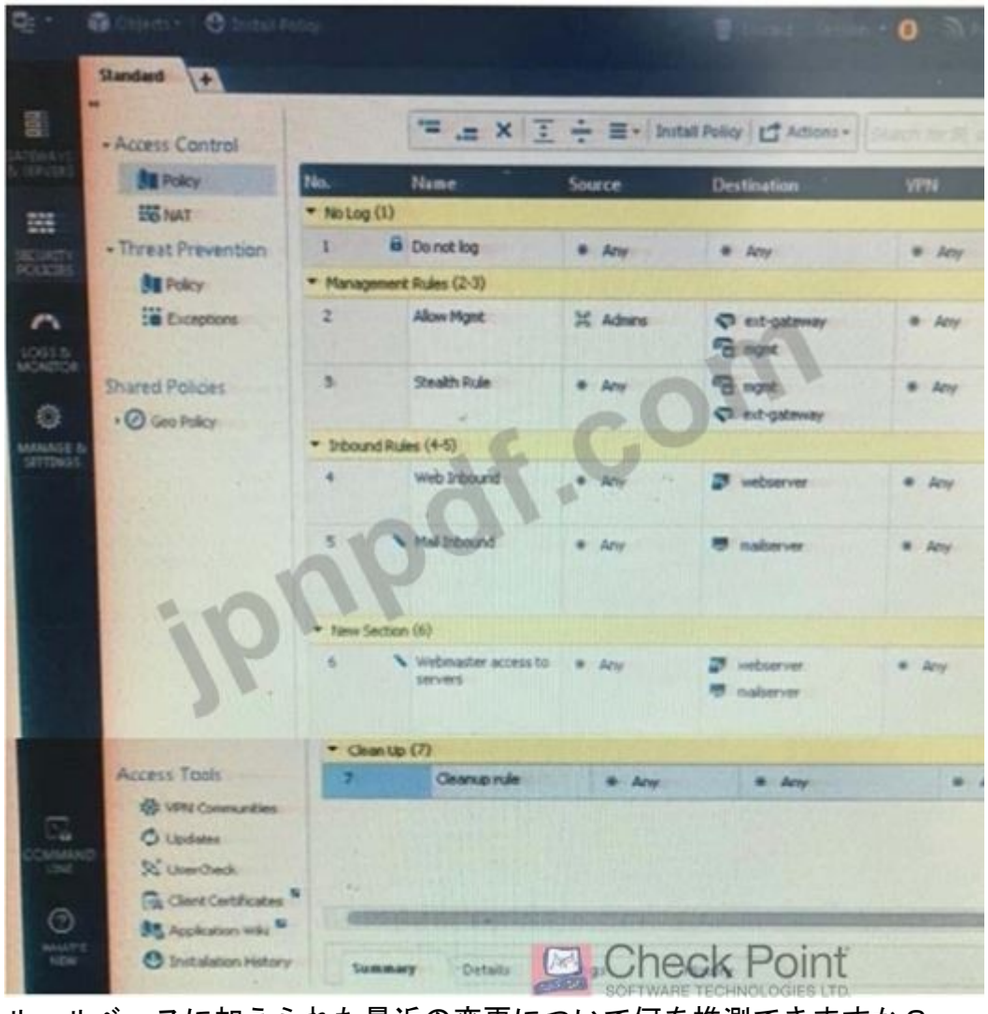
Menu Item	Purpose
7	DHCP Server Configuration	Configure SecurePlatform DHCP Server.
8	DHCP Relay Configuration	Setup DHCP Relay.

参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_Splat_AdminGuide/51548.htm注 :GAIAシステムでは回答が不可能なため、質問は間違っている必要があります。これはSPLATバージョンである必要があります。GAIAリファレンスのDHCPCLI構成 :https ://sc1.checkpoint.com/documents/R76/ CP_R76_Gaia_WebAdmin / 73181.htm#o80096

最新問題: **83**
帯域幅とトラフィック制御ルールを適用するために使用されるポリシータイプはどれですか？

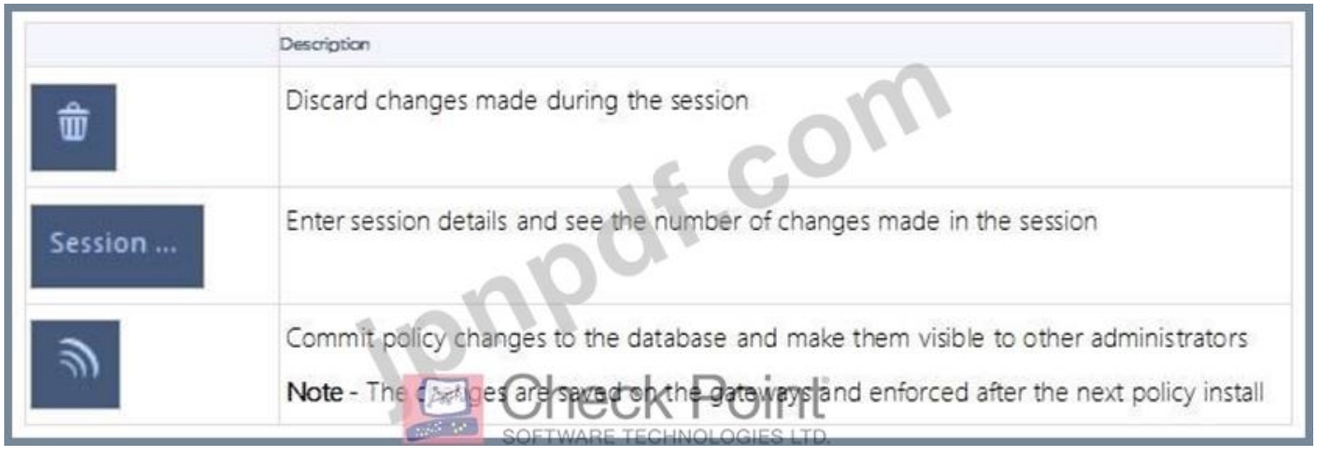
A. 脅威エミュレーション
B. アクセス制御
C. QoS
D. 脅威の防止
Answer: C (メーッセージを残す**)**
説明/参照：
Explanation:
チェックポイントのQoSソリューション
QoSは、Check Point Software Technologies Ltd.のポリシーベースのQoS管理ソリューションであり、帯域幅管理ソリューションのニーズを満たします。QoSは、ネットワークのハードウェアとソフトウェア全体に強制を分散することにより、ネットワーク全体でトラフィックをエンドツーエンドで管理する、ソフトウェアのみに基づく独自のアプリケーションです。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_QoS_AdminGuide/index.html

最新問題**: 84**
次のルールベースを調べます。



ルールベースに加えられた最近の変更について何を推測できますか？
A. ルール7は、現在のセッションで「admin」管理者によって作成されました
B. 前回のポリシーのインストール以降、管理者によって8つの変更が加えられました

C. ルール1、5、および6は「admin」管理者が編集できません
D. ルール1とオブジェクトWebサーバーが別の管理者によってロックされています
Answer: D (メッセージを残す)
説明/参照：
外植：印刷画面の上部には、行われた変更と保存されなかった変更の数を表す番号「8」があります。
セッション管理ツールバー（SmartConsoleの上部）



参照：https://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？トピック=ドキュメント/R80/ CP_R80_SecMGMT / 117948

最新問題: **85**
次のうち、VPN簡易モードとVPNコミュニティの要素ではないものはどれですか？
A. ルールベースの「暗号化」アクション
B. 恒久的なトンネル
C. ルールベースの「VPN」列
D. 設定チェックボックス「暗号化されたすべてのトラフィックを受け入れる」
Answer: A (メッセージを残す)
説明/参照：
Explanation:
従来のモードから簡体字モードへの移行
従来型モードVPNから簡体字モードに移行するには：
1.[グローバルプロパティ]>[VPN]ページで、次のいずれかのオプションを選択します。
*すべての新しいファイアウォールポリシーへの簡易モード
*新しいファイアウォールポリシーごとに従来型または簡体字
2.[OK]をクリックします。
3. R80 SmartConsoleメニューから、[ポリシーの管理]を選択します。
[ポリシーの管理]ウィンドウが開きます。
4.[新規]をクリックします。
[新しいポリシー]ウィンドウが開きます。
5.新しいポリシーに名前を付けて、[アクセス制御]を選択します。
セキュリティポリシールールベースで、VPNとマークされた新しい列が表示され、[アクション]列で[暗号化]オ

プションが使用できなくなりました。これで、簡易モードで作業しています。
参照 :http ://dl3.checkpoint.com/paid/05/05e695b2012b4fd1d2bdfeccecd29290/CP_R80BC_VPN_AdminGuide.pdf？HashKey = 1479823792_55fbc10656c87db4fcf742f4899ba90d &xtn = .pdf

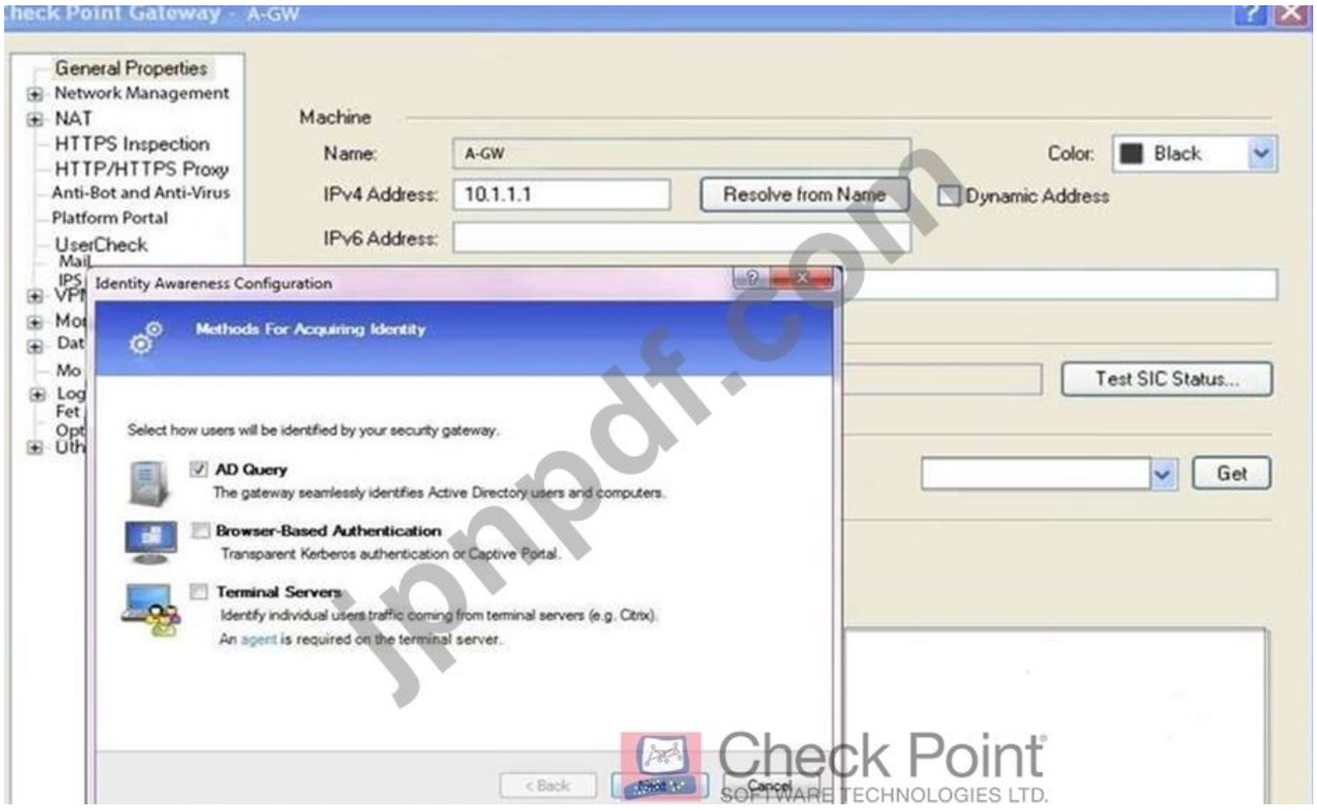
最新問題**: 86**
空欄に記入してください :ツール_____はR80セキュリティゲートウェイ構成レポートを生成します。
A. infoCP
B. infoview
C. cpinfo
D. fw cpinfo
Answer: C (メーッセージを残す**)**
CPInfoは、実行時に顧客のマシン上の診断データを収集し、それをチェックポイントサーバーにアップロードする自動更新可能なユーティリティです チェックポイントサーバーにファイルをアップロードするためのスタンドアロンのcp_uploaderユーティリティに代わるものです）。
CPinfo出力ファイルを使用すると、離れた場所から顧客の設定を分析できます。小切手
ポイントサポートエンジニアは、実際の顧客のセキュリティポリシーとオブジェクトを表示しながら、デモモードでCPinfoファイルを開くことができます。これにより、お客様の構成と環境設定の詳細な分析が可能になります。
Check Pointサポートに連絡するときは、セキュリティからcpinfoファイルを収集してください
ケースに関係する管理サーバーとセキュリティゲートウェイ。

最新問題**: 87**
ファイアウォールクラスターには2つのR77.30セキュリティゲートウェイがあります。それらはFW_AおよびFW_Bという名前です。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よりも優先度が高くなるように構成されています。FW_Aはアクティブで、午前中にトラフィックを処理していました。FW_Bはスタンバイでした。午前1100年頃、そのインターフェイスがダウンし、これにより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のインターフェースの問題は解決され、操作可能になりました。クラスタに再参加すると、自動的にアクティブになりますか？
A. いいえ、クラスターオブジェクトプロパティの[現在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
B. いいえ、 現在アクティブなクラスターメンバーを維持する」オプションがグローバルプロパティで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
D. 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です
Answer: A (メーッセージを残す**)**
説明/参照：

Explanation:
セキュリティゲートウェイが回復するとどうなりますか？
ロードシェアリング構成では、クラスター内の障害が発生したセキュリティゲートウェイが回復すると、すべての接続がすべてのアクティブなメンバーに再分散されます。ClusterXLの高可用性と負荷分散ClusterXL管理ガイドR77バージョン|31高可用性構成では、クラスター内の障害が発生したセキュリティゲートウェイが回復する場合、回復方法は構成されたクラスター設定によって異なります。オプションは次のとおりです。
*現在のアクティブセキュリティゲートウェイを維持するということは、1つのメンバーが優先度の低いメンバーに制御を渡した場合、優先度の低いメンバーに障害が発生した場合にのみ、優先度の高いメンバーに制御が戻されることを意味します。このモードは、フェイルオーバーイベントの数を最小限に抑えるために、すべてのメンバーがトラフィックを同等に処理できる場合に推奨されます。
*優先度の高いセキュリティゲートウェイに切り替えると、優先度の低いメンバーが制御権を持ち、優先度の高いメンバーが復元された場合、優先度の高いメンバーに制御が戻されます。このモードは、1つのメンバーが接続を処理するための設備が整っている場合に推奨されるため、デフォルトのセキュリティゲートウェイになります。
参照：
http ://dl3.checkpoint.com/paid/7e/7ef174cf00762ceaf228384ea20ea64a/CP_R77_ClusterXL_AdminGuide.pdf？HashKey = 1479822138_31410b1f8360074be87fd8f1ab682464＆xtn = .pdf

最新問題**: 88**
VMACモードが有効になっていることを確認するには、すべてのクラスターメンバーでどのCLIコマンドを実行する必要がありますか？
最良の答えを選択する。
A. fw ctl set int fwha vmac global param enabled
B. fw ctl get int fwha vmac global param enabled; コマンドの結果は値1を返す必要があります
C. cphaprob -a if
D. fw ctl get int fwha_vmac_global_param_enabled; コマンドの結果は値1を返す必要があります
Answer: B (メーッセージを残す**)**
説明/参照：
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_ClusterXL_AdminGuide/7292.htm

最新問題**: 89**
安全なネットワークの導入に関する3つの考慮事項は何ですか？
A. ブリッジモード、リモート、およびスタンドアロン
B. リモート、スタンドアロン、および分散
C. 分散、ブリッジモード、およびリモート
D. スタンドアロン、分散、およびブリッジモード
Answer: C (メーッセージを残す**)**
最新問題**: 90**
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、上記の構成がサポートされます。

A. ActiveDirectory統合で機能するKerberosSSO

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

C. キャプティブポータルの義務的な使用

D. ブラウザベースの構成済み認証で使用されるポート443または80

Answer: (解答を表示する**)**

IdentityAwarenessを有効にするには：

1.R80SmartConsoleにログインします。

2. [ゲートウェイとサーバー]ビューで、ID認識を有効にするセキュリティゲートウェイをダブルクリックします。

3. [ネットワークセキュリティ]タブで、[ID認識]を選択します。

IdentityAwarenessConfigurationウィザードが開きます。

4.1つ以上のオプションを選択します。これらのオプションは、管理対象資産と管理対象外資産のIDを取得するための方法を設定します。

*ADクエリ-SecurityGatewayがActiveDirectoryユーザーとコンピューターをシームレスに識別できるようにします。

*ブラウザベースの認証-ユーザーをWebページに送信して、身元不明のユーザーからIDを取得します。透過的なKerberos認証が構成されている場合、ADユーザーは透過的に識別される可能性があります。

*ターミナルサーバー-ターミナルサーバー環境でユーザーを識別します（1つのIPアドレスから発信）。

参照：https ://sc1.checkpoint.com/documents/R80/CP_R80BC_IdentityAwareness/ html_frameset.htm？topic = document / R80 / CP_R80BC_IdentityAwareness / 62050

最新問題: **91**
_____は、ネットワークユーザーの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. UserCheck
B. ユーザーディレクトリ
C. ユーザーサーバー
D. ユーザーインデックス
Answer: B (メーッセージを残す**)**

最新問題: **92**
Identity Awarenessブレードを有効にしている間、IdentityAwarenessウィザードはWindowsドメインを自動的に検出しません。Windowsドメインを検出しないのはなぜですか？
A. セキュリティゲートウェイはドメインの一部ではありません
B. SmartConsoleマシンはドメインの一部ではありません
C. SMSはドメインの一部ではありません
D. グローバルプロパティでID認識が有効になっていません
Answer: B (メーッセージを残す**)**
Identity Awarenessを有効にするには：
1.SmartDashboardにログインします。
2. [ネットワークオブジェクト]ツリーから、[チェックポイント]ブランチを展開します。
3.IdentityAwarenessを有効にするSecurityGatewayをダブルクリックします。
4. [ソフトウェアブレード]セクションで、[ネットワークセキュリティ]タブの[ID認識]を選択します。
IdentityAwarenessConfigurationウィザードが開きます。
5.1つ以上のオプションを選択します。これらのオプションは、管理対象資産と管理対象外資産のIDを取得するための方法を設定します。
*ADクエリ-SecurityGatewayがActiveDirectoryユーザーとコンピューターをシームレスに識別できるようにします。
*ブラウザベースの認証-ユーザーをWebページに送信して、身元不明のユーザーからIDを取得します。透過的なKerberos認証が構成されている場合、ADユーザーは透過的に識別される可能性があります。
*ターミナルサーバー-ターミナルサーバー環境でユーザーを識別します（1つのIPアドレスから発信）。
IDソースの選択を参照してください。
注-IPシリーズアプライアンス上にあるセキュリティゲートウェイでブラウザベースの認証を有効にする場合は、Voyager管理アプリケーションのポートを443または80以外のポートに設定してください。

6.[次へ]をクリックします。
[ActiveDirectoryとの統合]ウィンドウが開きます。
SmartDashboardがドメインの一部である場合、SmartDashboardはこのドメインを自動的に提案します。このドメインを選択すると、システムは組織のActiveDirectory内のすべてのドメインコントローラーを使用してLDAPアカウントユニットを作成します。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide / 62050.htm

最新問題: **93**
ファイアウォールルールのどのオプションが一致し、1つのコミュニティのVPNゲートウェイへのトラフィックのみを許可するか
一般？
A. すべての接続（クリアまたは暗号化）
B. 暗号化されたすべてのトラフィックを受け入れる
C. 特定のVPNコミュニティ
D. すべてのサイト間VPNコミュニティ
Answer: C (メーッセージを残す**)**

最新問題: **94**
ID共有とは何ですか？
A. 管理サーバーはIDを取得してセキュリティゲートウェイと共有できます
B. ユーザーは他のユーザーとIDを共有できます
C. セキュリティゲートウェイは、他のセキュリティゲートウェイとIDを取得して共有できます
D. 管理者は他の管理者とIDを共有できます
Answer: (解答を表示する**)**
説明
ID共有
ベストプラクティス多くのセキュリティゲートウェイとADクエリを使用する環境では、次のように設定することをお勧めします
それぞれの特定のActiveDirectoryドメインコントローラーからIDを取得するための1つのセキュリティゲートウェイのみ
物理的なサイト。複数のセキュリティゲートウェイが同じADサーバーからIDを取得する場合、ADサーバーは次のことができます。
WMIクエリで過負荷になります。
SecurityGatewayオブジェクトの[IdentityAwareness]>[IdentitySharing]ページで次のオプションを設定します。

最新問題: **95**
VPNトンネルを開始しようとすると、ログに「提案が選択されていません」というエラーが何度も表示されます。他のVPN関連のログエントリはありません。VPNネゴシエーションのどのフェーズが失敗しましたか？
A. IPSECフェーズ2

B. IPSECフェーズ1
C. IKEフェーズ2
D. IKEフェーズ1
Answer: C (メーッセージを残す**)**

最新問題**: 96**
ヒットカウントデータが保持されるデフォルトの時間の長さはどれくらいですか？
A. 3ヶ月
B. 4週間
C. 12か月
D. 6か月
Answer: A (メーッセージを残す**)**
ヒットカウントデータを最大に保つ時間範囲オプションの1つを選択します。デフォルトは6か月です。
この期間、データはSecurity Management Serverデータベースに保持され、[ヒット数]列に表示されます。

最新問題**: 97**
次のうち、推奨されるライセンスモデルはどれですか？ベストアンサーを選択してください。
A. パッケージライセンスをゲートウェイのIPアドレスに関連付け、
セキュリティ管理サーバーの依存関係。
B. パッケージライセンスをセキュリティ管理のIPアドレスに関連付けるための中央ライセンス
サーバーであり、ゲートウェイの依存関係はありません。
C. パッケージライセンスをゲートウェイ管理のMACアドレスに関連付けるためのローカルライセンス
インターフェイスであり、セキュリティ管理サーバーへの依存関係はありません。
D. パッケージライセンスをセキュリティ管理のMACアドレスに関連付けるための中央ライセンス
サーバー管理インターフェースであり、ゲートウェイの依存関係はありません。
Answer: B (メーッセージを残す**)**
説明
セントラルライセンス
中央ライセンスは、ゲートウェイではなく、セキュリティ管理サーバーのIPアドレスに付加されるライセンスです。
IPアドレス。セントラルライセンスの利点は次のとおりです。

最新問題**: 98**
ロギングとモニタリングでは、トラッキングオプションはログ、詳細ログ、拡張ログです。次のオプションのうち、各ログ、詳細ログ、拡張ログに追加できるのはどれですか？
A. 会計/抑制
B. アカウンティング/拡張
C. 抑制
D. 会計
Answer: A (メーッセージを残す**)**

最新問題: **99**
銀行の分散型R77インストールでは、セキュリティゲートウェイが更新可能になっています。どのSmartConsoleアプリケーションが、今後30日以内に期限切れになるライセンスを持っているセキュリティゲートウェイを教えてくれますか？
A. SmartViewトラッカー
B. SmartPortal
C. SmartUpdate
D. SmartDashboard
Answer: C (メーッセージを残す**)**
説明/参照：

最新問題: **100**
これらのチェックポイントプロトコルのうち、_____が使用しているのはどれですか？
A. ELAおよびCPD
B. FWDとLEA
C. FWDとCPLOG
D. ELAとCPLOG
Answer: B (メーッセージを残す**)**
説明/参照：

最新問題: **101**
どの脅威防止ソフトウェアブレードが、あなたに感染する可能性のある悪意のあるソフトウェアからの保護を提供しますか
ネットワークコンピュータ？
A. マルウェア対策
B. IPS
C. アンチボット
D. スパム対策
Answer: C (メーッセージを残す**)**
説明
アンチボット
アンチボットの必要性
今日の脅威の状況には、次の2つの新しい傾向があります。
これらの傾向は両方とも、ボット攻撃によって引き起こされています。
ボットは、コンピュータに侵入する可能性のある悪意のあるソフトウェアです。多くの感染方法があります。これらには以下が含まれます
脆弱性を悪用する添付ファイルを開き、悪意のあるダウンロードをもたらすWebサイトにアクセスします。

最新問題: **102**
境界セキュリティゲートウェイを介して受け入れられたすべてのトラフィックをログに記録するための管理要

件に準拠するには、セキュリティ管理者は何をする必要がありますか？
A. SmartUpdateを使用してViewImplicitRulesパッケージをインストールします。
B. R77ゲートウェイオブジェクトに2つのログサーバーを定義します。最初のログサーバーのLof暗黙ルール。2番目のログサーバーでログルールベースを有効にします。SmartReporterを使用して、2つのログサーバーレコードを同じデータベースにマージし、HIPPAログ監査を行います。
C. R77ゲートウェイオブジェクトの[暗黙のルールをグローバルにログに記録する]チェックボックスをオンにします。
D. [グローバルプロパティ]> [レポートツール]で、[すべてのルールの追跡を有効にする]チェックボックスをオンにします [追跡]列で[なし]とマークされたルールを含む）。完全なログ履歴については、これらのログをセカンダリログサーバーに送信してください。トラブルシューティングの標準ログには、通常のログサーバーを使用します。
Answer: D (メーッセージを残す)

最新問題: **103**
ユーザー認証の失敗の原因となるルールはどれですか？

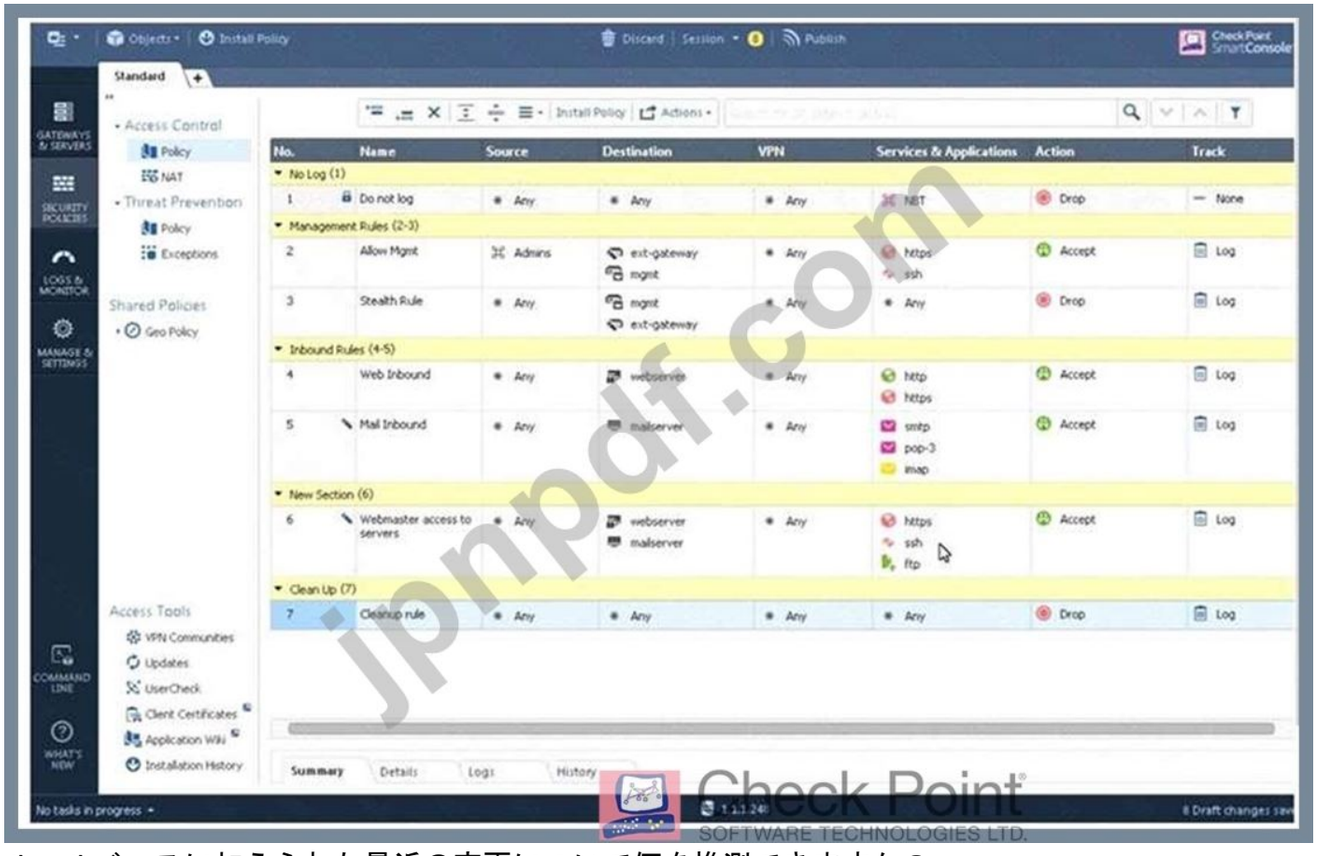
A. ルール4
B. ルール3
C. ルール6
D. ルール5
Answer: B (メーッセージを残す)

最新問題: **104**
セキュリティゲートウェイのCPUコアは通常100%使用されており、多くのパケットがドロップされていることに気づきました。現時点では、ハードウェアのアップグレードを実行するための予算はありません。ドロップを最適化するには、優先キューを使用し、ダイナミックディスパッチャーを完全に有効にすることにします。どうすればそれらを有効にできますか？
A. fw ctl multik dynamic_dispatching on
B. fw ctl multik dynamic_dispatching set_mode 9
C. fw ctl multik set_mode 9
D. fw ctl miltik pq enable
Answer: (解答を表示する)
説明/参照：

参照：https ://supportcenter.checkpoint.com/supportcenter/portal？eventSubmit_doGoviewsolutiondetails =&solutionid = sk105261

最新問題**: 105**

次のルールベースを調べます。



ルールベースに加えられた最近の変更について何を推測できますか？

A. ルール7は、現在のセッションで「admin」管理者によって作成されました

B. 前回のポリシーのインストール以降、管理者によって8つの変更が加えられました

C. ルール1、5、および6は「admin」管理者が編集できません

D. ルール1とオブジェクトWebサーバーが別の管理者によってロックされています

Answer: D (メーッセージを残す**)**

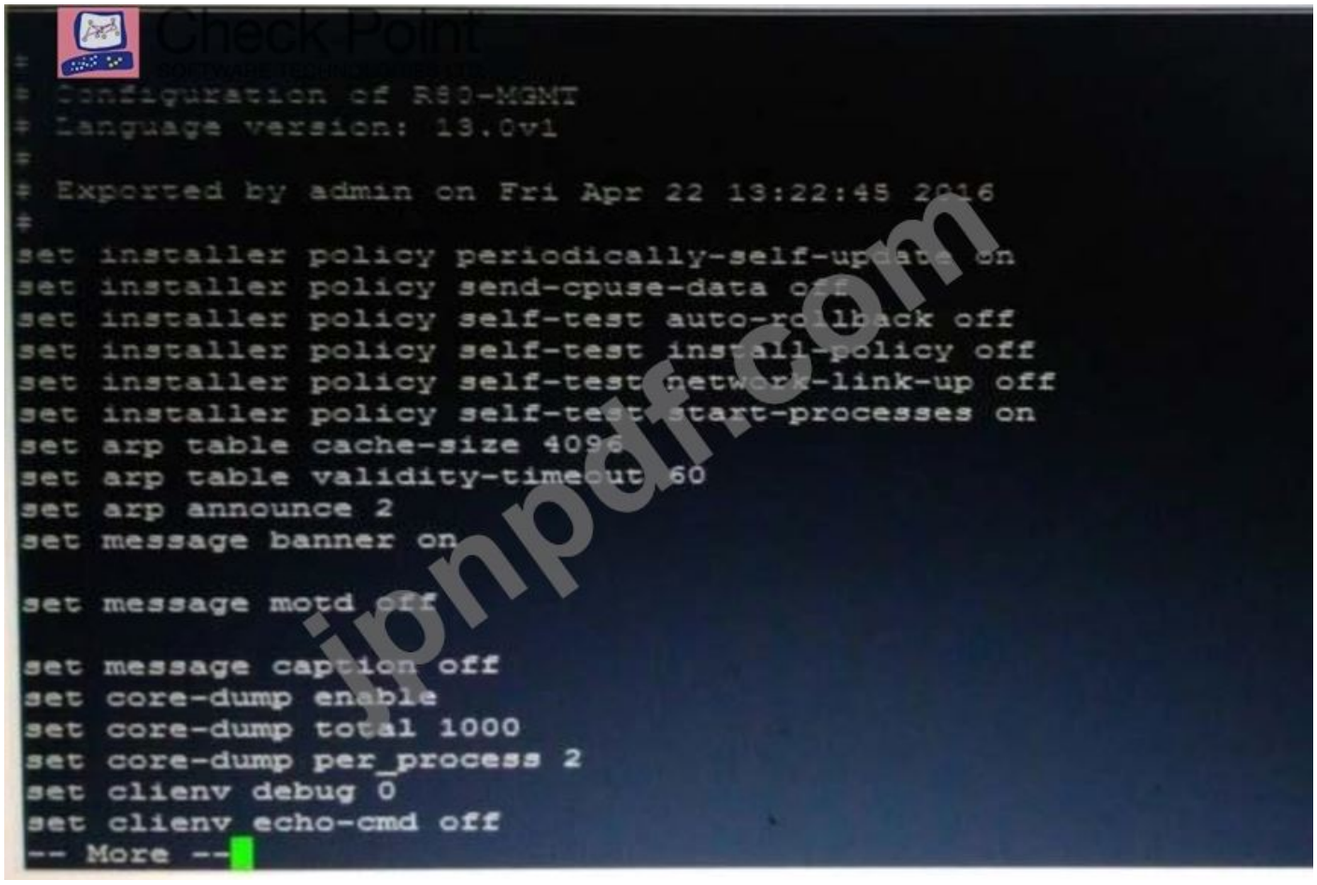
説明

印刷画面の上部には、行われた変更と保存されなかった変更の数を表す番号「8」があります。

セッション管理ツールバー（SmartConsoleの上部）

最新問題: **106**
ネットワークオペレーションセンターの管理者は、主にトラブルシューティングの目的で、チェックポイントセキュリティ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はありませんが、それでも彼女はtcpdumpを実行できるはずです。この要件をどのように達成できますか？
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のアクセスを追加します。
UID 0で新しいユーザーを作成し、そのユーザーに役割を割り当てます。
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、そのユーザーに役割を割り当てます。
C. 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の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、そのユーザーに役割を割り当てます。
D. 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、そのユーザーに役割を割り当てます。
Answer: B (メーッセージを残す**)**

最新問題: **107**
下のスクリーンショットを見てください。どのCLISHコマンドがこの出力を提供しますか？



A. 構成をすべて表示

B. confd構成を表示

C. confdconfigurationallを表示

D. 構成を表示

Answer: D (メーッセージを残す**)**

説明/参照：

Explanation:

To see the latest configuration settings, run:

```
show configuration
```

This example shows part of the configuration settings as last saved to a CLI script:

```
mem103> show configuration
#
# Configuration of mem103
# Language version: 10.0v1
#
# Exported by admin on Mon Mar 19 15:06:22 2012
#
set hostname mem103
set timezone Asia / Jerusalem
set password-controls min-password-length 6
set password-controls complexity 2
set password-controls palindrome-check true
set password-controls history-checking true
set password-controls history-length 10
set password-controls password-expiration never
set ntp active off
set router-id 6.6.6.103
set ipv6-state off
set snmp agent off
set snmp agent-version any
set snmp community public read-only
set snmp traps trap authorizationError disable
set snmp traps trap coldStart disable
set snmp traps trap configurationChange disable
```

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

最新問題**: 108**
どのコマンドを使用して、Gaiaベースのシステムの実行構成を表示できます。
A. 構成を表示
B. showrunning-configuration
C. conf-activeを表示
D. 構成をアクティブに表示
Answer: (解答を表示する**)**

最新問題**: 109**
このセキュリティポリシーを確認する際、ルール4に対応するためにどのような変更を加えることができますか？

No.	Hits	Name	Source	Destination	VPN	Service	Action
		Limit Access to Gateways (Rule 1)					
1	0	Stealth	Corporate-internal-net	GW-group	Any Traffic	Any	drop
		Access Rules (Rules 2-5)					
2	0	Site-to-Site	Any	Any	Any Traffic	CIFS ftp-port http https smtp	accept
3	0	Remote Access	Mobile-vpn-user@Any	Any	RemoteAccess	CIFS http https imap	accept
4	0	Clientless VPN	Clientless-vpn-user@Any	Corporate-WA-proxy-server	Any Traffic	https	User Auth
5	0	Web Server	L2TP-vpn-user@Any Customers@Any	Remote-1-web-server	Any Traffic	http	accept

A. ルール4の[サービス]列からサービスHTTPを削除します。
B. ルール4の[ソース]列または[宛先]列を変更します
C. 何もありません
D. ルール2の列VPNを変更して、特定のトラフィックへのアクセスを制限します。
Answer: (解答を表示する**)**

最新問題**: 110**
チェックポイントライセンスを表示および適用するために使用できるGUIツールはどれですか？
A. cpconfig
B. 管理コマンドライン
C. SmartConsole
D. SmartUpdate
Answer: (解答を表示する**)**
SmartUpdate GUIは、ライセンスを管理するための推奨される方法です。

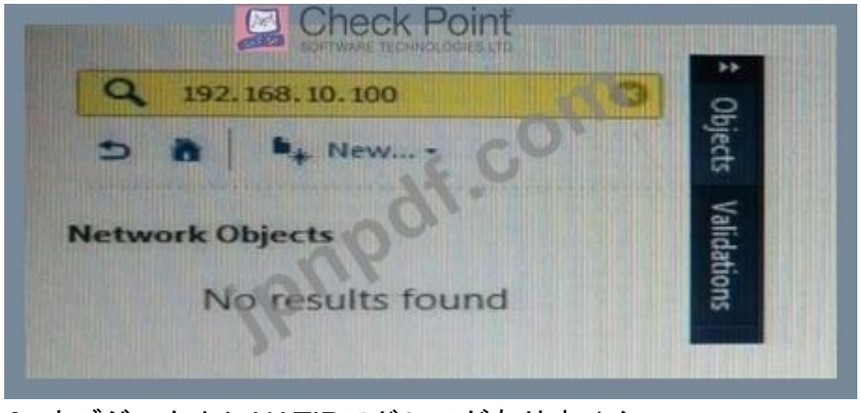
最新問題**: 111**
すべてのCheckPointMobile Accessソリューションで提供されていない機能はどれですか？
A. IPv6のサポート
B. きめ細かいアクセス制御
C. 強力なユーザー認証
D. 安全な接続
Answer: (解答を表示する**)**
ソリューションの種類
チェックポイントのすべてのリモートアクセスソリューションは、以下を提供します。

最新問題**: 112**
空欄に記入してください :セキュリティ管理サーバーによってセキュリティゲートウェイから証明書が取り消されると、証明書情報は_____になります。
A. セキュリティ管理サーバーに保存されます。
B. セキュリティ管理者に送信されます。
C. 証明書失効リストに保存されます。

D. 内部認証局に送信されます。
Answer: C (メーッセージを残す**)**

最新問題**: 113**
空欄に記入してください :_____の場合を除いて、次のすべての状況で新しいライセンスを生成してインストールする必要があります。
A. ライセンスが間違ったセキュリティゲートウェイに接続されています
B. 既存のライセンスの有効期限が切れます
C. ライセンスがアップグレードされます
D. セキュリティ管理またはセキュリティゲートウェイのIPアドレスが変更されました
Answer: (解答を表示する**)**
説明
この状況では、新しいライセンスを生成する必要はありません。間違ったセキュリティゲートウェイからライセンスを切り離して、適切なセキュリティゲートウェイに接続するだけです。

最新問題**: 114**
ボブがオブジェクト検索でこの結果を取得した場合、それはどういう意味ですか？下の画像を参照してください。最良の答えを選択する。



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

最新問題**: 115**
空欄に記入してください。永続的なVPNトンネルは、コミュニティ内のすべてのトンネル、特定のゲートウェイのすべてのトンネル、または_____に設定できます。
A. すべての衛星ゲートウェイから衛星ゲートウェイトンネル
B. 特定のゲートウェイの特定のトンネル
C. コミュニティ内の特定のトンネルについて
D. 特定の衛星ゲートウェイから中央ゲートウェイトンネルへ
Answer: C (メーッセージを残す**)**

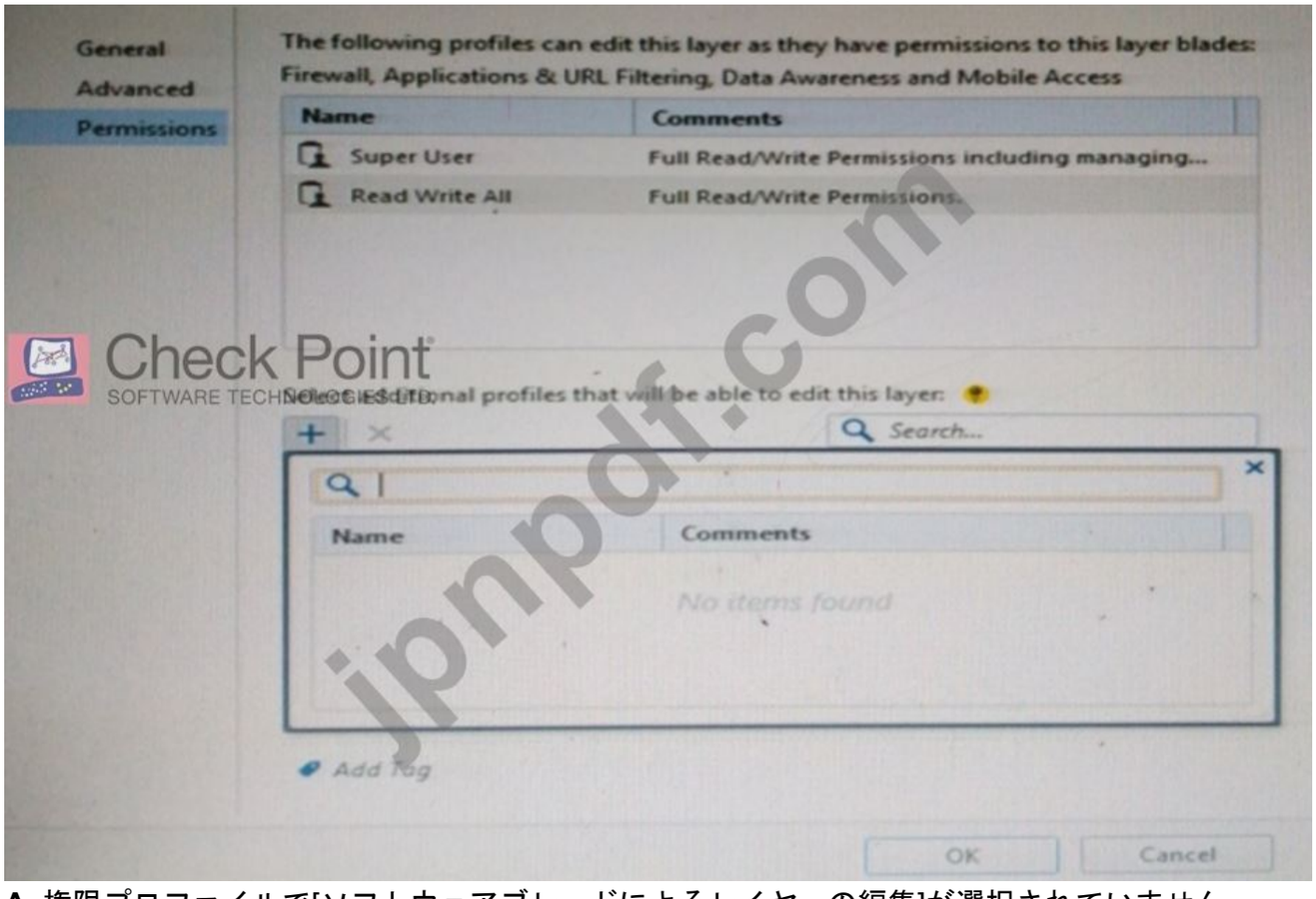
説明/参照：
Explanation:
コミュニティ内の各VPNトンネルは、永続トンネルとして設定できます。パーマネントトンネルは常に監視されているため、VPNトンネルがダウンしている場合は、ログ、アラート、またはユーザー定義のアクションを発行できます。VPNトンネルは、「トンネルテスト」パケットを定期的に送信することによって監視されます。パケットへの応答が受信されている限り、VPNトンネルは「稼働中」と見なされます。所定の時間内に応答が受信されない場合、VPNトンネルは「ダウン」していると見なされます。永続的なトンネルは、Check PointSecurityGateway間でのみ確立できます。パーマネントトンネルの設定は、コミュニティレベルで行われ、次のようになります。
コミュニティ全体に指定できます。このオプションは、コミュニティ内のすべてのVPNトンネルを次のように設定します
▪
永続。
特定のセキュリティゲートウェイに指定できます。このオプションを使用して、特定のセキュリティを構成します
▪
永続的なトンネルを持つゲートウェイ。
単一のVPNトンネルに指定できます。この機能により、間の特定のトンネルを構成できます
▪
永続的な特定のセキュリティゲートウェイ。
参照：
https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/html_frameset.htm？トピック=ドキュメント/R77/ CP_R77_VPN_AdminGuide / 14018

最新問題: **116**
ThreatCloudからのウイルスシグネチャと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CheckPoint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. アンチウイルス
Answer: D (メーッセージを残す**)**
強化されたCheckPointAntivirus Software Bladeは、リアルタイムのウイルスシグネチャと、サイバー犯罪と戦う最初のコラボレーションネットワークであるThreatCloudからの異常ベースの保護を使用して、ユーザーが影響を受ける前にゲートウェイでマルウェアを検出してブロックします。
参照 :https ://www.checkpoint.com/products/antivirus-software-blade/

最新問題: **117**
次のスクリーンショットを見て、最良の答えを選択してください。

A. Security Gatewayの外部のクライアントは、FTPを使用してFTP_Extサーバーに任意のファイルをアップロードできます。
B. 内部クライアントは、FTPを使用してアーカイブファイルをFTP_Extサーバーにアップロードおよびダウンロードできます。
C. Security Gatewayの外部のクライアントは、FTPを使用してFTP_Extサーバーからアーカイブファイルをダウンロードできます。
D. 内部クライアントは、FTPを使用して任意のファイルをFTP_Ext-serverにアップロードおよびダウンロードできます。
Answer: (解答を表示する**)**

最新問題**: 118**
レイヤーを編集するための選択した管理者の権限を定義する必要があります。ただし、「このレイヤーを編集できる追加のプロファイルを選択してください」の+記号をクリックしても、何も表示されません。この問題の最も可能性の高い原因は何ですか？最良の答えを選択してください。



A. 権限プロファイルで[ソフトウェアブレードによるレイヤーの編集]が選択されていません
B. 「レイヤーエディターで選択したプロファイルでレイヤーを編集する」は、権限プロファイルで選択されていません。
C. 使用可能な権限プロファイルがないため、最初に作成する必要があります。
D. すべての権限プロファイルが使用されています。
Answer: (解答を表示する**)**

最新問題: **119**
空欄に記入してください :R80より前のゲートウェイのIPSポリシーは、_____の間にインストールされます。
A. ファイアウォールポリシーのインストール
B. 脅威防止ポリシーのインストール
C. ボット対策ポリシーのインストール
D. アクセス制御ポリシーのインストール
Answer: B (メーッセージを残す**)**
https://sc1.checkpoint.com/documents/R80/CP_R80BC_ThreatPrevention/html_frameset.h tm？topic = document / R80 / CP_R80BC_ThreatPrevention / 136486

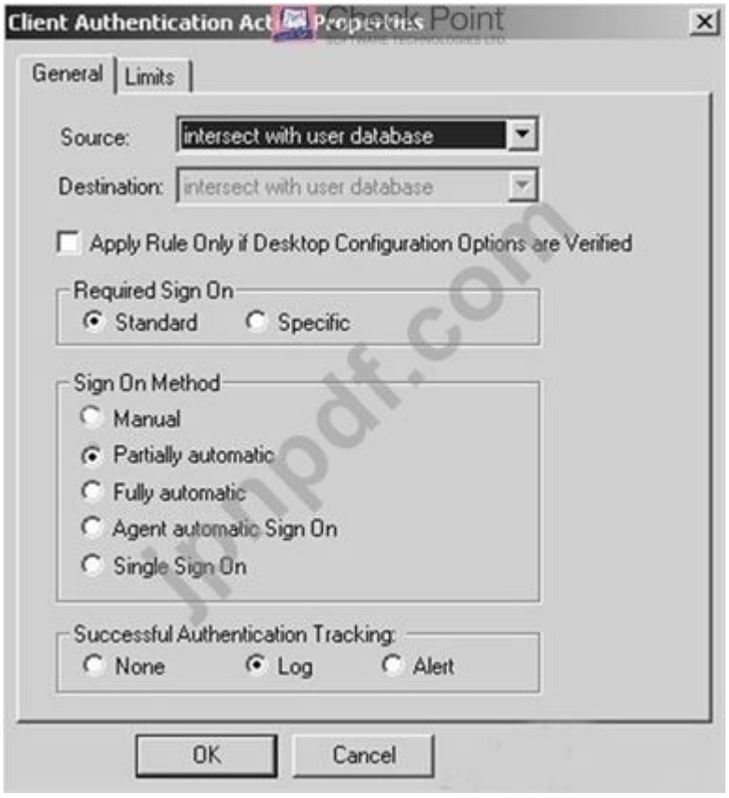
最新問題: **120**
R80では、統合ポリシーは
A. アクセス制御ポリシー、QoSポリシー、デスクトップセキュリティポリシー、およびエンドポイントポリシー。
B. アクセス制御ポリシー、QoSポリシー、デスクトップセキュリティポリシー、および脅威防止ポリシー。
C. ファイアウォールポリシー、アドレス変換とアプリケーションおよびURLフィルタリング、QoSポリシー、デスクトップセキュリティポリシー、および脅威防止ポリシー。
D. アクセス制御ポリシー、QoSポリシー、デスクトップセキュリティポリシー、VPNポリシー。
Answer: D (メーッセージを残す**)**
説明
選択肢を考えると、Dが最良の答えです。
統一されたポリシー
R80では、アクセス制御ポリシーは、これらのR80より前のソフトウェアブレードのポリシーを統合します。
*ファイアウォールとVPN
*アプリケーション制御とURLフィルタリング
*アイデンティティの認識
*データ認識
*モバイルアクセス
*セキュリティゾーン

最新問題: **121**
IKEによって実行される2フェーズネゴシエーションプロセスのフェーズ1は、_____モードで動作します。
A. メイン
B. 認証
C. クイック
D. 高アラート
Answer: A (メーッセージを残す**)**
説明
フェーズIモード
セキュリティゲートウェイの間には、IKEフェーズIの2つのモードがあります。

これらのモードはIKEv1にのみ適用されます。
*メインモード
*アグレッシブモード

最新問題: **122**
空欄に記入してください :LDAPがCheck Point Security Managementと統合されている場合、それは_____と呼ばれます。
A. UserCheck
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**)**
チェックポイントユーザーディレクトリは、LDAPおよびその他の外部ユーザー管理テクノロジーをチェックポイントソリューションと統合します。ユーザー数が多い場合は、セキュリティを強化するために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。
管理サーバーのパフォーマンス。

最新問題: **123**
ルールベースとクライアント認証アクションのプロパティ画面を確認します。



セキュリティゲートウェイによって認証された後、ユーザーはWebサイトへのHTTP接続を開始します。ユーザーがコマンドラインを使用して別のサイトにFTPで転送しようとするとどうなりますか？：

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

B. FTP接続はルール2によってドロップされます。

C. ユーザーが正常に認証された後、FTPデータ接続が切断されます。

D. ユーザーはセキュリティゲートウェイによる認証を再度求められます。

Answer: A (メーッセージを残す**)**

最新問題**: 124**

R80より前のゲートウェイのIPSポリシーは、_____の間にインストールされます。

A. ファイアウォールポリシーのインストール

B. 脅威防止ポリシーのインストール

C. ボット対策ポリシーのインストール

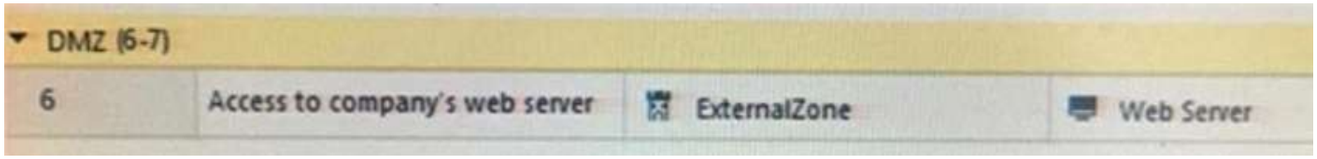
D. アクセス制御ポリシーのインストール

Answer: (解答を表示する**)**

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

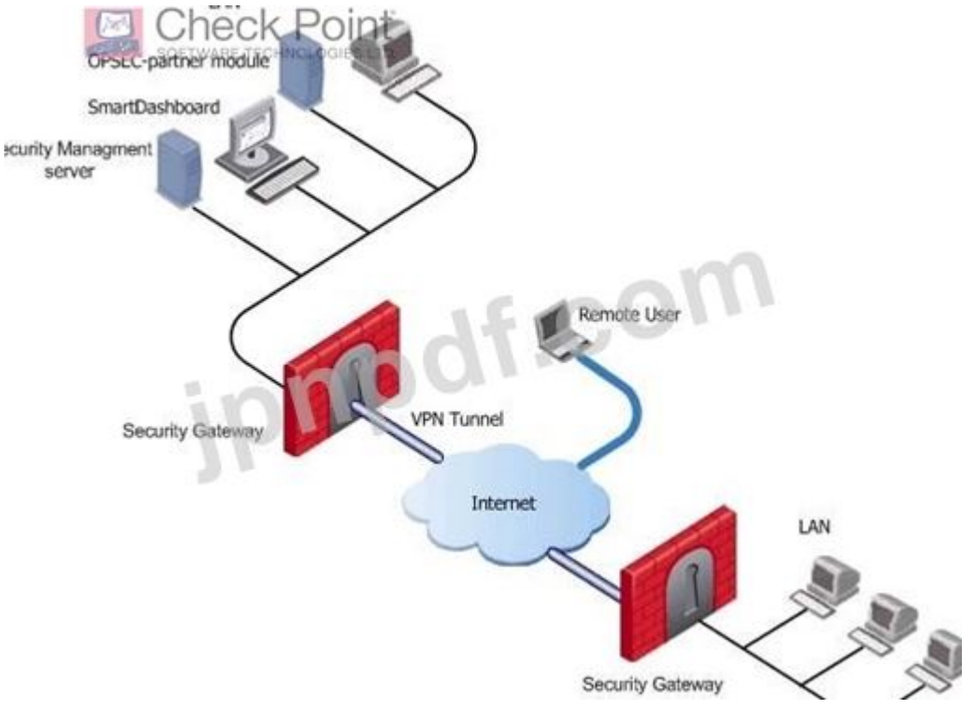
最新問題**: 125**

提示されたルールでExternalZoneは何を表していますか？



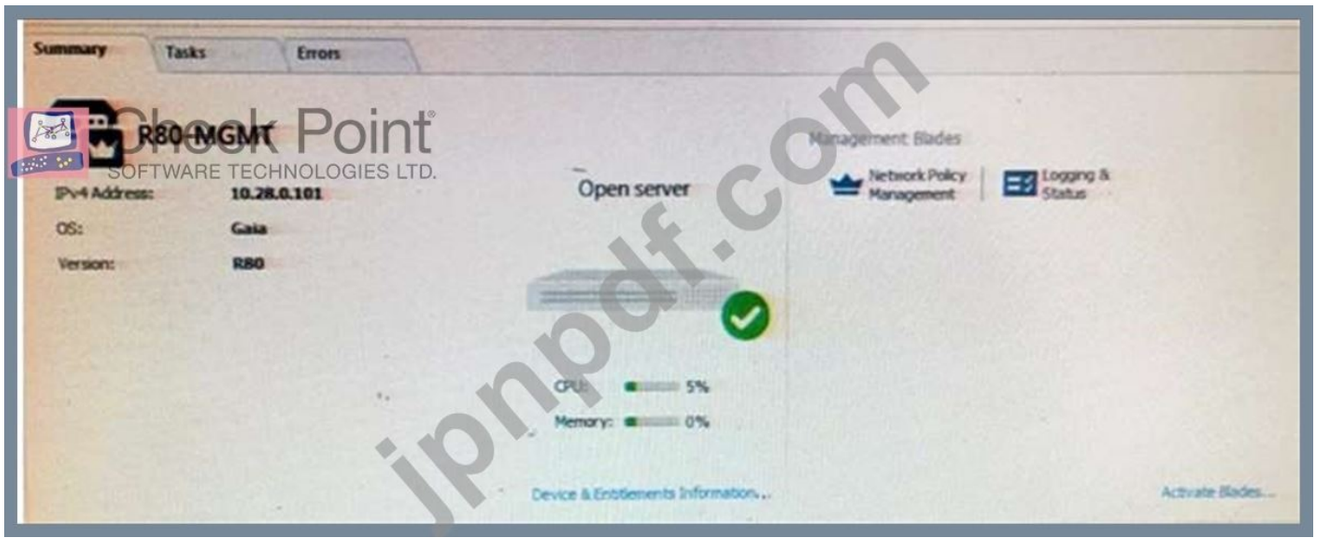
A. インターネット。
B. 管理者が外部セキュリティゾーンの一部として定義したインターフェイス。
C. すべてのセキュリティゲートウェイの外部インターフェイス。
D. 特定のゲートウェイの外部インターフェース。
Answer: (解答を表示する**)**
インターフェイスの構成
[セキュリティゲートウェイ]ウィンドウの[インターフェイス]タブで、セキュリティゲートウェイ80のインターフェイスを設定します。
インターフェイスを設定するには：
[セキュリティゲートウェイ]ウィンドウが開きます。
編集ウィンドウが開きます。

最新問題**: 126**
チェック ポイントのセキュリティ管理アーキテクチャの3つの重要なコンポーネントは何ですか？
A. SmartConsole、セキュリティ管理サーバー、セキュリティゲートウェイ
B. SmartConsole、SmartUpdate、Security Gateway
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、コマンドラインインターフェイス
D. WebUI、SmartConsole、セキュリティゲートウェイ
Answer: (解答を表示する**)**
説明/参照：
Explanation:展開
基本的な展開：
スタンドアロン展開セキュリティゲートウェイとセキュリティ管理サーバーがにインストールされている
▪
同じマシン。
分散展開セキュリティゲートウェイとセキュリティ管理サーバーがインストールされている
▪
別のマシン。



異なるサイトにゲートウェイがある環境を想定します。各セキュリティゲートウェイは、一方がインターネットに接続し、もう一方がLANに接続します。
2つのセキュリティゲートウェイ間に仮想プライベートネットワーク（VPN）を作成して、それらの間のすべての通信を保護できます。
セキュリティ管理サーバーはLANにインストールされ、セキュリティゲートウェイによって保護されています。セキュリティ管理サーバーはセキュリティゲートウェイを管理し、リモートユーザーが企業ネットワークに安全に接続できるようにします。SmartDashboardは、セキュリティ管理サーバーまたは別のコンピューターにインストールできます。
セキュリティ管理サーバーとそのセキュリティゲートウェイを使用してネットワークセキュリティを完了するために、他のOPSECパートナーモジュール（たとえば、アンチウイルスサーバー）が存在する場合があります。
参照：https://sc1.checkpoint.com/documents/R77/CP_R77_SecurityManagement_WebAdminGuide/html_frameset.htm？topic = document / R77 / CP_R77_SecurityManagement_WebAdminGuide / 118037

最新問題: **127**
Tinaは、新しいCheckPointR80管理コンソールインターフェイスを現在確認している新しい管理者です。[ゲートウェイ]ビューで、彼女は下のスクリーンショットのように[概要]画面を確認しています。 「オープンサーバー」とは何ですか？



A. CheckPoint以外のアプライアンスにデプロイされたCheckPointソフトウェア。
B. セキュリティと可用性の目的で使用されるOpenServerConsortium承認のサーバーハードウェア。
C. Open Systems Interconnection（OSI）サーバーとセキュリティ展開モデルを使用して展開されたCheck PointManagementServer。
D. OpenSSLを使用するCheckPointManagementServerソフトウェア。
Answer: (解答を表示する**)**

Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).

最新問題**: 128**
VMACモードが有効になっていることを確認するには、すべてのクラスターメンバーでどのCLIコマンドを実行する必要がありますか？
A. fw ctl get int fwha vmac global param enabled; コマンドの結果は値1を返す必要があります
B. fw ctl get int fwha_vmac_global_param_enabled; コマンドの結果は値1を返す必要があります
C. cphaprob -a if
D. fw ctl set int fwha vmac global param enabled
Answer: (解答を表示する**)**

最新問題**: 129**
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が同じアプライアンスにインストールされているのはどの展開ですか。
A. ブリッジモード
B. リモート
C. スタンドアロン
D. 分散
Answer: C (メーッセージを残す**)**
StandaloneStandaloneデプロイメントのインストールセキュリティ管理サーバーと

Security Gatewayは、同じコンピューターまたはアプライアンスにインストールされます。

最新問題: **130**
Identity Awarenessの認証方法としてLDAPを使用する場合、次のクエリを実行します。
A. 透過的であり、クライアントまたはサーバー側のソフトウェアやクライアントの介入を必要としません。
B. ユーザーに資格情報の入力を求めます。
C. 管理者は、LDAPサーバーおよびセキュリティゲートウェイとの間のLDAPトラフィックを明確に許可する必要があります。
D. クライアント側とサーバー側のソフトウェアが必要です。
Answer: A (メーッセージを残す**)**

最新問題: **131**
アプリケーションのスキャンと検出を可能にするチェックポイント機能はどれですか？
A. アプリケーション辞書
B. AppWiki
C. アプリケーションライブラリ
D. CPApp
Answer: B (メーッセージを残す**)**
AppWikiアプリケーション分類ライブラリ
AppWikiを使用すると、5,000を超える個別のアプリケーションのアプリケーションスキャンと検出が可能になります。
インスタントメッセージング、ソーシャルネットワーキング、ビデオストリーミング、VoIP、ゲームなどを含む300,000のWeb2.0ウィジェット。

最新問題: **132**
LDAPユーザーディレクトリ統合を構成する場合、ユーザーディレクトリテンプレートに適用される変更は次のとおりです。
A. テンプレートを使用しているすべてのユーザーにすぐに反映されます。
B. ローカルユーザーテンプレートが変更されない限り、どのユーザーにも反映されません。
C. そのテンプレートを使用しているすべてのユーザー、およびローカルユーザーテンプレートも変更された場合に反映されます。
D. そのテンプレートを使用しているユーザーには反映されません。
Answer: A (メーッセージを残す**)**

説明
ユーザーとユーザーグループは、LDAPサーバーのツリー構造のアカウントユニットに配置されます。ユーザーディレクトリのユーザー管理は、ローカルではなく外部です。ユーザーディレクトリテンプレートを変更できます。このテンプレートに関連付けられているユーザーは、変更をすぐに取得します。SmartDashboardでユーザー定義を手動で変更でき、変更はサーバー上で即座に行われます。

最新問題: **133**
Check Point Security Gatewayを使用せずに、電子メールトラフィックとインラインモード専用にTE250X Check Pointアプライアンスをどのように展開しますか？
A. MTAモードのLANスイッチのSpanPortにアプライアンスTE250Xをインストールします
B. アプライアンスTE250Xをスタンドアロンモードでインストールし、MTAをセットアップします
C. このシナリオではチェックポイントクラウドサービスのみを利用できます
D. 不可能です。SandBlastアプライアンスにメールを転送するには、常にCheckPointSGWが必要です。
Answer: (解答を表示する**)**
説明
説明/参照 :http ://dl3.checkpoint.com/paid/f2/f2faf02dba06acad8cc4c57833593df6/CP_TE100X_TE250X_Appliance_GettingStartedGuide.pdf？HashKey = 1517091196_a292abdde351bbdb4b3d28e82654b240 &xtn = .pdf

最新問題: **134**
次のブレードのうち、サブスクリプションベースではないため、更新する必要がないブレードはどれですか。定期的に？
A. 高度なネットワークブレード
B. アンチウイルス
C. 脅威エミュレーション
D. アプリケーション制御
Answer: (解答を表示する**)**

最新問題: **135**
R80管理にデフォルトで含まれていない脅威防止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-最近の攻撃または人気のある攻撃に対して、一般的なネットワーク製品とプロトコルに優れた保護を提供します
C. 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
D. 厳密-ネットワークパフォーマンスに影響を与える、すべての製品とプロトコルに幅広いカバレッジを提供します
Answer: C (メーッセージを残す**)**

最新問題: **136**

あなたはABCCorpの管理者です。R80管理サーバーにログインしました。ルールベースにいくつかの変更を加えていますが、ルールNo.6の横に鉛筆アイコンがあることに注意してください。

これは何を意味するのでしょうか？

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

B. ルールNo.6は、管理セッションで削除対象としてマークされています。

C. ルールNo.6は、管理セッションで編集するためにマークされています。

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

Answer: C (メーッセージを残す**)**

最新問題: **137**

次のテクノロジーのうち、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格納するのはどれですか？

A. アプリケーション層ファイアウォール

B. INSPECTエンジン

C. ステートフルインスペクション

D. パケットフィルタリング

Answer: C (メーッセージを残す**)**

最新問題: **138**

CPDデーモンはファイアウォールカーネルプロセスであり、次のうちどれを実行しませんか？

A. セキュア内部通信 $IC）

B. デーモンが失敗した場合は再起動します

C. ファイアウォールプロセス間でメッセージを転送する

D. アプリケーションの監視ステータスを取得します

Answer: D (メーッセージを残す**)**

説明/参照 :https ://supportcenter.checkpoint.com/supportcenter/portal？eventSubmit_doGoviewsolutiondetails =&solutionid = sk97638

最新問題: **139**
ロギングとモニタリングでは、トラッキングオプションはログ、詳細ログ、拡張ログです。次のオプションのうち、各ログ、詳細ログ、拡張ログに追加できるのはどれですか？
A. 会計
B. 抑制
C. 会計/抑制
D. アカウンティング/拡張
Answer: C (メーッセージを残す**)**
説明/参照：
参照：https ://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/ html_frameset.htm？topic = document / R80 / CP_R80_LoggingAndMonitoring / 131914

最新問題: **140**
次のコマンドのうち、クラスターメンバーを監視するために使用されるのはどれですか？
A. クラスターの状態
B. cphaprob
C. cphaprobステータス
D. cphaprob stat
Answer: D (メーッセージを残す**)**

最新問題: **141**
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したときに開始します。
B. 管理者がSmartConsoleを介してセキュリティ管理サーバーにログインしたときに開始し、公開されたときに終了します。
C. ポリシーがセキュリティゲートウェイにプッシュされると、セッションは終了します。
D. Sessions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セキュリティ管理サーバーに接続できます。すべての管理者は独自のユーザー名を持ち、他の管理者から独立したセッションで作業します。
管理者がSmartConsoleを介してセキュリティ管理サーバーにログインすると、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、その管理者のみが利用できます。他の管理者には、編集中のオブジェクトとルールに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。
参照：https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 117948

最新問題: **142**

SICの3つの認証方法は何ですか？
A. セキュリティチャネルを作成するためのパスワード、ユーザー、および標準ベースのSSL
B. 証明書、セキュリティで保護されたチャネルを作成するための標準ベースのSSL、および3DESまたはAES128
暗号化
C. パケットフィルタリング、証明書、および暗号化用の3DESまたはAES128
D. 証明書、パスワード、およびトークン
Answer: (解答を表示する**)**
説明
安全な内部通信 $IC）
Secure Internal Communication $IC）を使用すると、CheckPointプラットフォームと製品を相互に認証できます。
SICプロシージャは、ゲートウェイ、管理サーバー、およびその他のチェックポイント間に信頼できるステータスを作成します
コンポーネント。SICは、ゲートウェイにポリシーをインストールし、ゲートウェイ間でログを送信する必要があります。
管理サーバー。
これらのセキュリティ対策により、SICの安全性が確保されます。

最新問題**: 143**
空欄に記入してください。RADIUSプロトコルは_____を使用してゲートウェイと通信します。
A. UDP
B. TDP
C. CCP
D. HTTP
Answer: (解答を表示する**)**
パラメーター：

Parameter	Description
port	UDP port on the RADIUS server. This value must match the port as configured on the RADIUS server. Typically this 1812 (default) or 1645 (non-standard but a commonly used alternative).

最新問題**: 144**
問題のあるホストからの疑わしい接続を見つけました。問題のあるホストだけでなく、ネットワーク全体からすべてをブロックすることにしました。さらに調査している間、これを1時間ブロックしたいが、ルールベースにルールを追加したくない。これをどのように達成しますか？
A. dbedittoスクリプトを使用して、ルールをRuleBases_5_0.fwsconfigurationファイルに直接追加します。
B. SmartViewTrackerの[ツール]メニューから[侵入者のブロック]を選択します。
C. SmartMonitorで疑わしいアクティビティルールを作成します。

D. SmartDashboardを使用して一時的なルールを追加し、[ルールを非表示]を選択します。
Answer: (解答を表示する**)**
説明/参照：

最新問題**: 145**
次の自動生成ルールNATルールのうち、実装の優先度が最も低いのはどれですか？
A. マシン非表示NAT
B. アドレス範囲非表示NAT
C. ネットワーク非表示NAT
D. マシン静的NAT
Answer: B,C (メーッセージを残す**)**
SmartDashboardは、自動NATルールを次の順序で編成します。
1.ファイアウォールまたはノード ロンピューターまたはサーバー)オブジェクトの静的NATルール
2.ファイアウォールまたはノードオブジェクトのNATルールを非表示にする
3.ネットワークまたはアドレス範囲オブジェクトの静的NATルール
4.ネットワークまたはアドレス範囲オブジェクトのNATルールを非表示にします
参照：
https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/6724.htm

最新問題**: 146**
Webコントロールレイヤーは、次のダイアログの設定を使用してセットアップされています。

次のポリシーを検討し、最良の回答を選択してください。

A. サブポリシーのどのルールにも一致しないトラフィックはドロップされます。
B. すべての従業員はYoutubeとVimeoにのみアクセスできます。
C. YoutubeとVimeoへのアクセスは1日1回のみ許可されています。
D. 内部ネットワークの誰でもインターネットにアクセスでき、ドロップルール5.2、5.5、および5.6で定義されたトラフィックを期待できます。
Answer: D (メーッセージを残す)
説明
ポリシーレイヤーとサブポリシー
R80は、レイヤーとサブポリシーの概念を導入し、ネットワークセグメントまたはビジネスユニット/機能に従ってポリシーをセグメント化できるようにします。さらに、レイヤーまたはサブポリシーごとにきめ細かい特権を割り当てて、ワークロードとタスクを最も資格のある管理者に分散することもできます。
*レイヤーを使用すると、ルールベースは一連のセキュリティルールに編成されます。これらのルールまたはレイヤーのセットは、定義された順序で検査されるため、ルールベースフローと優先されるセキュリティ機能を制御できます。レイヤー全体で 承認」アクションが実行された場合、検査は次のレイヤーに進みます。たとえば、コンプライアンスレイヤーを作成して、ルールの断面全体にオーバーレイすることができます。
*サブポリシーは、特定のネットワークセグメント、ブランチオフィス、またはビジネスユニット用に作成された一連のルールであるため、ルールが一致した場合、検査はこのルールのサブセットを通過してから次に進みます。
*次のルール。
*サブポリシーとレイヤーは、権限プロファイルに従って、特定の管理者が管理できます。これにより、タスクの委任とワークロードの分散が容易になります。

最新問題: **147**
あなたはABCCorp.の上級ファイアウォール管理者であり、最近、CheckPointの新しい高度なR80管理プラットフォームのトレーニングコースから戻ってきました。チェックポイントR80管理の新機能の社内概要をABCCorpの他の管理者に提示しています。

R80管理コンソールの新しい[公開]ボタンをどのように説明しますか？

A. [公開]ボタンは、管理者が管理セッションで行った変更をすべて取得し、コピーをR80のチェックポイントに公開してから、R80データベースに保存します。
B. [公開]ボタンは、管理者が管理セッションで行った変更をすべて取得し、コピーをR80のチェックポイントクラウドに公開しますが、R80には保存しません。
C. [公開]ボタンを使用すると、管理者が管理セッションで行った変更が他のすべての管理者セッションに表示され、データベースに保存されます。
D. [公開]ボタンを使用すると、管理者が管理セッションで行った変更が新しいユニファイドポリシーセッションに表示され、データベースに保存されます。
Answer: C (メーッセージを残す**)**
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、セッションを公開する必要があります。セッションを公開すると、新しいデータベースバージョンが作成されます。
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？
トピック=ドキュメント/R80/ CP_R80_SecMGMT / 126197

最新問題**: 148**
SmartView Trackerを使用しているときに、Bradyは、侵入の可能性があると考えてい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分間トラフィックをブロックすることにしましたが、すべてのステップを思い出せません。ブロックを設定するために必要な手順の正しい順序は何ですか？
1）SmartViewTrackerで[アクティブモード]タブを選択します。
2）[ツール]>[侵入者のブロック]を選択します。
3）SmartViewTracker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）ブロックする必要のある接続を強調表示します。
A. 3、5、2、4
B. 1、2、5、4
C. 3、2、5、4
D. 1、5、2、4
Answer: (解答を表示する**)**

最新問題**: 149**
IT管理チームは、チェックポイントR80.x管理の新機能に関心があり、アップグレードしたいと考えていますが、既存のR77.30 Gaiaゲートウェイは非常に異なるため、R80.xで管理できないことを懸念しています。ファイアウォールを担当する管理者として、これらの懸念にどのように答えたり確認したりできますか？
A. R80.x Managementには、R80より前のバージョンのCheckPointGatewayを管理するための互換性パッケージが含まれています。詳細については、R80リリースノートを参照してください。
B. R80.x管理では、R80より前のバージョンのCheck Point Gatewayを管理するために、互換性修正プログラムパッケージを個別にインストールする必要があります。詳細については、R80リリースノートを参照してください。
C. R80.x管理は、完全に異なる管理システムとして設計されているため、R80より前のチェックポイントゲート

ウェイのみを監視できます。
D. R80.x Managementは、R80より前のバージョンのCheckPointGatewayを管理できません。R80以降のゲートウェイのみを管理できます。詳細については、R80リリースノートを参照してください。
Answer: A (メーッセージを残す)
説明

最新問題: **150**
ローミングユーザーにIdentityAwarenessを展開するための最良の方法は何ですか？
A. オフィスモードを使用する
B. ID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を共有する
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
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: **151**
Johnは、rR77.30チェックポイントセキュリティを管理するR80セキュリティ管理サーバーの管理者です。ゲートウェイ。Johnは現在、ネットワークオブジェクトを更新し、SmartConsoleを使用してルールを修正しています。作る
他の管理者が利用できるJohnの変更、および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、何をする必要がありますか
ジョンは？
A. セッションのログアウト
B. ファイル>保存
C. データベースをインストールします
D. セッションを公開する
Answer: D (メーッセージを残す)
説明

インストールと公開
公開とインストールの違いを理解することが重要です。
これを行う必要があります：
あなたがこれをした後：
公開
SmartConsoleでセッションを開き、変更を加えました。
公開操作は、SmartConsoleのすべての変更を他の管理者に送信し、変更を加えます
プライベートセッションで公開しました。
データベースをインストールします
サーバー、ユーザー、サービス、IPSプロファイルなどの変更されたネットワークオブジェクト。ただし、ルールベースは変更されません。
更新は、管理サーバーとログサーバーにインストールされます。
ポリシーをインストールする
ルールベースを変更しました。
Security Management Serverは、更新されたポリシーとデータベース全体をSecurityGatewayにインストールします
（ネットワークオブジェクトを変更しなかった場合でも）。

最新問題: **152**
キャプティブポータルツール：
A. グローバルプロパティ設定の[ID認識]ページから展開されます。
B. すでに識別されているユーザーへのアクセスを許可します。
C. ゲストユーザー認証にのみ使用されます。
D. 身元不明のユーザーからIDを取得します。
Answer: D (メーッセージを残す)

最新問題: **153**
証明書がSecurityManagementServerによってSecurityGateWayから取り消されると、証明書情報は_____になります。
A. セキュリティ管理サーバーに保存されます。
B. セキュリティ管理者に送信されます。
C. 証明書失効リストに保存されます。
D. 内部認証局に送信されます。
Answer: C (メーッセージを残す)

最新問題: **154**
R80.10では、LEA（Log Export API）を使用してログを読み取るようにサードパーティの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. 18184
C. 257
D. 18191
Answer: (解答を表示する**)**
説明
参照：

最新問題: **155**
ステートフルインスペクションの利点ではないものは何ですか？
A. 優れたセキュリティ
B. 高性能
C. ネットワーク層の上にスクリーニングなし
D. 透明性
Answer: B (メーッセージを残す**)**

最新問題: **156**
Check Pointアプライアンスに最初にインストールした後、管理インターフェースとデフォルトゲートウェイが正しくないことに気づきました。IPを192.168.80.200/24に設定し、デフォルトゲートウェイを192.168.80.1に設定するために使用できるコマンドはどれですか。
A. set interface Mgmt ipv4-address 192.168.80.200 mask-length 24
静的ルートのデフォルトのネクストホップゲートウェイアドレス192.168.80.1をオンに設定します
設定を保存
B. インターフェースMgmt ipv4-address192.168.80.200255.255.255.0を追加します
static-route 0.0.0.0.0.0.0.0gw192.168.80.1を追加します
設定を保存
C. set interface Mgmt ipv4-address 192.168.80.200 255.255.255.0
static-route 0.0.0.0.0.0.0.0gw192.168.80.1を追加します
設定を保存
D. インターフェイス管理を追加ipv4-address 192.168.80.200 mask-length 24
静的ルートのデフォルトのネクストホップゲートウェイアドレス192.168.80.1を追加します
設定を保存
Answer: (解答を表示する**)**
説明

最新問題: **157**
セキュリティゲートウェイがActiveDirectoryユーザーとコンピューター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？

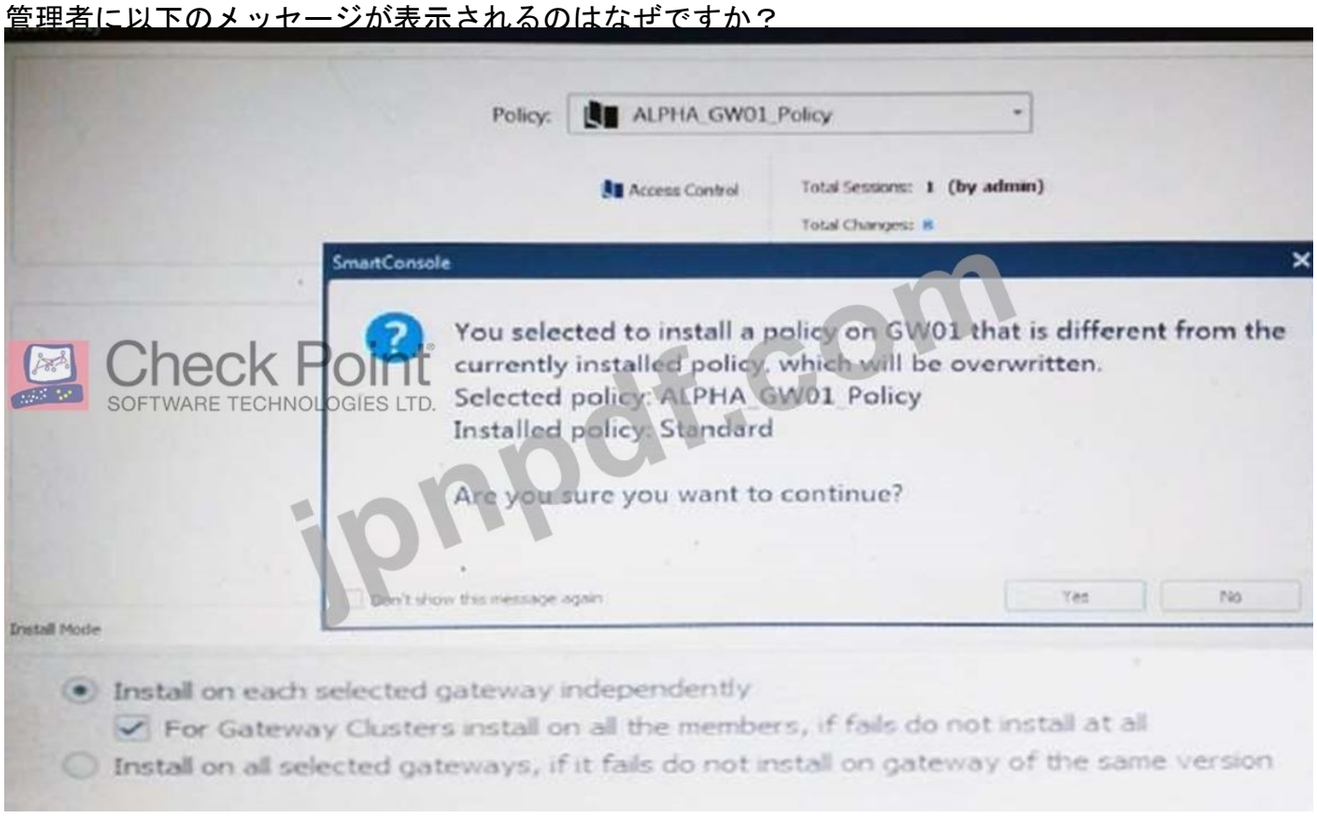
A. UserCheck
B. ActiveDirectoryクエリ
C. アカウントユニットクエリ
D. ユーザーディレクトリクエリ
Answer: B (メーッセージを残す**)**
説明
ADクエリは、ActiveDirectoryセキュリティイベントログからユーザーとコンピューターのID情報を抽出します。
ユーザーまたはコンピューターがネットワークリソースにアクセスすると、システムはセキュリティイベントログエントリを生成します。
たとえば、これは、ユーザーがログインしたとき、画面のロックを解除したとき、またはネットワークドライブにアクセスしたときに発生します。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_IdentityAwareness_AdminGuide/62402.htm

最新問題**: 158**
SmartView Trackerで使用できる3つのタブは何ですか？
A. ネットワークとエンドポイント、管理、アクティブ
B. ネットワーク、エンドポイント、アクティブ
C. 事前定義、すべてのレコード、カスタムクエリ
D. エンドポイント、アクティブ、およびカスタムクエリ
Answer: C (メーッセージを残す**)**
説明/参照：

最新問題**: 159**
次のうち、推奨されるライセンスモデルはどれですか？ベストアンサーを選択してください。
A. パッケージライセンスをゲートウェイのIPアドレスに関連付け、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。
B. パッケージライセンスをセキュリティ管理サーバーのIPアドレスに関連付け、ゲートウェイの依存関係がないため、中央ライセンス。
C. ローカルライセンス。パッケージライセンスをゲートウェイ管理インターフェイスのMACアドレスに関連付け、セキュリティ管理サーバーに依存しないためです。
D. パッケージライセンスをセキュリティ管理サーバー管理インターフェイスのMACアドレスに関連付け、ゲートウェイの依存関係がないため、中央ライセンス。
Answer: B (メーッセージを残す**)**
セントラルライセンス
セントラルライセンスは、ゲートウェイIPアドレスではなく、セキュリティ管理サーバーのIPアドレスに付加されるライセンスです。セントラルライセンスの利点は次のとおりです。
*すべてのライセンスに必要なIPアドレスは1つだけです。
*ライセンスは、あるゲートウェイから取得して別のゲートウェイに付与できます。
*ゲートウェイのIPアドレスを変更しても、新しいライセンスは引き続き有効です。新しいライセンスを作成し

てインストールする必要はありません。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_Installation_and_Upgrade_Guide- webAdmin / 13128.htm#o13527

最新問題: **160**
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クする必要があります。
B. 管理で作成された新しいポリシーパッケージが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、ゲートウェイの定期的なバックアップから復元できます。
D. ゲートウェイで作成された新しいポリシーパッケージが既存の管理にインストールされます。
Answer: B (メーッセージを残す)

最新問題: **161**
パケットフィルタリングの利点ではないものは何ですか？
A. セキュリティが低く、ネットワーク層の上にスクリーニングがない
B. アプリケーションの独立性
C. 高性能
D. スケーラビリティ
Answer: A (メーッセージを残す)
説明/参照：
Explanation:パケットフィルターの長所と短所

Advantages	Disadvantages
Application independence	Low security
High performance	No screening above the network layer
Scalability	

参照 :https ://www.checkpoint.com/smb/help/utm1/8.2/7078.htm

最新問題: **162**
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。両方のオフィスは、同じセキュリティ管理サーバーによって管理されるCheck PointSecurityGatewayによって保護されています。事前共有シークレットを指定するようにVPNコミュニティを構成しているときに、管理者は事前共有シークレットを有効にするチェックボックスが共有されており、有効にできないことに気付きました。なぜ彼は事前共有秘密を指定できないのですか？
A. 証明書ベースの認証は、2つの間で使用できる唯一の認証方法です
同じSMSによって管理されるセキュリティゲートウェイ。
B. 事前共有は、サードパーティベンダーと
チェック -ポイント -セキュリティ -ゲートウェイ。
C. 両方のセキュリティゲートウェイでIPsecVPNブレードを有効にする必要があります。
D. セキュリティゲートウェイはR75.40より前のものです。
Answer: A (メーッセージを残す**)**

最新問題: **163**
空欄に記入してください :ユーザーディレクトリソフトウェアブレードを使用すると、a &n）でR80ユーザー定義を作成できます。
_____サーバー。
A. NTドメイン
B. SMTP
C. LDAP
D. SecurID
Answer: (解答を表示する**)**
説明/参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？トピック=ドキュメント/R80/ CP_R80_SecMGMT / 126197

最新問題: **164**
IT管理チームは、チェックポイントR80管理の新機能に関心があり、アップグレードしたいと考えていますが、既存のR77.30 Gaiaゲートウェイは非常に異なるため、R80で管理できないことを懸念しています。ファイアウォールを担当する管理者として、これらの懸念にどのように答えたり確認したりできますか？
A. R80 Managementには、R80より前のバージョンのCheckPointGatewayを管理するための互換性パッケージが含まれています。詳細については、R80リリースノートを参照してください。
B. R80管理では、R80より前のバージョンのCheck Point Gatewayを管理するために、互換性修正プログラム

パッケージを個別にインストールする必要があります。詳細については、R80リリースノートを参照してください。

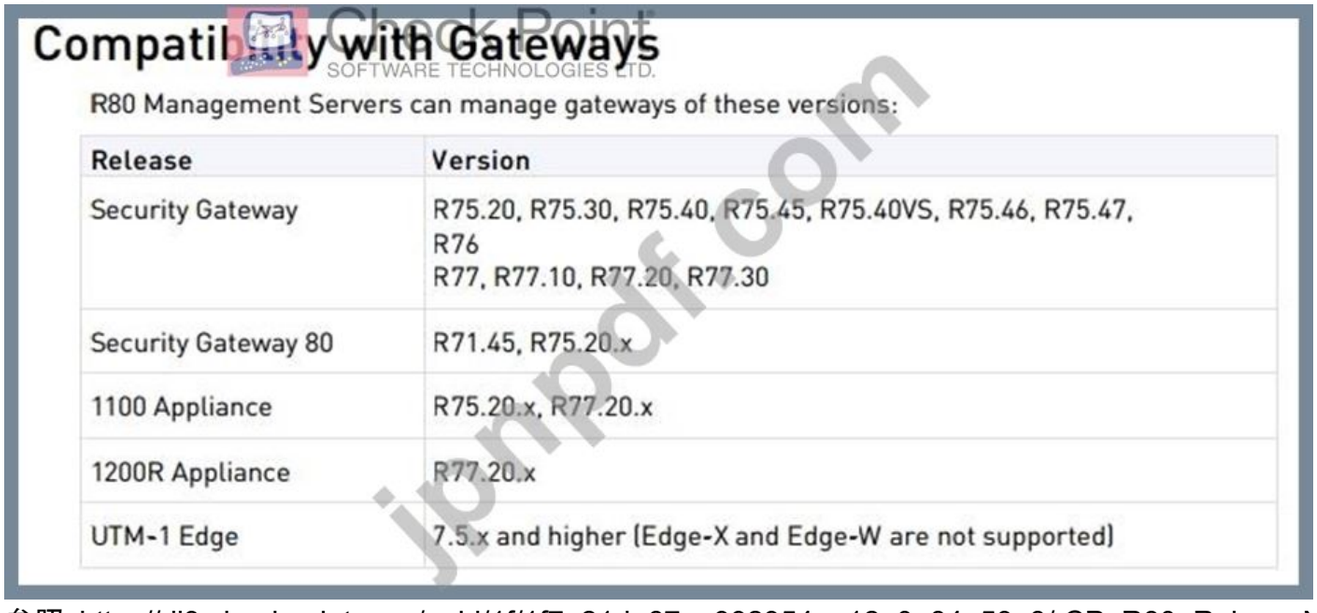
C. R80管理は、完全に異なる管理システムとして設計されているため、R80より前のチェックポイントゲートウェイのみを監視できます。

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

Answer: (解答を表示する**)**

説明/参照：

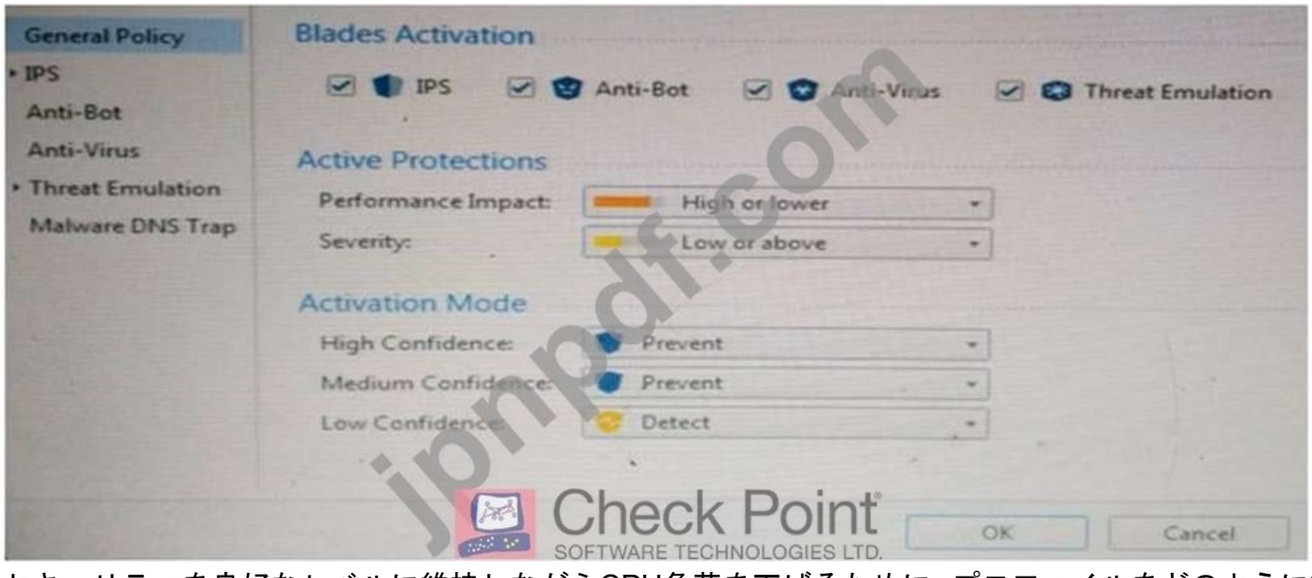
Explanation:



参照：http ://dl3.checkpoint.com/paid/1f/1f7e21da67aa992954aa12a0a84e53a8/ CP_R80_ReleaseNotes.pdf？HashKey = 1479838085_d6ffcb36c6a3128708b3f6d7bcc4f94e＆xtn = .pdf

最新問題**: 165**

すべての製品とプロトコルに非常に広い範囲を提供し、パフォーマンスに顕著な影響を与えます。



セキュリティを良好なレベルに維持しながらCPU負荷を下げるために、プロファイルをどのように調整できますか？最良の答えを選択してください。

A. パフォーマンスへの影響を中以下に設定します。
B. パフォーマンスへの影響を非常に低い信頼度に設定して防止します。
C. 問題は脅威防止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。
D. [高信頼度]を[低]に設定し、[低信頼度]を[非アクティブ]に設定します。
Answer: A (メーッセージを残す**)**

最新問題**: 166**
ThreatCloudからのウイルスシグネチャと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CheckPoint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. アンチウイルス
Answer: D (メーッセージを残す**)**
説明
強化されたCheckPointAntivirus Software Bladeは、リアルタイムのウイルスシグネチャと、サイバー犯罪と戦う最初のコラボレーションネットワークであるThreatCloudからの異常ベースの保護を使用して、ユーザーが影響を受ける前にゲートウェイでマルウェアを検出してブロックします。
参照：

最新問題**: 167**
_____は、VPNゲートウェイによって使用され、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します。
A. VPNトンネルインターフェース
B. VPNコミュニティ
C. VPNルーター
D. VPNインターフェース
Answer: A (メーッセージを残す**)**
説明
ルートベースのVPN
VPNトラフィックは、Security Gatewayオペレーティングシステムのルーティング設定（静的または動的）に従ってルーティングされます。セキュリティゲートウェイは、VTI（VPNトンネルインターフェイス）を使用し

て、VPNトラフィックを物理インターフェイスであるかのように送信します。VPNコミュニティのセキュリティゲートウェイの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: **168**
チェックポイントAPIを使用すると、システムエンジニアと開発者は、CLIツールとWebサービスを使用して、以下を除くすべての組織のセキュリティポリシーを変更できます。
A. サードパーティのタスクを管理するための新しいダッシュボードを作成します
B. サードパーティのソリューションを使用および強化する製品を作成する
C. 自動スクリプトを実行して一般的なタスクを実行する
D. チェックポイントソリューションを使用および強化する製品を作成する
Answer: A (メーッセージを残す**)**
説明
説明/参照 :http ://dl3.checkpoint.com/paid/29/29532b9eec50d0a947719ae631f640d0/CP_R80_CheckPoint_API_ReferenceGuide.pdf？HashKey = 1517081623_70199443034f806cf2dd0a7ba15f201c＆xtn = .pdf

最新問題: **169**
セキュリティゲートウェイでダイナミックディスパッチャを完全に有効にするには：
A. エキスパートモードでfw ctl multik set_mode 9を実行してから、再起動します
B. cpconfigを使用して、CoreXLメニューでDynamicDispatcherの値を「full」に更新します
C. / proc/interruptsを編集してファイルの下部にmultikset_mode1を含め、保存して再起動します
D. エキスパートモードでfw ctl multik set_mode 1を実行してから、再起動します
Answer: (解答を表示する**)**
参照：
https://supportcenter.checkpoint.com/supportcenter/portal？eventSubmit_doGoviewsolutiondetails =＆solutionid = sk105261＃Configuration%20R80.10

最新問題: **170**
どのCheckPointソフトウェアブレードがCheckPointデバイスを監視し、ネットワークの画像を提供し、セキュリティパフォーマンス？
A. 脅威エミュレーション
B. ログとステータス
C. アプリケーション制御
D. 監視
Answer: D (メーッセージを残す**)**

最新問題: **171**
Tomは、分散展開にCheckPointR80をインストールするように任命されました。トムがこの方法でシステムをインストールする前に、計算にSmartConsoleマシンを含めない場合、トムは何台のマシンを必要としますか？
A. 1台のマシンですが、互換性のためにSecurePlatformを使用してインストールする必要があります。
B. 1台のマシン

C. 2台のマシン
D. 3台のマシン
Answer: C (メーッセージを残す)
説明/参照：
Explanation:
1つはセキュリティ管理サーバー用で、もう1つはセキュリティゲートウェイ用です。

最新問題**: 172**
次のうち、VPN簡易モードとVPNコミュニティの要素ではないものはどれですか？
A. ルールベースの 暗号化」アクション
B. 恒久的なトンネル
C. ルールベースの VPN」列
D. 設定チェックボックス 暗号化されたすべてのトラフィックを受け入れる」
Answer: A (メーッセージを残す)
従来のモードから簡体字モードへの移行
従来型モードVPNから簡体字モードに移行するには：
1.[グローバルプロパティ]>[VPN]ページで、次のいずれかのオプションを選択します。
*すべての新しいファイアウォールポリシーへの簡易モード
*新しいファイアウォールポリシーごとに従来型または簡体字
2.[OK]をクリックします。
3. R80 SmartConsoleメニューから、[ポリシーの管理]を選択します。
[ポリシーの管理]ウィンドウが開きます。
4.[新規]をクリックします。
[新しいポリシー]ウィンドウが開きます。
5.新しいポリシーに名前を付けて、[アクセス制御]を選択します。
セキュリティポリシールールベースで、VPNとマークされた新しい列が表示され、[アクション]列で[暗号化]オプションが使用できなくなりました。これで、簡易モードで作業しています。
参照 :http ://dl3.checkpoint.com/paid/05/05e695b2012b4fd1d2bdfeccecd29290/CP_R80BC_VPN_AdminGuide.pdf？HashKey = 1479823792_55fbc10656c87db4fcf742f4899ba90d＆xtn = .pdf

最新問題**: 173**
Tinaは、新しいCheckPointR80管理コンソールインターフェイスを現在確認している新しい管理者です。[ゲートウェイ]ビューで、彼女は下のスクリーンショットのように[概要]画面を確認しています。 オープンサーバー」とは何ですか？

A. CheckPoint以外のアプライアンスにデプロイされたCheckPointソフトウェア。
B. セキュリティと可用性の目的で使用されるOpenServerConsortium承認のサーバーハードウェア。
C. Open Systems Interconnection（OSI）サーバーとセキュリティ展開モデルを使用して展開されたCheck PointManagementServer。
D. OpenSSLを使用するCheckPointManagementServerソフトウェア。
Answer: (解答を表示する**)**
説明/参照：
Explanation:

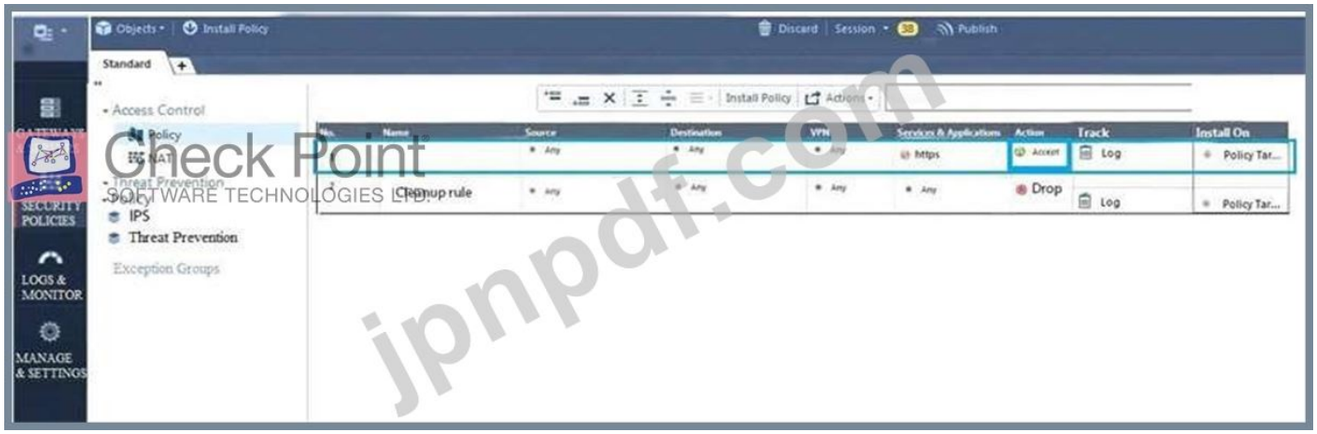
Open Server	Non-Check Point hardware platform that is certified by Check Point as supporting Check Point products. Open Servers allow customers the flexibility of deploying Check Point software on systems which have not been pre-hardened or pre-installed (servers running standard versions of Solaris, Windows, Red Hat Linux).

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

最新問題**: 174**
次のうち、識別名の構成要素ではないものはどれですか？
A. 組織単位
B. 国
C. 一般名
D. ユーザーコンテナ
Answer: D (メーッセージを残す**)**
説明
Explanation:
識別名コンポーネント
CN =共通名、OU =組織単位、O =組織、L =地域、ST =州または県、C =国名参照：
https ://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm？

トピック=ドキュメント/R76/ CP_R76_SecMan_WebAdmin / 71950

最新問題: **175**
次の図には、ポリシーのレイヤーがあります。



定義されたポリシーのトラフィック検査の優先順位は何ですか？
A. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。暗黙のドロップルールがパケットをドロップすると、IPSレイヤーの隣に到着し、パケットを受け入れた後、脅威防止レイヤーに渡されます。。
B. パケットはゲートウェイに到着し、ネットワークポリシーレイヤーのルールと照合されます。パケットを受け入れるルールがある場合は、IPSレイヤーの隣に来て、パケットを受け入れた後、脅威に渡されます。防止層。
C. パケットはゲートウェイに到着し、ネットワークポリシー層のルールと照合されます。パケットを受け入れるルールがある場合は、脅威防止層の隣に来て、パケットを受け入れた後、次の宛先に渡されます。IPSレイヤー。
D. パケットはゲートウェイに到着し、IPSポリシー層のルールと照合され、受け入れられた場合はネットワークポリシー層の隣に来て、パケットを受け入れた後、脅威防止層に渡されます。
Answer: B (メーッセージを残す**)**
説明
ポリシー管理を簡素化するために、R80はポリシーをポリシーレイヤーに編成します。レイヤーは、ルールのセット、またはルールベースです。
たとえば、以前のバージョンからR80にアップグレードする場合：
*ファイアウォールとアプリケーション制御ソフトウェアブレードが有効になっているゲートウェイでは、アクセス制御ポリシーがネットワークとアプリケーションの2つの順序付けられたレイヤーに分割されます。
ゲートウェイがレイヤー内のルールと一致すると、ゲートウェイは次のレイヤー内のルールの評価を開始します。
* IPSおよび脅威エミュレーションソフトウェアブレードが有効になっているゲートウェイでは、脅威防止ポリシーがIPSと脅威防止の2つの並列レイヤーに分割されます。
すべてのレイヤーが並行して評価されます

最新問題: **176**
SmartConsoleに表示される 不明な」SICステータスはどういう意味ですか？
A. SMSはセキュリティゲートウェイに接続できますが、安全な内部通信を確立できません。

B. SICアクティベーションキーをリセットする必要があります。
C. SICアクティベーションキーはどの管理者にも認識されていません。
D. セキュリティゲートウェイとSMSの間に接続はありません。
Answer: D (メーッセージを残す)
説明/参照：
Explanation:
最も一般的なステータスは通信です。その他のステータスは、SIC通信に問題があることを示しています。たとえば、SICステータスが不明の場合、ゲートウェイとセキュリティ管理サーバーの間に接続はありません。SICステータスが通信中でない場合、セキュリティ管理サーバーはゲートウェイに接続できますが、SIC通信を確立できません。
参照：https ://sc1.checkpoint.com/documents/R76/CP_R76_SecMan_WebAdmin/html_frameset.htm？topic = document / R76 / CP_R76_SecMan_WebAdmin / 118037

最新問題**: 177**
すべてのCheckPointMobile Accessソリューションで提供されていない機能はどれですか？
A. IPv6のサポート
B. きめ細かいアクセス制御
C. 強力なユーザー認証
D. 安全な接続
Answer: A (メーッセージを残す)
説明/参照：
Explanation:
ソリューションの種類
チェックポイントのすべてのリモートアクセスソリューションは、以下を提供します。
企業リソースへのエンタープライズグレードの安全な接続。
▪
強力なユーザー認証。
▪
きめ細かいアクセス制御。
▪
参照：https ://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/83586.htm

最新問題**: 178**
帯域幅とトラフィック制御ルールを適用するために使用されるポリシータイプはどれですか？
A. 脅威エミュレーション
B. アクセス制御
C. QoS
D. 脅威の防止
Answer: C (メーッセージを残す)
説明
チェックポイントのQoSソリューション
QoSは、Check Point Software Technologies Ltd.のポリシーベースのQoS管理ソリューションであり、帯域幅管理ソリューションのニーズを満たします。QoSは、ネットワークのハードウェアとソフトウェア全体に強制を

分散することにより、ネットワーク全体でトラフィックをエンドツーエンドで管理する、ソフトウェアのみに基づく独自のアプリケーションです。

最新問題: **179**
クリーンアップ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削除する
B. 不要なルールを決定するためのメトリックを提供します。
C. ポリシーをより適切に最適化するために使用されます
D. クリーンアップルールは目的を果たしません
Answer: A (メーッセージを残す**)**

最新問題: **180**
ルールに適用すると、特定のVPNコミュニティのVPNゲートウェイへのトラフィックを許可するオプションはどれですか。
A. すべての接続（クリアまたは暗号化）
B. 暗号化されたすべてのトラフィックを受け入れる
C. 特定のVPNコミュニティ
D. すべてのサイト間VPNコミュニティ
Answer: B (メーッセージを残す**)**
最初のルールは、すべての暗号化トラフィックを受け入れる機能の自動ルールです。BranchOfficesおよびLondonOfficesVPNコミュニティのセキュリティゲートウェイのファイアウォールは、これらのコミュニティのクライアントのホストからのすべてのVPNトラフィックを許可します。セキュリティゲートウェイへのトラフィックはドロップされます。このルールは、これらのコミュニティのすべてのセキュリティゲートウェイにインストールされます。
2.サイト間VPN-すべてのサイト間VPNコミュニティのVPNドメイン内のホスト間の接続が許可されます。許可されているプロトコルは、FTP、HTTP、HTTPS、SMTPのみです。
3.リモートアクセス-RemoteAccessVPN　コミュニティのVPNドメイン内のホスト間の接続が許可されます。許可されるプロトコルは、HTTP、HTTPS、およびIMAPのみです。
参照 :https ://sc1.checkpoint.com/documents/R76/CP_R76_Firewall_WebAdmin/92709.htm

最新問題: **181**
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. 送信元アドレス
B. 宛先アドレス
C. TCP確認応答番号
D. ソースポート
Answer: (解答を表示する**)**
説明
参照：

最新問題**: 182**
空欄に記入してください :Security Gateways R75以降では、SICは暗号化に_____を使用します。
A. AES-128
B. AES-256
C. DES
D. 3DES
Answer: A (メーッセージを残す**)**
説明/参照：
参照 :https ://sc1.checkpoint.com/documents/R80/CP_R80_SecMGMT/html_frameset.htm？トピック=ドキュメント/R80/ CP_R80_SecMGMT / 125443

最新問題**: 183**
ゼロデイおよび未発見の脅威からの保護を提供するCheckPoint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. 脅威エミュレーション
C. アプリケーション制御
D. 脅威の抽出
Answer: D (メーッセージを残す**)**
説明
SandBlast脅威エミュレーション
次世代脅威抽出ソフトウェアバンドル（NGTX）の一部として、SandBlast脅威エミュレーション機能は、ゼロデイ攻撃や標的型攻撃による未発見のエクスプロイトによる感染を防ぎます。この革新的なソリューションは、ファイルをすばやく検査し、仮想サンドボックスで実行して悪意のある動作を発見します。
検出されたマルウェアはネットワークに侵入できなくなります。
参照：

最新問題**: 184**
空欄に記入してください :セキュリティポリシーは_____に作成され、_____に保存されます。さまざまな_____に配布されます。
A. SmartConsole、セキュリティゲートウェイ、セキュリティ管理サーバー
B. SmartConsole、セキュリティ管理サーバー、セキュリティゲートウェイ
C. ルールベース、セキュリティ管理サーバー、セキュリティゲートウェイ

D. チェックポイントデータベース、SmartConsole、セキュリティゲートウェイ
Answer: C (メッセージを残す**)**

最新問題**: 185**
Joeyは、R80セキュリティ管理サーバーでNTPを構成したいと考えています。彼はこれをWebUI経由で行うことにしました。ブラウザ経由でGaiaプラットフォームのWebUIにアクセスするための正しいアドレスは何ですか？
A. https ://<Device_IP_Address>
B. https ://<Device_IP_Address> :443
C. https ://<Device_IP_Address> :10000
D. https ://<Device_IP_Address> :4434
Answer: A (メッセージを残す**)**
説明
Web UI Gaia管理インターフェースへのアクセス、ブラウザーからデフォルトの管理IPアドレスへの接続を開始します。WebUIへのログインログインWebUIにログインするには：
*ブラウザに次のURLを入力してください：
https ://<ガイアIPアドレス>
*ユーザー名とパスワードを入力します。

最新問題**: 186**
「フルログ」追跡オプションに含まれているが、「ログ」追跡オプションには含まれていない情報はどれですか？
A. ファイル属性
B. アプリケーション情報
C. 宛先ポート
D. データ型情報
Answer: D (メッセージを残す**)**
説明/参照：
Explanation:追跡オプション
ネットワークログ基本的なファイアウォール情報（送信元、宛先、送信元ポート、
宛先ポート、およびプロトコル。
ログ-ネットワークログオプションと同等ですが、アプリケーション名も含まれます（たとえば、
Dropbox）、およびアプリケーション情報（たとえば、WebサイトのURL）。これはデフォルトの追跡オプションです。
フルログ-ログオプションと同等ですが、行われた各URLリクエストのデータも記録します。
-抑制が選択されていない場合、完全なログが生成されます（R80以前の管理で定義されているとおり）。
-抑制が選択されている場合、拡張ログが生成されます（R80以前の管理で定義されているとおり）。
なし-ログを生成しません。
参照：https ://sc1.checkpoint.com/documents/R80/CP_R80_LoggingAndMonitoring/ html_frameset.htm？topic = document / R80 / CP_R80_LoggingAndMonitoring / 131914

最新問題: **187**
次のスクリーンショットを見て、最良の答えを選択してください。

A. Security Gatewayの外部のクライアントは、FTPを使用してFTP_Extサーバーからアーカイブファイルをダウンロードできます。
B. Security Gatewayの外部のクライアントは、FTPを使用してFTP_Extサーバーに任意のファイルをアップロードできます。
C. 内部クライアントは、FTPを使用して任意のファイルをFTP_Ext-serverにアップロードおよびダウンロードできます。
D. 内部クライアントは、FTPを使用してアーカイブファイルをFTP_Extサーバーにアップロードおよびダウンロードできます。
Answer: A (メーッセージを残す**)**