Juniper.JN0-232.v2026-06-27.q23

試験コード:	JN0-232
試験名称:	Security, Associate (JNCIA-SEC)
認定資格:	Juniper
無料問題数:	23
バージョン:	v2026-06-27
アクセス数:	111
ページビュー数:	230
https://www.jpnpdf.com/Juniper.JN0-232.v2026-06-27.q23-mondaishu.html	

最新問題: **1**

展示」ボタンをクリックします。

展示物に関して、正しい記述はどれですか。(2 つ選択してください。)

A. URL は定義済みの Web フィルタリング カテゴリと一致します。

B. NextGen Web フィルタリング タイプが使用されています。

C. SRX ファイアウォールには SSL プロキシ構成がありません。

D. これはカスタム Web フィルタリング ブロック メッセージです。

Answer: (解答を表示する**)**

展示より:

* ユーザーは https://www.wikipedia.org にアクセスしようとしました。
* ブロックページには次の内容が表示されます:
* カテゴリー: NG_リファレンス
* 理由: 事前定義済み
* ヘッダーには 『Juniper Web Filteringはこのサイトをブロックするように設定されています。」と記載されています。オプションの分析：

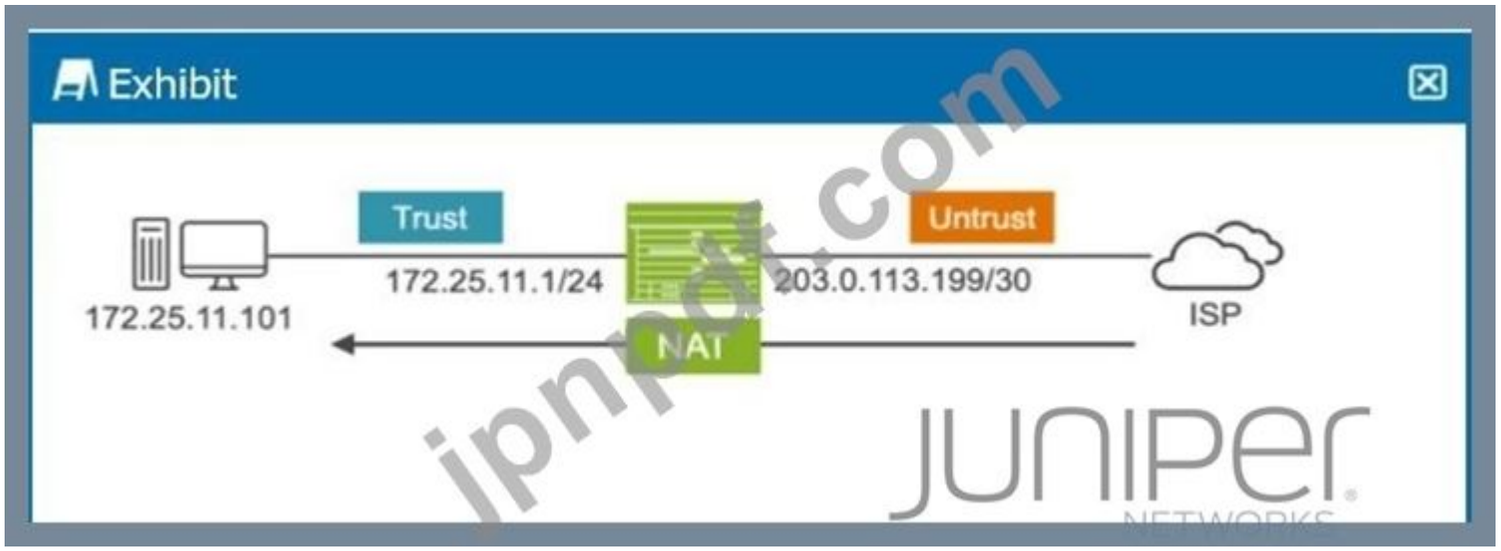
* オプションA: 正解です。ログには「REASON: BY_PRE_DEFINED」と表示されています。これは、Webフィルタリングデータベースの定義済みカテゴリに一致したため、サイトがブロックされたことを意味します。
* オプションB: 正解です。カテゴリ「NG_Reference」は、NextGen（拡張クラウドベース）Webフィルタリングタイプが使用されていることを示します。
* 選択肢C：不正解です。この図ではSSLプロキシ設定に関する情報は提供されておらず、HTTPSサイトがブロックされたことのみが示されています。
* オプションD：不正解です。表示されるブロックページは、カスタムメッセージではなく、Juniperの標準のデフォルトブロックページです。
正しい記述: URL は定義済みの Web フィルタリング カテゴリと一致しており、NextGen Web フィルタリング タイプが使用されています。
参考資料:Juniper Networks - Web フィルタリング (SurfControl、拡張、および NextGen Web フィルタリング)、Junos OS セキュリティの基礎。

最新問題**: 2**
Junos OS で論理インターフェースを個別のセキュリティ ゾーンに割り当てる目的は何ですか?
A. ネットワークインターフェースの設定を簡素化する
B. ルーティングプロトコルとアップデートを管理する
C. セキュリティポリシーを使用して、異なるVLANを通過するトラフィックを制御する
D. SNMP によるネットワーク監視を有効にする
Answer: C (メーッセージを残す**)**
Junos OSでは、セキュリティゾーンがSRXファイアウォールポリシー適用の基盤となります。論理インターフェースをゾーンに割り当てる必要があります。これにより、以下のことが可能になります。
* ゾーン境界によるトラフィックの分離。
* ゾーン間を通過するトラフィックに対するセキュリティ ポリシーの適用。
* VLAN、サブネット、または機能領域 (信頼、非信頼、DMZ など) 全体のトラフィックの制御。
その他のオプション:
* ゾーン割り当ては、インターフェース構成を簡素化するために使用されません (A)。
* ルーティング プロトコルと更新 (B) は、ゾーンではなくルーティング インスタンスによって処理されます。
* SNMP 監視 (D) は、ゾーンではなく、システムまたはサービスの構成で有効になります。
参考資料:Juniper Networks - セキュリティ ゾーンとポリシーの適用、Junos OS セキュリティの基礎。

最新問題**: 3**
SRX シリーズ ファイアウォールの Null ゾーンに関する次の 2 つの記述のうち正しいものはどれですか。(2 つ選択してください。)
A. トランジット インターフェイスは、デフォルトで null ゾーンに割り当てられます。
B. セキュリティ ポリシーによって拒否されたトラフィックは、ログ記録のために null ゾーンに送信されます。
C. ヌル ゾーンは、SRX シリーズ ファイアウォールとの間のトラフィックを受け入れるように設定できます。
D. セキュリティ ゾーンに設定された論理インターフェイスは、ヌル ゾーンから削除されます。
Answer: (解答を表示する**)**
* デフォルトの割り当て: すべての論理インターフェイスは、ユーザー定義のセキュリティ ゾーンに明示的に割り当てられるまで、デフォルトでヌル ゾーンに配置されます (オプション A が正解)。
* ヌル ゾーンからの削除: インターフェイスがセキュリティ ゾーンに割り当てられると、ヌル ゾーンから削除されます (オプション D が正解です)。
* トラフィック受け入れなし: ヌル ゾーンは破棄ゾーンであるため、トラフィックを受け入れるように設定することはできません (オプション C は誤りです)。
* ポリシーの動作 :セキュリティポリシーによって拒否されたトラフィックは、ポリシーアクションに従ってドロップされます。ログ記録のためにヌルゾーンに転送されることはありません（オプションBは誤りです）。

正しい記述 :AとD
参考資料:Juniper Networks - セキュリティ ゾーンと Null ゾーン、Junos OS セキュリティの基礎。

最新問題: **4**
展示」ボタンをクリックします。



セッションは外部デバイスからのみ確立できるようにする必要があります。
展示物を参照すると、どのタイプの NAT が実行されていますか?
A. 宛先NATのみ
B. 送信元NATのみ
C. 静的PATのみ
D. 静的NATとソースNAT
Answer: (解答を表示する**)**
展示より:
* 内部ホスト (172.25.11.101) は信頼ゾーンにあります。
* ISPとの通信には外部アドレス（203.0.113.199/30）が使用されます。
* 要件は、セッションが外部デバイス (ISP または信頼できない側) から内部ホストに向かってのみ開始できることです。
この要件は、Destination NAT の動作と一致します。
* 宛先NATのみ（オプションA）：外部パブリックIP（203.0.113.199）を内部/プライベートIP（172.25.11.101）にマッピングします。これにより、着信接続が変換され、内部ホストに送信されます。変換は着信トラフィックにのみ適用されるため、内部ホストは発信セッションを開始できません。
* ソース NAT のみ (オプション B): 内部プライベート IP からインターネットへの送信セッションに使用されます。
これは要件を満たしていません。
* 静的PAT（オプションC）：パブリックIPアドレスの単一ポートをプライベートIPアドレス/ポートにマッピングします。この図はポートベースの変換を示すものではありません。
* 静的NATと送信元NAT（オプションD）：双方向通信が可能になり、双方向にセッションを開始できるようになります。これは要件に反します。
正しいNATタイプ:宛先NATのみ
参考資料:Juniper Networks - NAT タイプ (ソース NAT、宛先 NAT、静的 NAT)、Junos OS セキュリティの基礎。

最新問題: **5**
セキュリティ ゾーンについて正しい記述はどれですか。(2 つ選択してください。)

A. インターフェイスは複数のセキュリティ ゾーンに存在できます。
B. 同じセキュリティ ゾーン内のインターフェイスは、同じルーティング インスタンスを共有する必要があります。
C. 同じセキュリティ ゾーン内のインターフェイスは、個別のルーティング インスタンスを使用する必要があります。
D. セキュリティ ゾーンには複数のインターフェイスを含めることができます。
Answer: B,D (メーッセージを残す**)**
* オプション B: 正解。同じセキュリティ ゾーン内のインターフェイスは同じルーティング インスタンスに属している必要があります。ゾーンは複数のルーティング インスタンスにまたがることはできません。
* オプション D: 正解。セキュリティ ゾーンには複数のインターフェイスを含めることができ、同様の信頼レベルをグループ化できます (例: 信頼ゾーン内の複数の LAN サブネット)。
* オプションA: 不正解です。インターフェースは一度に1つのゾーンにのみ属することができます。
* オプション C: 不正解です。同じゾーン内のインターフェースをルーティングインスタンス間で分割することはできません。
正しい記述: 同じゾーン内のインターフェースは同じルーティングインスタンスを共有する必要があり、ゾーンには複数のインターフェースを含めることができます。
参考資料:Juniper Networks - セキュリティ ゾーンとルーティング インスタンス、Junos OS セキュリティの基礎。

最新問題**: 6**
ルール セット内の NAT ルールの処理について正しい記述はどれですか (2 つ選択してください)。
A. NAT ルール処理はすべてのルールを処理します。
B. NAT ルールの処理は最初の一致で停止します。
C. NAT ルールは上から下に処理されます。
D. NAT ルールは下から上に処理されます。
Answer: (解答を表示する**)**
SRX デバイスでの NAT ルール処理は、決定論的な順序に従います。
* 上から下の順序 (オプション C): NAT ルールは常に、設定に表示される順序で上から評価されます。
* 最初に一致したものが勝ち (オプション B): パケットが NAT ルールに一致すると、処理が停止します。
* オプションA: 不正解です。すべてのルールが処理されるわけではなく、最初の一致で評価が停止します。
* オプション D: 不正解です。NAT ルールは下から上に処理されることはありません。
正しい記述: NAT ルールの処理は最初の一致で停止し、NAT ルールは上から下へ処理されます。
参考:Juniper Networks - NAT ルールの処理順序、Junos OS セキュリティの基礎。

最新問題**: 7**
コンテンツ フィルタリングは、次のプロトコルのうちどれをサポートしていますか (2 つ選択してください)。
A. SMTP
B. SNMP
C. TFTP
D. HTTP
Answer: (解答を表示する**)**
SRX デバイスのコンテンツ フィルタリングは、特定のアプリケーション プロトコルを介して転送される特定のファイル タイプを検査および制御します。
* SMTP（オプションA）サポートされています。コンテンツフィルタリングにより、メール内の特定の添付ファイルをブロックできます。

* HTTP オプションD）サポートされています。コンテンツフィルタリングにより、Webトラフィック経由の特定のファイルタイプのダウンロードをブロックできます。
* SNMP (オプション B): サポートされていません。SNMP は管理プロトコルであり、コンテンツ配信プロトコルではありません。
* TFTP (オプション C):コンテンツ フィルタリングではサポートされません。
正しいプロトコル:SMTPとHTTP
参考資料:Juniper Networks - コンテンツ セキュリティとフィルタリングでサポートされるプロトコル、Junos OS セキュリティの基礎。

最新問題**: 8**
パケット フローをデバッグするには、トレース オプションを有効にするように求められます。
このシナリオでは、[edit security flow traceoptions] 階層でどのフラグを設定しますか?
A. パケットダンプ
B. 一般
C. 状態
D. 基本データパス
Answer: A (メーッセージを残す**)**
セキュリティ フロー階層のトレース オプションは、フロー モジュールでパケットが処理される方法のデバッグを提供します。
* 詳細なパケットレベルのデバッグをキャプチャするための正しいフラグは、packet-dump オプションA）です。これにより、フロー決定、NAT処理、ポリシー一致を示すパケットレベルのトレースメッセージが出力されます。
* 一般 (オプション B): 基本的なフロー トレース情報は提供しますが、完全なパケット検査は提供しません。
* state (オプション C): フロー状態の遷移を追跡します。パケットダンプよりも詳細度は低くなります。
* basic-datapath (オプション D): 詳細なフロー トラブルシューティングではなく、高レベルのデータパス デバッグを提供します。
正しいフラグ:パケットダンプ
参考:Juniper Networks - セキュリティ フロー トレース オプション、Junos OS セキュリティの基礎。

最新問題**: 9**
ハイエンドの SRX シリーズ デバイスでコントロール プレーン トラフィックをキャプチャする必要があります。
このタスクをどのように達成しますか?
A. edit security datapath-debug capture 階層の下にパケット キャプチャを設定します。
B. サンプルアクションを使用して、目的のトラフィックに一致するファイアウォール フィルターを適用します。
C. シェルを起動し、tcpdump ツールを使用します。
D. 転送オプションの編集階層の下にポートミラーリング構成を適用します。
Answer: B (メーッセージを残す**)**
ハイエンドの SRX プラットフォームでは、コントロール プレーン (ルーティング エンジン宛て) トラフィックはループバック (lo0) を通過し、then sample アクションで lo0 にファイアウォール フィルターを適用し、転送オプションでトラフィック サンプリングを行ってパケットをファイルに書き込むことで、最も効果的にキャプチャされます。
* サンプルは一致したコントロール プレーン パケットをサンプリング プロセスに送信し、分析のために記録することができます。
* datapath-debug キャプチャはデータ プレーン/SPC パスに重点を置いており、一般的なコントロール プレーン パケット キャプチャ用のツールではありません。

* シェルからの tcpdump は SRX でサポートされているワークフローではありません。操作コマンドは monitor traffic ですが、ハイエンドのコントロール プレーン キャプチャの場合は、推奨されるスケーラブルな方法は lo0 filter + サンプリングです。
* ポートミラーリングは、RE 宛てのコントロールプレーン パケットではなく、通過データプレーン トラフィックをミラーリングします。
参考資料:Juniper Networks - Junos OS セキュリティの基礎、「コントロール プレーン トラフィックのキャプチャ (lo0 フィルタとサンプリング)」。

最新問題: **10**
管理機能ゾーンに関する次の記述のうち正しいものはどれですか。(2 つ選択してください。)
A. 管理機能ゾーンは、デバイスへのアクセスが許可される管理関連のトラフィックを制御するために使用されます。
B. 管理機能ゾーンには、ユーザー定義のセキュリティ ゾーンに割り当てられるまで、使用可能なすべての収益ポートが含まれます。
C. 管理機能ゾーンは、SRX シリーズ ファイアウォール上に自動的に作成されます。
D. 管理機能ゾーンはどのセキュリティ ポリシーでも参照できません。
Answer: A,C (メーッセージを残す**)**
SRX デバイスの管理機能ゾーンは、固有の特性を持つ特別な定義済みゾーンです。
* 自動的に作成され(オプション C)、削除することはできません。
* SSH、Telnet、Web 管理 (J-Web)、SNMP、その他のコントロール プレーン サービスなどの管理関連トラフィック (オプション A) に特に使用されます。
* 収益（データ）インターフェースは含まれていません（オプションBは誤りです）。インターフェースはユーザー定義ゾーンに明示的に設定する必要があります。
* 管理トラフィックを含むゾーン間通信が必要な場合、ポリシーで管理ゾーンを参照できます (オプション D は誤りです)。
正しい記述：AとC
参考資料:Juniper Networks - セキュリティ ゾーンと管理機能ゾーン、Junos OS セキュリティの基礎。

最新問題: **11**
SRX シリーズ ファイアウォールの統合セキュリティ ポリシーについて正しい記述はどれですか (2 つ選択してください)。
A. 統合セキュリティ ポリシーは、ポリシー ステートメントを処理する前にアプリケーションを照合します。
B. 統合セキュリティ ポリシーは、ゾーンベースまたはグローバルにすることができます。
C. 統合セキュリティ ポリシーは、アプリケーション識別 (AppID) エンジンを使用します。
D. 複数の一致がある統合セキュリティ ポリシーでは、最も制限の厳しい一致が使用されます。
Answer: B,C (メーッセージを残す**)**
統合セキュリティポリシーは、従来のゾーンベースのポリシーとアプリケーションベースのポリシーを統合します。その特徴は次のとおりです。
* ゾーンベースまたはグローバル (オプション B):統合ポリシーは、ゾーン固有ポリシーまたはグローバル ポリシーとして適用できます。
* AppID エンジン (オプション C): アプリケーション識別に AppID エンジンを活用し、アプリケーション層でのきめ細かな制御を可能にします。
* ポリシー マッチング (オプション A): ポリシーは標準のセキュリティ ポリシーと同様に順番に評価されます。ポリシー処理の前にアプリケーションはマッチングされません。
* 複数の一致（オプション D）：複数ポリシーが一致する場合、「最も制限の厳しい」ポリシーではなく、最初の一致（順番が適用されます。正しい記述：B および C 参照：Juniper Networks - 統合セキュリティ ポリシーと AppSecure の統合、Junos OS セキュリティの基礎。

最新問題: **12**
セキュリティ ゾーンに関する次の記述のうち正しいものはどれですか。(2 つ選択してください。)
A. トラフィックを送受信する前に、ネットワーク インターフェイスをセキュリティ ゾーンに追加します。
B. セキュリティ ゾーンは、ネットワーク インターフェイスによって受け入れられる例外トラフィックの種類を制御します。

C. 同じセキュリティ ゾーン内のインターフェイスは、異なるルーティング インスタンスを使用できます。
D. セキュリティ ゾーンには、異なるルーティング インスタンスに割り当てられたインターフェイスが含まれます。
Answer: (解答を表示する**)**
* インターフェースの追加 オプションA）インターフェースは、トラフィックを通過させる前にセキュリティゾーンに割り当てる必要があります。デフォルトでは、インターフェースはヌルゾーンに配置され、トラフィックを送受信できません。
* 例外トラフィック (オプション B): セキュリティ ゾーンは、ホストの受信トラフィック設定を定義します。これにより、許可される管理またはコントロール プレーン トラフィック (SSH、ICMP、SNMP) の種類が決まります。
* ルーティングインスタンス オプションCおよびD）セキュリティゾーンはルーティングインスタンスに固有であり、複数のインスタンスのインターフェースを含めることはできません。したがって、同じゾーン内のインターフェースは、異なるルーティングインスタンスに属することはできません。
正しい記述 :AとB
参考:Juniper Networks - セキュリティ ゾーンの概要、Junos OS セキュリティの基礎。

最新問題**: 13**
セキュリティ ポリシーのマッチングに使用される 2 つの基準はどれですか (2 つ選択してください)。
A. MACアドレス
B. 送信元アドレス
C. インターフェース名
D. アプリケーション
Answer: (解答を表示する**)**
Junos OS のセキュリティ ポリシーは、特定の基準に基づいてトラフィックを照合します。
* 送信元アドレスと宛先アドレス オプション B）。
* アプリケーション (オプション D)。サービスとして定義されるか (例: tcp/80)、AppID を通じて認識されます。
その他のオプション:
* MAC アドレス (オプション A) はポリシー マッチングでは使用されません。ポリシーはレイヤー 3/4 で動作します。
* インターフェース名 (オプション C) は、セキュリティ ポリシー定義ではなく、ファイアウォール フィルターで使用されます。
正しい基準:送信元アドレスとアプリケーション
参考:Juniper Networks - セキュリティ ポリシーの一致条件、Junos OS セキュリティの基礎。

最新問題**: 14**
SRX シリーズ ファイアウォールが SBL サーバーに接続されていることを確認します。
このシナリオではどの操作モード コマンドを使用しますか?
A. セキュリティ UTM ウイルス対策ステータスを表示
B. セキュリティウェブフィルタリングのステータスを表示する
C. セキュリティ UTM コンテンツフィルタリングの統計情報を表示する
D. セキュリティ UTM のスパム対策ステータスを表示
Answer: B (メーッセージを残す**)**
SBL $urfControl Web Filtering）サーバー統合は、SRX上のUTM Webフィルタリング機能の一部です。ファイアウォールがSBLサーバーに正しく接続され、通信していることを確認するには、次のコマンドを使用します。
セキュリティウェブフィルタリングステータスを表示
このコマンドは、SBL サーバとの接続情報、ライセンス ステータス、フィルタリング操作を表示します。

その他のオプション:
* ウイルス対策 (オプション A) は、ウイルス対策エンジンの状態を確認します。
* コンテンツ フィルタリング統計 (オプション C) には、ローカル コンテンツ フィルタリング カウンターが表示されます。
* スパム対策ステータス (オプション D) は、スパム エンジンの接続をチェックします。
正しいコマンド: セキュリティウェブフィルタリングステータスの表示
参考:Juniper Networks - UTM Web フィルタリング操作コマンド、Junos OS セキュリティの基礎。

最新問題**: 15**
Junos OS はさまざまな形式の NAT をどのような順序で処理しますか?
A. 静的NAT、宛先NAT、送信元NAT
B. 宛先NAT、送信元NAT、静的NAT
C. 送信元NAT、静的NAT、宛先NAT
D. 送信元NAT、宛先NAT、静的NAT
Answer: (解答を表示する**)**
Junos OS の NAT 処理は、正しいパケット処理を保証するために厳密なシーケンスに従います。
* 静的 NAT - 永続的な 1 対 1 の双方向マッピングを提供するため、最初に適用されます。
* 宛先 NAT - 着信宛先アドレスを変換するために 2 番目に適用され、プライベート ネットワーク内のサーバーでよく使用されます。
* ソース NAT - 最後に適用され、送信プライベート ソース アドレスをパブリック アドレスに変換します。
これにより、決定論的な動作が保証され、翻訳タイプ間の競合が回避されます。
* オプション B、C、および D には誤ったシーケンスがリストされています。
正しい順序:静的NAT # 宛先NAT # 送信元NAT
参考:Juniper Networks - NAT 処理順序、Junos OS セキュリティの基礎。

最新問題**: 16**
グローバル セキュリティ ポリシーに関する次の 2 つの記述のうち、正しいものはどれですか。(2 つ選択してください。)
A. グローバル セキュリティ ポリシーでは、from-zone コンテキストと to-zone コンテキストは必要ありません。
B. グローバル セキュリティ ポリシーには特定のゾーン コンテキストが必要です。
C. グローバル ポリシーは、ゾーンベースのセキュリティ ポリシーの前に処理されます。
D. ゾーンベースのセキュリティ ポリシーとグローバル セキュリティ ポリシーの両方を同時に使用できます。
Answer: (解答を表示する**)**
グローバルセキュリティポリシーは、SRX全体にわたるポリシー適用の柔軟性を高めます。特定の送信元ゾーンや宛先ゾーンに縛られることはありません。
* 送信元ゾーンと送信先ゾーンのコンテキストは不要です（オプションA）。一致条件によって制限されない限り、グローバルポリシーはすべてのゾーンに適用されます。
* グローバル セキュリティ ポリシーでは特定のゾーン コンテキストは必要ありません (オプション B は誤りです)。
* グローバルポリシーはゾーンベースポリシーの前ではなく後に処理されます。つまり、ゾーンベースセキュリティポリシーが優先されます（オプションCは誤りです）。
* 管理者は、同じデバイス上でゾーンベースのセキュリティ ポリシーとグローバル セキュリティ ポリシーの両方を同時に構成できます (オプション D が正解です)。

これにより、特定のポリシーをゾーンごとに適用しながら、複数のゾーンにわたってルールを重複させることなく一般的なポリシーをグローバルに適用できる柔軟な設計が可能になります。
参考:Juniper Networks - Junos OS セキュリティの基礎、グローバル セキュリティ ポリシー。

最新問題: **17**
フロー モジュールではいつスクリーニングが行われますか?
A. セッション検索の前
B. ポリシー検索中
C. ルート検索中
D. セッション検索後
Answer: A (メーッセージを残す**)**
Juniper SRXのフローベースパケット処理では、フローモジュールがスクリーニング、セッション管理、NAT、ポリシー適用などのセキュリティ機能を担います。処理順序は非常に重要です。
* スクリーンはセッション検索の前に適用されます。これにより、セッション管理のためにリソースを消費する前に、パケットに異常、フラッド、またはプロトコル違反がないか検査されます。これらのスクリーンの例には、TCP SYNフラッド保護、ICMPフラッド保護、ポートスキャン保護などがあります。
* スクリーニング後、セッション検索が行われます。この時点で、ファイアウォールはパケットがセッションテーブル内の既存のセッションに属しているかどうかを確認します。一致するセッションが見つかった場合、パケットはポリシー評価をバイパスし、セッション状態に従って転送されます。
* 既存のセッションが見つからない場合、新しいセッションが作成される前に、パケットはルート検索、NAT 処理、およびセキュリティ ポリシー評価を続行します。
このように、スクリーニングはセッション検索の前に行われ、フロープロセスの早い段階でシステムを保護します。この設計により、セッションリソースを割り当てる前に悪意のあるトラフィックや不正なトラフィックをドロップすることで、効率性が確保されます。
参考資料:Juniper Networks - SRX シリーズ サービス ゲートウェイのセキュリティ処理 (フロー モジュール シーケンス)、Junos OS セキュリティの基礎、公式コース ガイド。

最新問題: **18**
宛先 NAT に関する次の 2 つの記述のうち正しいものはどれですか。(2 つ選択してください。)
A. 宛先 NAT により、プライベート ネットワーク上のホストがインターネット上のリソースにアクセスできるようになります。
B. SRX シリーズ ファイアウォールは、インターフェース ベースの宛先 NAT をサポートします。
C. 宛先 NAT により、インターネット上のホストがプライベート ネットワーク上のリソースにアクセスできるようになります。
D. SRX シリーズ ファイアウォールは、プールベースの宛先 NAT をサポートします。
Answer: C,D (メーッセージを残す**)**
* 宛先NATの目的（オプションC）インターネット上の外部ホストが内部ネットワークにアクセスできるようにするために使用されます。/private リソース（DMZ 内の Web サーバーなど）の場合、宛先 NAT は、受信トラフィックの宛先 IP を内部サーバーに合わせて変更します。
* プールベースの NAT (オプション D):SRX は宛先 NAT プールをサポートし、複数のパブリック IP アドレスまたは範囲を内部サーバーに変換できます。

* 誤ったオプション:
* オプション A は、宛先 NAT ではなく、送信元 NAT について説明します。
* オプション B は、SRX が 「インターフェースベース」の宛先 NAT をサポートしていないため、正しくありません。
正しい記述:CとD
参考資料:Juniper Networks - NAT のタイプと構成 (ソース、宛先、静的)、Junos OS セキュリティの基礎。

最新問題**: 19**
外部向けファイアウォールのセキュリティ設定の複雑さを軽減するよう求められています。以前の管理者が、様々なRFC1918アドレスをカバーする数百ものプライベートサブネットNATルールを設定していたことに気付きました。
これらすべてのルールを、すべての RFC1918 アドレスをカバーする単一のルールに置き換えます。
このシナリオではどのルールを使用しますか?
A. セキュリティ NAT ソース ルール セット private-to-pub ルール RFC1918 一致ソース アドレス [10.0.0.0/8 192.168.0.0/16 172.16.0.0/12]
B. セキュリティ NAT ソース ルール セット private-to-pub ルール RFC1918 一致ソース アドレス [10.0.0.0/8 192.16.0.0/12 172.168.0.0/16]
C. セキュリティ NAT ソース ルール セット private-to-pub ルール RFC1918 一致ソース アドレス [10.0.0.0/8 172.168.0.0/16 192.0.2.0/24 203.1.113.0/24]
D. セキュリティ NAT ソース ルール セット private-to-pub ルール RFC1918 一致ソース アドレス [10.0.0.0/8 192.168.0.0/16 172.16.0.0/12 192.0.2.0/24]
Answer: (解答を表示する**)**
RFC 1918 では、次の 3 つのプライベート IPv4 ブロックが定義されています。
* 10.0.0.0/8
* 172.16.0.0/12
* 192.168.0.0/16
オプション A は、単一のソース NAT ルール内のこれらの範囲に正確に一致し、サブネットごとの多数のエントリを置き換えます。
* オプション B および C には、無効または RFC1918 以外のネットワークが含まれます (例: 192.16.0.0/12、172.168.0.0/16)。
* オプション D は、RFC1918 ではない network192.0.2.0/24 というドキュメントを誤って追加します。
参考:Juniper Networks - Junos OS セキュリティの基礎、「ソース NAT マッチング」および RFC 1918 プライベート アドレス範囲。

最新問題**: 20**
「展示」ボタンをクリックします。

Exhibit

```
[edit security policies from-zone Trust to-zone Trust]
user@SRX# show
policy allow-all {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
```


展示品にはどのようなタイプのポリシーが示されていますか?

A. グローバルポリシー

B. ゾーン間ポリシー

C. ゾーン内ポリシー

D. デフォルトポリシー

Answer: C (メーッセージを残す**)**

展示構成より：

[セキュリティポリシーを編集 from-zone Trust to-zone Trust]

ポリシーすべて許可 {

マッチ {

送信元アドレス 任意;

宛先アドレス 任意;

アプリケーション任意;

}

それから {

許可する;

}

}

* from-zone と to-zone は両方とも Trust # Trust に設定されています。

* これは、ポリシーが同じゾーン内のトラフィックを管理していることを意味します。

* 同じゾーン内のポリシーは、ゾーン内ポリシーと呼ばれます。

オプションの分析:

* グローバルポリシー (A): ゾーン固有ではなく、ゾーン全体に普遍的に適用されます。ただし、ここでは当てはまりません。

* ゾーン間ポリシー (B): 2つの異なるゾーン間に適用されます（例TrustゾーンとUntrustゾーン）。両方のゾーンがTrustゾーンであるため、このポリシーは適用されません。
* ゾーン内ポリシー (C): 正解。同じゾーン (信頼番号 Trust) 内のトラフィックに適用されます。
* デフォルトポリシー (D): 一致するポリシーがない場合に適用される暗黙的な全拒否ポリシー。この図には示されていません。
正しいポリシータイプ:ゾーン内ポリシー
参考資料:Juniper Networks - セキュリティ ポリシー タイプ (ゾーン間、ゾーン内、およびグローバル)、Junos OS セキュリティの基礎。

最新問題**: 21**
SRX シリーズ デバイスがコンテンツを識別する 2 つの方法は何ですか? (2 つ選択してください。)
A. 各ファイルのファイル拡張子を識別して検査します。
B. AppID を使用します。
C. HTTP、FTP、電子メール プロトコルのファイル タイプを識別します。
D. ALG を使用します。
Answer: B,C (メーッセージを残す**)**
SRXシリーズデバイスは、高度な識別メカニズムを活用したコンテンツセキュリティ機能を提供します。ファイルの識別は、ファイル拡張子（簡単に偽装できます）だけでなく、詳細な検査技術に基づいています。
* AppID（アプリケーション識別）AppIDはAppSecureスイートの一部であり、ポートやプロトコルに関係なく、デバイスがアプリケーションとコンテンツを分類できるようにします。これにより、SRXはアプリケーションとその関連コンテンツを検出し、適用することができます。
* プロトコルベースのファイルタイプ識別 :SRXは、HTTP、FTP、および電子メール （SMTP、IMAP、POP3）プロトコルに埋め込まれたファイルタイプを認識し、識別できます。これにより、ファイルの命名規則に左右されることなく、正確なコンテンツ検査とフィルタリングが可能になります。
* 他の人はなぜダメなのですか?
* ファイル拡張子 (オプション A) はコンテンツのセキュリティにとって信頼できないため、SRX では使用されません。
* ALG (オプション D) は、コンテンツの識別ではなく、SIP または FTP 制御チャネルなどのプロトコル処理に使用されます。
参考資料:Juniper Networks - コンテンツ セキュリティと AppSecure の概要、Junos OS セキュリティの基礎、公式コース ガイド。

最新問題**: 22**
SRX シリーズ ファイアウォールのインターフェイスに ping を実行できません。
この問題を解決するには、どの 2 つのアクションを実行する必要がありますか? (2 つ選択してください。)
A. インターフェイスをセキュリティ ゾーンに割り当てます。
B. ping トラフィックを許可するセキュリティ ポリシーを作成します。
C. インターフェイスをヌルゾーンに割り当てます。
D. ホスト受信トラフィックの ICMP プロトコルを設定します。
Answer: A,D (メーッセージを残す**)**
SRX ファイアウォール インターフェイスが ICMP ping などの管理トラフィックに応答するには、次の手順を実行します。
* インターフェースはセキュリティゾーンに割り当てられている必要があります （オプションA）。インターフェースがどのゾーンにも属していない場合、ヌルゾーンに配置され、すべてのトラフィックがドロップされます。
* さらに、ゾーンは管理トラフィックタイプとしてhost-inbound-traffic （オプションD）を許可するように設定する必要があります。ICMPの場合、そのゾーンのhost-inbound-trafficでプロトコルを明示的に許可する必要があります。
その他のオプション:

* セキュリティ ポリシー (オプション B) は、SRX デバイス自体宛てのトラフィックではなく、ファイアウォールを通過するトラフィックを制御します。
* インターフェイスをヌル ゾーンに割り当てると (オプション C)、管理を含むすべての通信が防止されます。
正しいアクション: インターフェイスをゾーンに割り当て、host-inbound-traffic で ICMP を設定します。
参考資料:Juniper Networks - ホストの受信トラフィックとゾーン構成、Junos OS セキュリティの基礎。

最新問題**: 23**
Junos OS で例外トラフィックをレート制限する目的は何ですか?
A. 転送プレーンのパフォーマンスを向上させる
B. ネットワークインターフェースの設定を簡素化する
C. ルーティングエンジンへのサービス拒否攻撃を防ぐため
D. ルーティングプロトコルとアップデートを管理する
Answer: C (メーッセージを残す**)**
例外トラフィックとは、ルーティング プロトコルの更新、管理トラフィック、その他のコントロール プレーン パケットなど、処理のためにパケット転送エンジン (PFE) からルーティング エンジン (RE) に送信する必要があるトラフィックです。
RE は限られた重要なリソースであるため、Junos OS は例外トラフィックに対してレート制限を実装します。
* 目的は、ルーティング エンジンに向けられるトラフィックの量を制御することにより、ルーティング エンジンに対するサービス拒否 (DoS) 攻撃を防ぐことです。
* これにより、潜在的な攻撃やトラフィック量の多い状況でも、RE がコントロール プレーン操作を継続的に確実に処理できるようになります。
* レート制限では、転送プレーンのパフォーマンスは向上しません (オプション A)、インターフェイス構成は簡素化されません (オプション B)、ルーティング プロトコルは直接管理されません (オプション D)。
参考:Juniper Networks - Junos OS セキュリティの基礎、例外トラフィック処理。