Juniper.JN0-335.v2024-05-15.q99

試験コード:	JN0-335
試験名称:	Security, Specialist (JNCIS-SEC)
認定資格:	Juniper
無料問題数:	99
バージョン:	v2024-05-15
アクセス数:	401
ページビュー数:	990
https://www.jpnpdf.com/Juniper.JN0-335.v2024-05-15.q99-mondaishu.html	

最新問題: **1**
統合セキュリティ ポリシーに関する 2 つの記述が正しいのはどれですか? (2つお選びください。)
A. 統合セキュリティ ポリシーには高度な機能ライセンスが必要です。
B. 統合セキュリティ ポリシーは、グローバル セキュリティ ポリシーの後に評価されます。
C. トラフィックは、最初は複数の統合セキュリティ ポリシーに一致する可能性があります。
D. APPID の結果は、最終的なセキュリティ ポリシーを決定するために使用されます。
Answer: C,D (メーッセージを残す)
統合セキュリティ ポリシーは、既存の 5 タプルまたは 6 タプルの一致条件とともに、動的アプリケーションを一致条件として使用できるようにするセキュリティ ポリシーです。これらは、レイヤー 7 でのアプリケーションベースのセキュリティ ポリシー管理を簡素化し、動的なアプリケーション トラフィックを管理するための優れた制御と拡張性を提供します。

最新問題: **2**
ユーザー ゾーンのホストからインターネット ゾーンのホストに向かうアプリケーション トラフィックを監視するために AppTrack を有効にするように求められます。
このシナリオでは、どの記述が真実ですか?
A. ユーザー ゾーンに関連付けられたインターフェイス構成内で AppTrack 機能を有効にする必要があります。
B. インターネット ゾーンに関連付けられたイングレス インターフェイス構成内で AppTrack 機能を有効にする必要があります。
C. ユーザー ゾーン設定内で AppTrack 機能を有効にする必要があります。
D. インターネット ゾーン構成内で AppTrack 機能を有効にする必要があります。
Answer: (解答を表示する)

最新問題: **3**
JSA データ収集に関して正しい 2 つの記述はどれですか? (2つお選びください。)

A. Event Collector は、BGP FlowSpec を使用して情報を収集します。
B. フロー コレクターは統計サンプリングを使用できます。
C. フロー コレクターはログを解析します。
D. Event Collector はログを解析します
Answer: (解答を表示する**)**
説明
Juniper Secure Analytics (JSA) は、ネットワーク デバイス、エンドポイント、アプリケーションからの監視データを統合、分析、管理するセキュリティ情報およびイベント管理 (SIEM) システムです。JSA は、イベント コレクターとフロー コレクター 1 の 2 種類のデータ コレクターを使用します。イベント コレクターは、ファイアウォール、ルーター、サーバー、侵入検出または防御システムなどのさまざまなログ ソースからログを収集し、解析します。Event Collector は、ログ データを共通形式に正規化し、さらなる分析と関連付けのために JSA コンソールに送信します。イベント コレクターは、syslog、SNMP、JDBC、SDEE12 などのログ収集用のさまざまなプロトコルをサポートします。フロー コレクターは、フローログ ファイル、NetFlow、J-Flow、sFlow、Packeteer などのさまざまなフロー ソースからネットワーク トラフィック データを収集して処理します。フロー コレクターは、アプリケーションの識別、位置情報、脅威インテリジェンスなどの追加情報を使用してフロー データを強化します。フロー コレクターは、さらなる分析と関連付けのためにフロー データを JSA コンソールに送信します。フロー コレクターは統計サンプリングを使用して、収集および処理されるフロー データの量を削減でき、システムのパフォーマンスとスケーラビリティを向上させることができます12。イベント コレクターは、BGP FlowSpec を使用して情報を収集しません。BGP FlowSpec は、イベントの配布を可能にするプロトコルです。BGP ピア間のトラフィック フロー仕様ルール。BGP FlowSpec は、JSA3 でサポートされているフロー ソースではありません。フロー コレクターは、ログ ソースによって生成されたネットワーク アクティビティのテキスト レコードであるログを解析しません。フロー コレクターは、フロー ソースによって生成されたネットワーク トラフィックのバイナリ レコードであるフロー データのみを処理します12。JSA 7.5.0 | ジュニパーネットワークス 2: データ収集 - TechLibrary - ジュニパーネットワークス 3: BGP FlowSpec について - TechLibrary - ジュニパーネットワークス

最新問題**: 4**
Juniper Identity Management Service (JIMS) がユーザー名とデバイスの IP アドレスを収集するために使用する 2 つのソースはどれですか? (2つお選びください。)
A. Microsoft Exchange Server イベント ログ
B. DNS
C. Active Directory ドメイン コントローラー イベント ログ
D. OpenLDAP サービス ポート
Answer: B,C (メーッセージを残す**)**
Juniper Identity Management Service (JIMS) は、DNS と Active Directory ドメイン コントローラーのイベント ログの両方からユーザー名とデバイスの IP アドレスを収集します。DNS はホス

ト名を IP アドレスに解決するために使用され、Active Directory ドメイン コントローラーのイベント ログはユーザー アカウントに関する情報 (最終ログイン日時など) を取得するために使用されます。

最新問題: **5**
ICMP および UDP トラフィックのデフォルトのセッション タイムアウト値は何ですか?
A. 30 秒
B. 30 分
C. 60 秒
D. 5 分
Answer: C (メーッセージを残す**)**

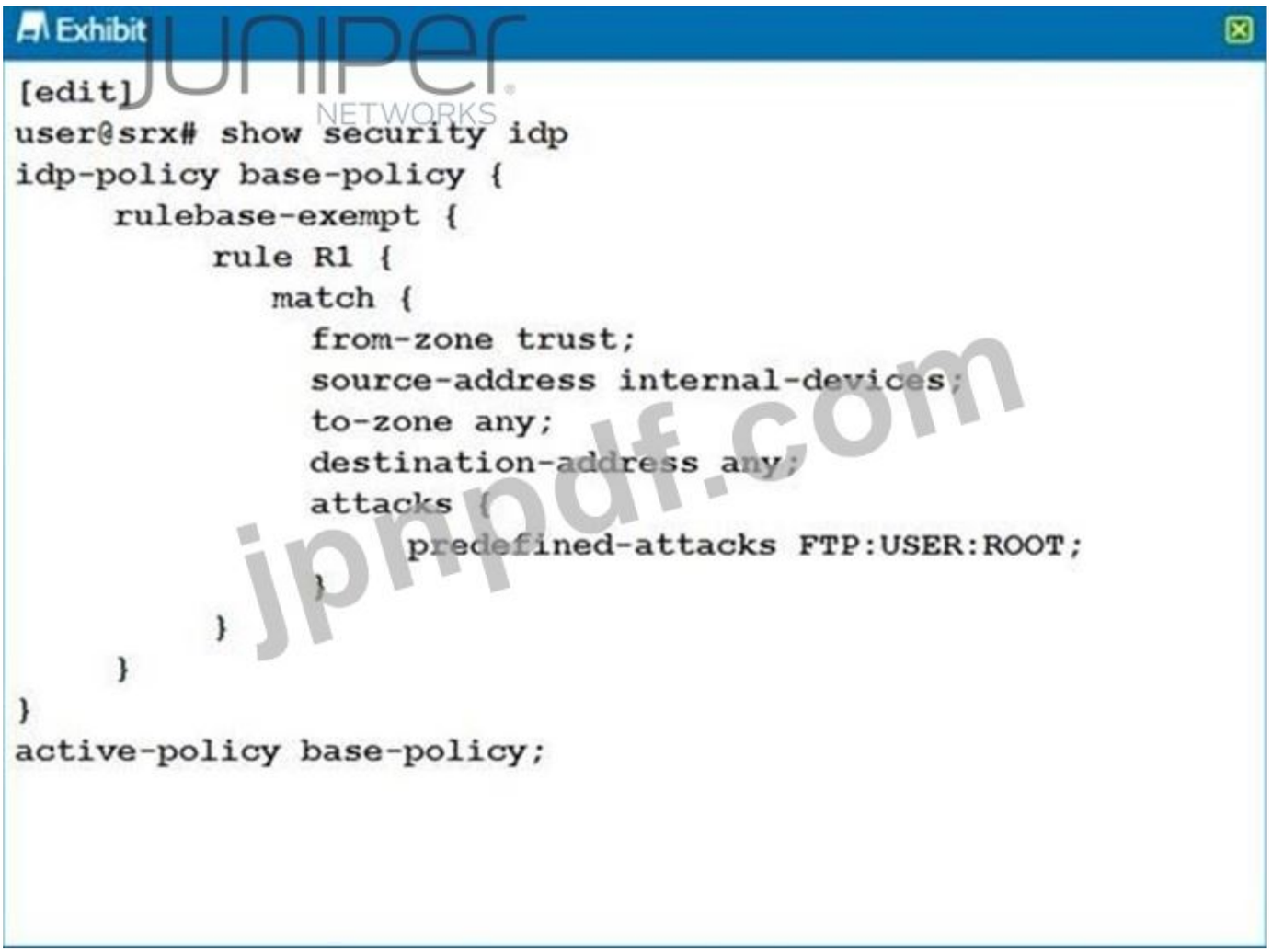
最新問題: **6**
IPS シグネチャを使用してトラフィックを監視したいと考えています。
AppSecure スイートのどのモジュールがこのタスクに役立ちますか?
A. AppTrack
B. アプリの QoS
C. AppFW
D. APPID
Answer: C (メーッセージを残す**)**
AppSecure スイートの AppFW モジュールは、トラフィックの監視と悪意のあるアクティビティの検出に使用できる IPS シグネチャを提供します。AppFW は、Web アプリケーション ファイアウォール、URL フィルタリング、アプリケーション レベルの可視性などの他のセキュリティ制御も提供します。

最新問題: **7**
Juniper Identity Management Service (JIMS) ドメイン PC プローブに関する次の記述はどれが真実ですか?
A. JIMS ドメイン PC プローブは、デフォルトでドメイン コントローラーのセキュリティ イベント ログを 60 ミュート間隔で分析します。
B. ドメイン セキュリティ イベント ログにユーザー名と IP アドレスのマッピングが見つからない場合、JIMS ドメイン PC プローブがトリガーされます。
C. JIMS ドメイン PC プローブがトリガーされ、ユーザー名をグループ メンバーシップ情報にマッピングします。
D. JIMS ドメイン PC プローブは、認証テーブル情報を確認するために SRX シリーズ デバイスによって開始されます。
Answer: (解答を表示する**)**
説明
JIMS ドメイン PC プローブは、顧客のドメイン内のデバイスからユーザー名と IP アドレスのマッピング情報を取得するメカニズムです。JIMS は、SRX シリーズ デバイスから、ドメイン セ

キュリティ イベント ログに見つからないユーザー名と IP アドレスのマッピングの要求を受信すると、ドメイン PC プローブを開始します。JIMS は、PC プローブ用に構成された管理資格情報を使用してデバイスにアクセスし、Windows Management Instrumentation (WMI) サービスにユーザー名と IP アドレスのマッピングを照会します12。
1: Juniper Identity Management サービス機能ガイド - TechLibrary - Juniper Networks
2: Juniper Identity Management Service (JIMS) ドキュメント - ジュニパーネットワークス

最新問題: **8**
SRX シリーズ高可用性クラスター ペアのプライマリ ルーティング エンジンを手動でフェイルオーバーしたいと考えています。
このタスクを達成するにはどの手順が必要ですか?
A. プライマリ ノードで setchassisclusterdisablereboot コマンドを発行します。
B. 優先順位を調整する前に、制御リンクの回復/ソリューションを実装します。
C. 手動でフェイルオーバーを要求し、セカンダリ ノードを識別します
D. セカンダリ ノードの構成で優先度を調整します。
Answer: (解答を表示する**)**
説明
SRX シリーズ高可用性クラスター ペアのプライマリ ルーティング エンジンを手動でフェールオーバーするには、プライマリ ノードで request ChassisClusterFailoverredundancy-groupgroup-idnodenode-id コマンドを発行する必要があります。ここで、group-id は冗長グループ番号です。また、node-id はセカンダリ ノードのノード番号です。
このコマンドは、指定された冗長グループのセカンダリ ノードへの正常なフェールオーバーを開始し、それを新しいプライマリ ノードにします。他のオプションは、このタスクには必要ないか、または正しくありません。オプション A では、シャーシ クラスタが無効になり、プライマリ ノードが再起動されますが、これは正常なフェールオーバーではありません。制御リンク回復ソリューションは、フェイルオーバーを開始するためではなく、ノード間の制御リンク接続を復元するために使用されるため、オプション B は関係ありません。オプション D では、セカンダリ ノードの優先順位が再起動または制御リンクの障害後にのみ有効になるため、フェイルオーバーはトリガーされません。参考文献:
シャーシクラスタ冗長グループの手動フェイルオーバー
シャーシクラスタの手動冗長グループフェイルオーバーの開始
SRX 入門 - 高可用性 (HA) のトラブルシューティング

最新問題: **9**
 展示」ボタンをクリックします。



展示物に関して、どの記述が真実ですか?

A. IDP はすべてのユーザーをブロックします。

B. IDP は root ユーザーをブロックします。

C. IDP は、一致したセッションの接続を無視します。

D. IDP は、一致したセッションの接続を閉じます。

Answer: C (メーッセージを残す**)**

最新問題**: 10**

vSRX がサポートされている 3 つのハイパーバイザーはどれですか? (3つお選びください。)

A. VMware ESXi

B. Citrix ハイパーバイザー

C. Hyper-V

D. KVM

E. Oracle VM

Answer: (解答を表示する**)**

説明

vSRX は、VMware ESXi、Microsoft Hyper-V、KVM などのさまざまなハイパーバイザー上で実行される仮想ファイアウォールです。vSRX は、仮想化環境の境界またはエッジでセキュリティおよびネットワーキング サービスを提供します。

vSRX は、Junos OS リリースと vSRX フレーバーに応じて、さまざまなバージョンの VMware ESXi、Hyper-V、および KVM をサポートします。Citrix Hypervisor および Oracle VM は、vSRX でサポートされているハイパーバイザーではありません。参考文献:
vSRX の概要
Microsoft Hyper-V を使用した vSRX について理解する
VMware 上の vSRX 仮想ファイアウォールの要件
Microsoft Hyper-V の vSRX 導入ガイド
vSRX シャーシ クラスター/vSRX の高可用性のサポート

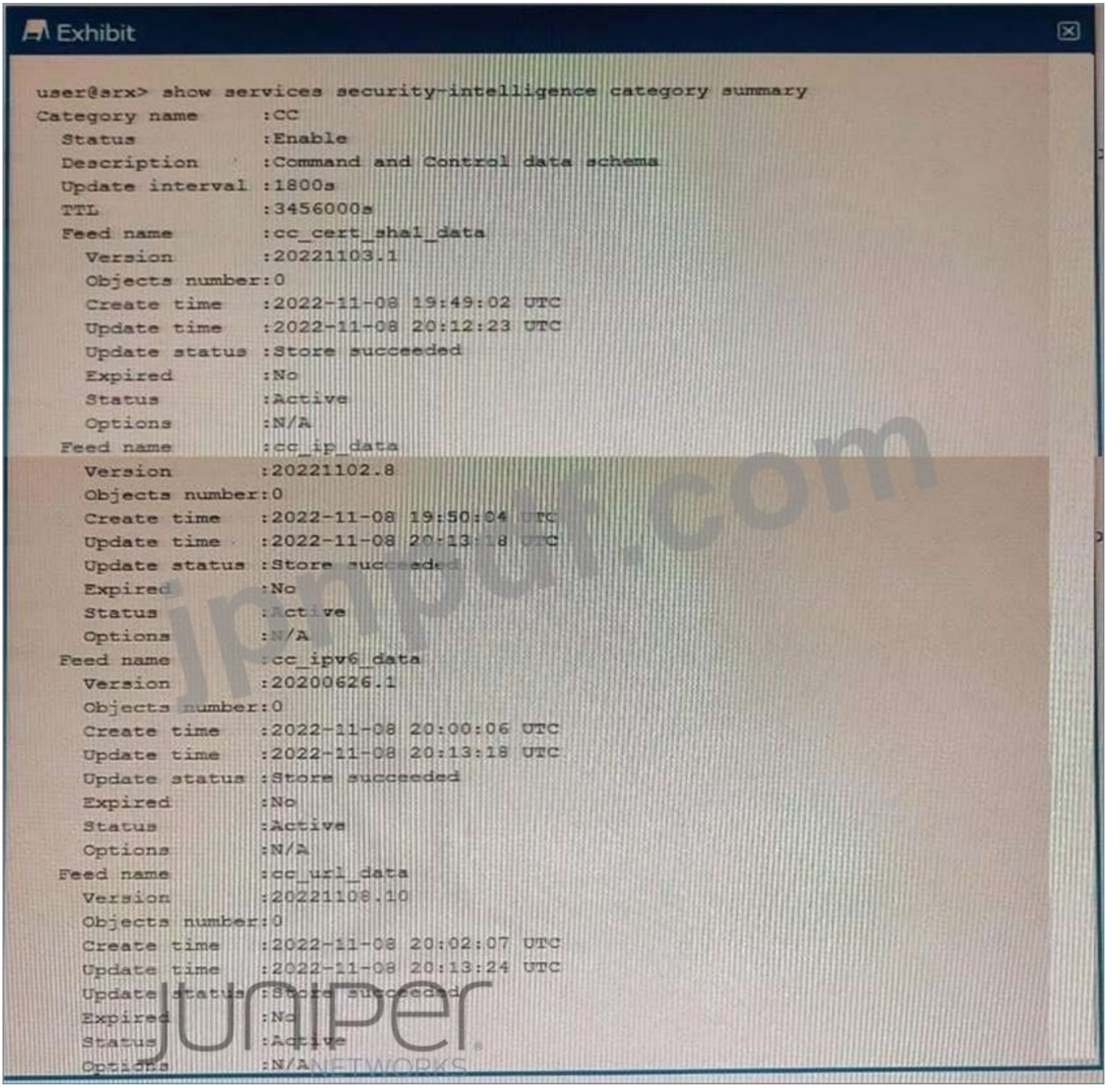
最新問題: **11**
JSA をデプロイしたので、ルール基準に一致するイベントとネットワーク アクティビティを表示する必要があります。このデータは単一のインターフェイスを使用して表示する必要があります。
このシナリオではどの JSA 機能を使用する必要がありますか?
A. ネットワークアクティビティ
B. 資産
C. オフェンスマネージャー
D. ログコレクター
Answer: (解答を表示する**)**

最新問題: **12**
JATP ソリューション アナライザーの .jar、.xls、および .doc ファイルが必要です。

展示を参照して、このタスクを実行するにはどの 2 つのファイル タイプを選択する必要がありますか? (2つお選びください。)

A. ライブラリ
B. 実行可能ファイル
C. Java
D. ドキュメント
Answer: A,D (メーッセージを残す**)**

最新問題**: 13**
展示する



Juniper ATP Cloud を使用したコマンド アンド コントロール (C&C) カテゴリのセットアップが完了しました。すべてのフィードにオブジェクトが含まれていないことがわかります。
このシナリオではどの記述が正しいでしょうか?

A. セキュリティ インテリジェンス ポリシーを構成する必要があります。統一されたセキュリティポリシーについて
B. commit full コマンドを使用してダウンロードを開始します。
C. アクションは必要ありません。フィードのダウンロードには数分かかります。
D. Juniper ATP Cloud GUI 内で最大 C&C エントリを設定します。
Answer: C (メーッセージを残す**)**
説明
Juniper ATP Cloud は、ジュニパーの顧客向けの脅威インテリジェンス ハブであり、ネットワーク上のユーザーとデバイスの侵害の兆候を特定します。コマンド アンド コントロール (C&C) や感染したホストなどのセキュリティ インテリジェンス フィードを提供し、悪意のあるトラフィックのブロックやログ記録に使用できます。Juniper ATP Cloud で C&C カテゴリを構成する場合は、認証トークン、URL、フィードの更新間隔を指定する必要があります。構成をコミットすると、フィードが Juniper ATP Cloud サーバーから自動的にダウンロードされます。ネットワークの遅延とフィードのサイズによっては、これには数分かかる場合があります。したがって、ユーザーによるアクションは必要なく、ダウンロードが完了すると、フィードにはゼロ以外のオブジェクトが含まれます。例に示すように、show services security Intelligence category summary コマンドを使用してフィードのステータスを確認できます。参考文献:
ジュニパー ATP クラウドの概要
セキュリティインテリジェンス (サービス)
Juniper ATP クラウド CLI リファレンス ガイド

最新問題**: 14**
展示」ボタンをクリックします。

```
user@srx> show configuration services
advanced-anti-malware {
  policy TPP {
    http {
      inspection-profile default profile;
      action block;
      notification {
        log;
      }
    }
    verdict-threshold 7;
    fallback-options {
      action permit;
      notification {
        log;
      }
    }
    default-notification {
        log;
    }
    whitelist-notification {
        log;
    }
    blacklist-notification {
        log;
    }
  }
}

user@srx> show configuration security policies
from-zone Client to-zone Internet {
  policy Rule-1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          advanced-anti-malware-policy TPP;
        }
      }
    }
  }
}
```


Sky ATP を展開してネットワークを攻撃から保護し、ユーザーが悪意のあるファイルをダウンロードできないようにしました。ただし、ユーザーが悪意のあるファイルをダウンロードしようとした後でも、SRX シリーズ デバイスを介して通信できます。

展示物に関して正しいのはどれですか?

A. 高度なマルウェア対策ポリシーの判定しきい値を下げます。

B. 高度なマルウェア対策ポリシーのフォールバック オプションを削除します。
C. セキュリティ インテリジェンス ポリシーを構成し、セキュリティ ポリシーに適用します。
D. セキュリティ ポリシーを標準セキュリティ ポリシーから統合セキュリティ ポリシーに変更します。
Answer: C (メーッセージを残す**)**

最新問題**: 15**
SRX シリーズ デバイス シャーシ クラスタに関する 3 つの記述のうち、正しいものはどれですか？ 3つお選びください。）
A. シャーシ クラスタ制御リンクは、RFC 1918 IP アドレスを使用して設定する必要があります。
B. シャーシ クラスタ メンバー デバイスは、制御リンクを使用して設定を同期します。
C. 制御リンク障害により、セカンダリ クラスタ ノードが無効になります。
D. 制御リンク障害から回復するには、セカンダリ メンバー デバイスを再起動する必要があります。
E. ハートビート メッセージは、シャーシ クラスタ制御リンクが動作していることを確認します。
Answer: B,C,E (メーッセージを残す**)**
説明
B: シャーシ クラスタ メンバー デバイスは、制御リンクを使用して設定を同期します。制御リンクは、シャーシ クラスタの 2 つのノード間で制御メッセージと構成情報を交換するために使用されます1。プライマリ ノードは設定をセカンダリ ノードにプッシュし、両方のノードが同じ設定になるようにします2。
C: 制御リンク障害により、セカンダリ クラスタ ノードが無効になります。制御リンクに障害が発生すると、プライマリ ノードはセカンダリ ノードと通信できなくなり、セカンダリ ノードがダウンしていると見なされます1。その後、プライマリ ノードがセカンダリ ノードを無効にし、すべてのトラフィック処理を引き継ぎます2。
E: ハートビート メッセージは、シャーシ クラスタ制御リンクが動作していることを確認します。制御リンクは、デフォルトで 2 つのノード間で 500 ミリ秒ごとに交換されるハートビート メッセージも伝送します1。ハートビート メッセージは、ノードと制御リンク 2 のステータスと正常性を示します。
A: シャーシ クラスタ制御リンクは、RFC 1918 IP アドレスを使用して設定する必要があります。これは虚偽の発言です。制御リンクは、クラスタ ノード上の他のインターフェイスまたはルートと競合しない限り、任意の IP アドレス範囲を使用できます1。RFC 1918 IP アドレスは、インターネット上でルーティングできないプライベート アドレスです4。
D: 制御リンク障害から回復するには、セカンダリ メンバー デバイスを再起動する必要があります。これも虚偽の発言です。制御リンク障害からの回復には、セカンダリ ノード 1 を再起動する必要はありません。制御リンクが復元され、構成が同期されると、セカンダリ ノードはクラスタに再参加できます2。
参考文献:
1: SRX シリーズ デバイスでのシャーシ クラスタリングの構成

2: SRX シリーズ デバイス用シャーシ クラスター ユーザー ガイド
3: SRX シリーズ ファイアウォールを接続してシャーシ クラスターを作成する
4: RFC 1918 - プライベート インターネットのアドレス割り当て
https://supportportal.juniper.net/s/article/SRX-Secondary-node-of-a-Chassis-Cluster-is-in-Disabled-state-how-do

最新問題: **16**
展示品に示されている構成に関して正しい 2 つの記述はどれですか? (2つお選びください。)

A. セッション テーブルの容量が 80% に達すると、積極的なエージングがトリガーされます。
B. セッションは、非アクティブ状態が 10 ミリ秒続いた後にセッション テーブルから削除されます。
C. セッション テーブルの容量が 95% に達すると、積極的なエージングがトリガーされます。
D. セッションは、非アクティブ状態が 10 秒続くとセッション テーブルから削除されます。
Answer: C,D (メーッセージを残す)

最新問題: **17**
展示」ボタンをクリックします。

JATP ソリューション アナライザーの .jar、.xls、および .doc ファイルが必要です。
展示を参照して、このタスクを実行するにはどの 2 つのファイル タイプを選択する必要がありますか? (2つお選びください。)

A. 実行可能ファイル
B. ライブラリ
C. ドキュメント
D. Java
Answer: C,D (メーッセージを残す**)**

最新問題**: 18**
ネットワークでは、ユーザーへの電子メールの送受信に使用されるリモート電子メール サーバーが使用されます。
このシナリオでは、電子メールを通じて悪意のあるファイルを受信しないようにユーザーを保護するには何をすべきでしょうか?

A. Sky ATP IMAP 電子メール保護を展開します。
B. Sky ATP SMTP 電子メール保護を展開します。
C. Sky ATP POP3 電子メール保護を展開します。
D. Sky ATP MAPI 電子メール保護を展開します。
Answer: B (メーッセージを残す**)**

最新問題**: 19**
展示する

```
user@srx> show security policies
Default policy: deny-all
Default policy log Profile ID: 0
Pre ID default policy: permit-all
From zone: Trust, To zone: Untrust
  Policy: BlockUbuntu, State: enabled, Index: 4, Scope Policy: 0, Sequence
number: 1, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: junos-defaults
    Dynamic Applications: junos:UBUNTU
    Source identity feeds: any
    Destination identity feeds: any
    Action: deny
  Policy: AllowWeb, State: enabled, Index: 9, Scope Policy: 0, Sequence
number: 2, Log Profile ID: 0
    Source vrf group: any
    Destination vrf group: any
    Source addresses: any
    Destination addresses: any
    Applications: junos-http, junos-https, junos-dns-udp
    Source identity feeds: any
    Destination identity feeds: any
    Action: permit
user@srx>
```


Ubuntu OS を実行しているサーバーのアクセスを SRX ファイアウォールでブロックすることで、自動的に更新できないようにするよう求められます。Blockuburrtu という名前の統合セキュリティ ポリシーを構成しましたが、OS の更新はブロックされていません。

展示を参照すると、Ubuntu OS のアップデートをブロックするステートメントはどれですか?

A. Blockubuntu ポリシーをAllowweb ポリシーの後に移動します。

B. junos-https アプリケーション パラメーターを使用して Blockubuntu ポリシーを構成します。

C. デフォルトのポリシーをpermit-allに変更します。

D. 任意の動的アプリケーションを持つように、Allowweb ポリシーを構成します。

Answer: (解答を表示する**)**

説明

参考文献:

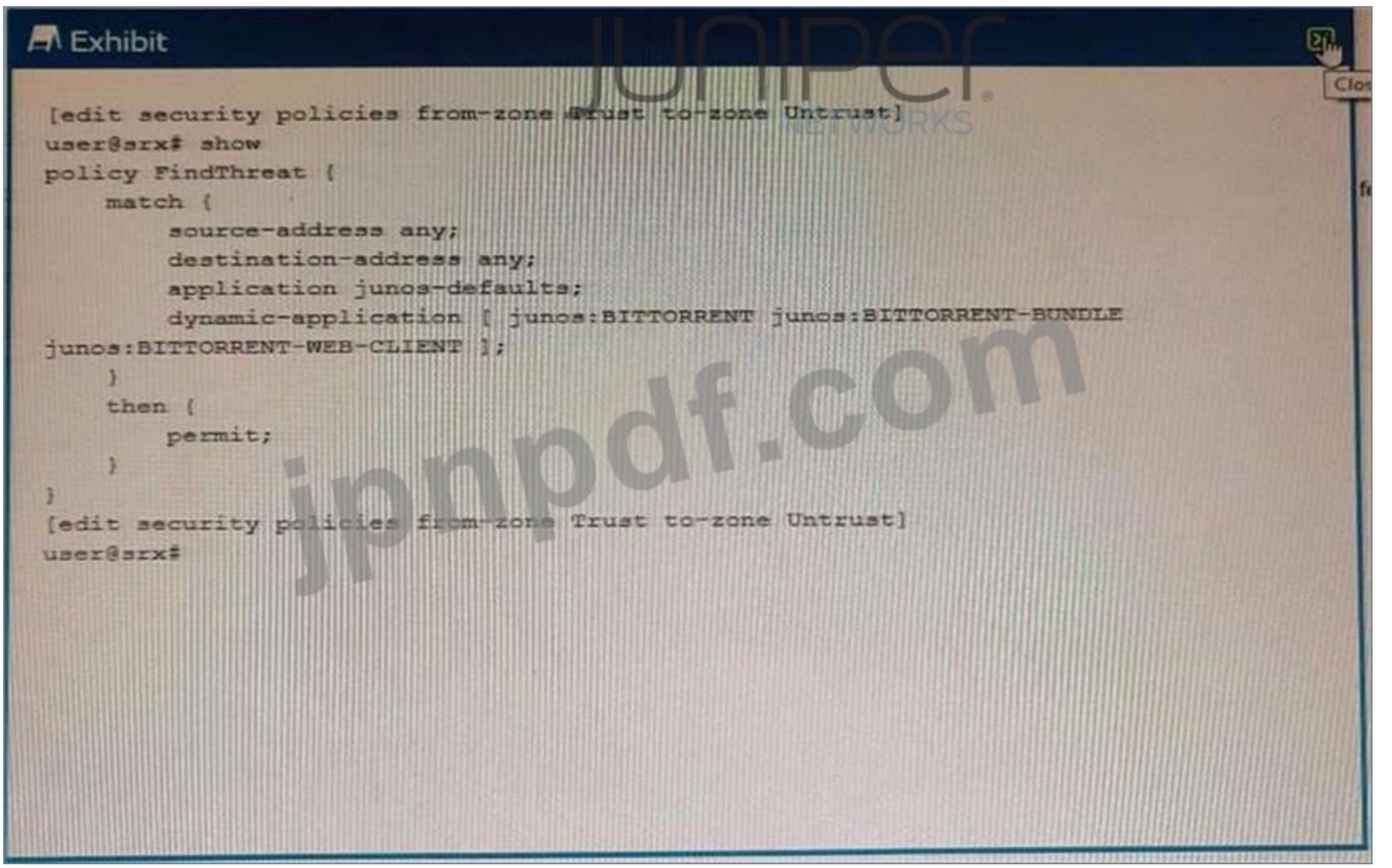
[Juniper Security, Professional (JNCIP-SEC) 参考資料] 1

[ジュニパー セキュリティ スペシャリスト (JNCIS-SEC) 参考資料] 2

[アプリケーション ファイアウォール (AppFW) を使用して特定の URL をブロックするカスタム シグネチャを設定する方法] 3

最新問題**: 20**

展示する



ネットワーク上の BitTorrent トラフィックを追跡するように求められます。将来の脅威を軽減するには、ワークステーションを High_Risk_Workstations フィードに、サーバーを BitTorrent_Servers フィードに自動的に追加する必要があります。

この機能を FindThreat ポリシーに追加する 2 つのコマンドはどれですか? (2つお選びください。)

A.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-ip-to-feed High_Risk_Workstations
```

B.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-identity-to-feed High_Risk_Workstations
```

C.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-identity-to-feed BitTorrent_Servers
```

D.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-ip-to-feed BitTorrent_Servers
```

Answer: B,C (メーッセージを残す)

説明

ネットワーク上の BitTorrent トラフィックを追跡するには、事前定義またはカスタム フィードに基づいてトラフィックにアクションを適用できるセキュリティ インテリジェンス機能を使用する必要があります。High_Risk_Workstations と BitTorrent_Servers は、特定の条件に一致するデバイスの IP アドレスを作成して設定できるカスタム フィードの例です。ワークステーションと

サーバーをそれぞれのフィードに自動的に追加するには、アプリケーション サービス セキュリティ インテリジェンス階層の下で管理フィード オプションを使用する必要があります。
このオプションは、フィード名と、フィードに一致するトラフィックに対して実行されるアクションを指定します。たとえば、ワークステーションを High_Risk_Workstations フィードに追加してトラフィックをドロップするには、次を使用します。
ゾーンからのセキュリティ ポリシーを設定します untrust ポリシー FindThreat その後、アプリケーション サービスのセキュリティ インテリジェンス管理フィードを許可します High_Risk_Workstations ドロップ サーバーを BitTorrent_Servers フィードに追加してトラフィックをログに記録するには、次のコマンドを使用します。
ゾーンからのセキュリティ ポリシーを設定します untrust ポリシー FindThreat から許可しますアプリケーション サービス セキュリティ インテリジェンス 管理フィード BitTorrent_Servers ログ オプション B およびオプション C は、これらのシナリオに適したコマンドを示します。オプション A とオプション D は、管理フィード オプションに間違った構文を使用しているため、正しくありません。また、フィードでは大文字と小文字が区別され、セキュリティ インテリジェンス階層で定義されたフィードと一致する必要があるため、間違ったフィード名も使用されます。参考資料: Juniper Security, Specialist (JNCIS-SEC) 参考資料および Juniper Security, Professional (JNCIP-SEC) 参考資料

最新問題: **21**
SRX5800 シャーシ クラスタでソフトウェア アップグレードを実行した後、node1 がプライマリ状態、node0 がバックアップ状態になっていることがわかります。ネットワーク標準では、node0 がプライマリ状態である必要があると規定されています。
このシナリオでは、ネットワーク標準に準拠するにはどのコマンドを使用する必要がありますか?
A. シャーシ クラスタ フェイルオーバー冗長性グループ 254 ノード 1 を要求します
B. シャーシ クラスタ フェイルオーバー冗長性のリクエスト - グループ 0 ノード 0
C. シャーシ クラスタ フェイルオーバー冗長グループ 254 モード 0 を要求します
D. シャーシ クラスター フェイルオーバー冗長性を要求します - グループ 0 ノード 1
Answer: B (メーッセージを残す**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-chassis-cluster-redundancy-group-failover.html

最新問題: **22**
仮想化された SRX を環境に展開したいと考えています。
このシナリオでは、なぜ cSRX ではなく vSRX を使用するのでしょうか? (2つお選びください。)
A. vSRX はレイヤー 2 およびレイヤー 3 構成をサポートします。
B. vSRX のみがクラスタリングを提供します。
C. vSRX の起動時間は速くなります。
D. vSRX のみが NAT、IPS、および UTM サービスを提供します
Answer: (解答を表示する**)**

vSRX はレイヤー 2 構成とレイヤー 3 構成の両方をサポートしますが、cSRX はレイヤー 3 構成に限定されます。さらに、vSRX は起動時間が短いため、特定のシナリオでは有利です。vSRX と cSRX は両方とも、NAT、IPS、および UTM サービスを提供します。

最新問題: **23**
新しい出力インターフェイスの選択を伴うルーティング変更が SRX シリーズ デバイスで発生します。
このシナリオでは、影響を受けるすべての現在のセッションに当てはまるのはどれですか?
A. 現在のセッションは破棄され、新しいルートに基づいて最初のパス処理が行われます。
B. 現在のセッションは、対応するセキュリティ ポリシーに基づいて変更される可能性があります。
C. 現在のセッションは変更されません。
D. 現在のセッションは、ポリシー再照合オプションが有効になっている場合にのみ破棄されます。
Answer: C (メーッセージを残す)

最新問題: **24**
展示」ボタンをクリックします。

```
user@srx> show chassis cluster status redundancy-group 1

Cluster: 1, Redundancy-Group: 1
    Device name                  Priority    Status    Preempt
 Manual failover
    node0                        0           Secondary No       No
    node1                        200         Primary   No       No
```


展示に示されている出力を説明する 2 つのステートメントはどれですか? (2つお選びください。)
A. 冗長グループ 1 で動作障害が発生しました。
B. 冗長グループ 1 は管理上フェイルオーバーされました。
C. ノード 0 は冗長グループ 1 のトラフィックを制御しています。
D. ノード 1 は冗長グループ 1 のトラフィックを制御しています。
Answer: B,D (メーッセージを残す)
この出力には、SRX シリーズ デバイス上のシャーシ クラスタ冗長グループ (RG) のステータスが表示されます。シャーシ クラスタ RG は、障害や手動介入が発生した場合に、あるノードから別のノードに一緒にフェールオーバーするインターフェイスやサービスなどのオブジェクトの集合です。シャーシ クラスタ RG は、いつでも 1 つのノードでプライマリとなり、別のノードでバックアップになることができます。展示に示されている出力を説明する 2 つのステートメントは次のとおりです。

冗長グループ 1 は管理的にフェイルオーバーされました。出力には、冗長グループ 1 の 手動フェイルオーバー」が 「はい」に設定されていることが示されています。これは、request ChassisClusterFailoverredundancy-group コマンドを使用して、冗長グループ 1 があるノードから別のノードに手動で切り替えられたことを示します。
ノード 1 は冗長グループ 1 のトラフィックを制御しています: 出力は、ノード 1 の冗長グループ 1 の 「ステータス」が 「プライマリ」に設定されていることを示しています。これは、ノード 1 がアクティブであり、冗長グループ 1 のトラフィックを制御していることを意味します。

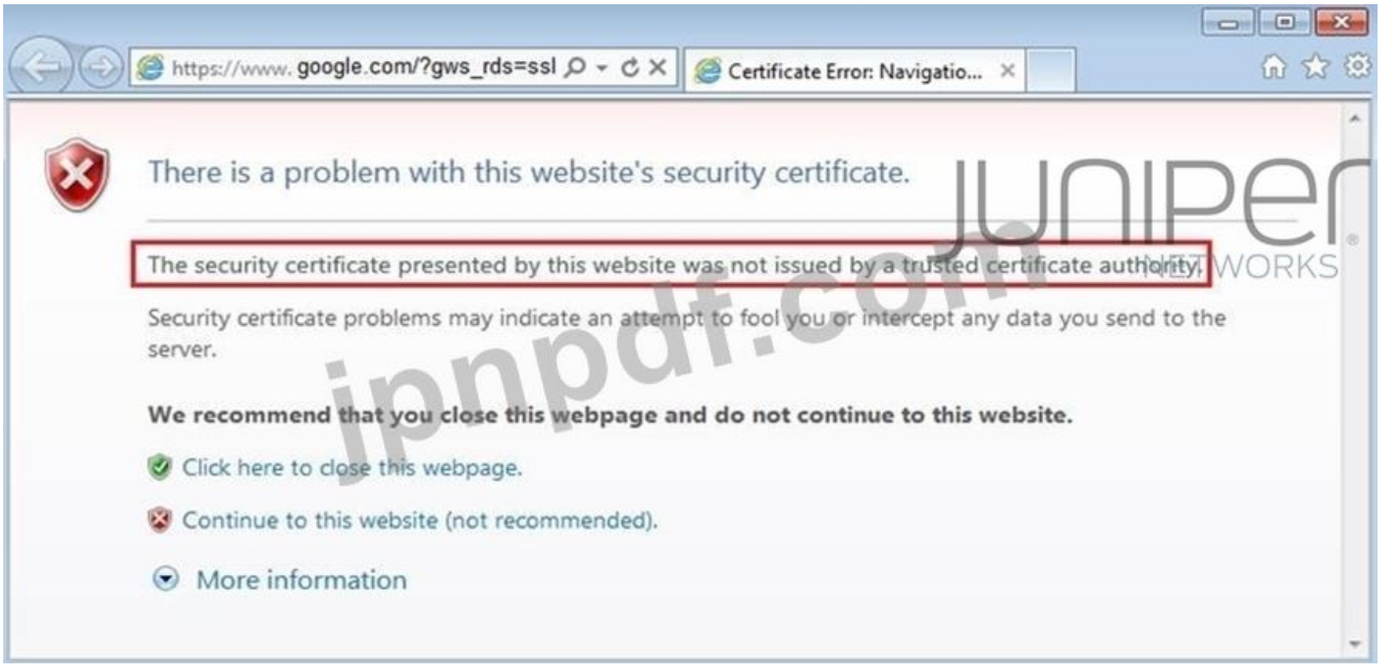
最新問題: **25**
Juniper Identity Management Service (JIMS) によって実行される 2 つの機能はどれですか? (2つお選びください。)
A. JIMS は、Active Directory 認証情報を信頼されていない Active Directory ドメイン コントローラーに複製します。
B. JIMS は Active Directory 認証情報を SRX シリーズ クライアント デバイスに転送します。
C. JIMS は、Active Directory ドメインから認証情報のデータベースを収集し、維持します。
D. JIMS は、プライマリ JIMS サーバーとセカンダリ JIMS サーバーの間で Active Directory 認証情報を同期します。
Answer: (解答を表示する**)**

最新問題: **26**
SRX5800 シャーシ クラスタでソフトウェア アップグレードを実行した後、node1 がプライマリ状態、node0 がバックアップ状態になっていることがわかります。ネットワーク標準では、node0 がプライマリ状態である必要があると規定されています。
このシナリオでは、ネットワーク標準に準拠するにはどのコマンドを使用する必要がありますか?
A. シャーシ クラスタ フェイルオーバー冗長性を要求します - グループ 0 ノード 1
B. シャーシ クラスタ フェイルオーバー冗長グループ 254 モード 0 を要求します
C. シャーシ クラスタ フェイルオーバー冗長性グループ 254 ノード 1 を要求します
D. シャーシ クラスタ フェイルオーバー冗長性のリクエスト - グループ 0 ノード 0
Answer: (解答を表示する**)**

最新問題: **27**
JATP 事件について正しいのはどれですか?
A. インシデントには、関連付けられた脅威番号が割り当てられています。
B. インシデントは、単一の脅威に関連するすべてのイベントで構成されます。
C. インシデントは常に自動的に軽減されます。
D. インシデントはカテゴリ、次に重大度によって並べ替えられます。
Answer: (解答を表示する**)**

最新問題: **28**

SSL プロキシ クライアント保護が実装されました。この機能を実装した後、ユーザーは展示に表示される警告メッセージについて苦情を言うようになります。



警告メッセージを消去するにはどのアクションを実行する必要がありますか?

A. SRX 自己署名 CA 証明書を再生成し、正しい組織名を含めます。

B. クライアント Web ブラウザで SRX シリーズ デバイスを信頼済みサイトとして構成します。

C. SRX 自己署名 CA 証明書を SRX 証明書パブリック ストアにインポートします。

D. SRX 自己署名 CA 証明書をクライアント Web ブラウザにインポートします。

Answer: (解答を表示する**)**

最新問題**: 29**

SRX シリーズ ファイアウォール上で、暗号化トラフィック インサイトがトラフィックの脅威を評価する 2 つの方法は何ですか? (2つお選びください。)

A. サンドボックスでファイルを復号化します。

B. 使用される証明書を検証します。

C. データを復号化してハッシュを検証します。

D. 接続のタイミングと頻度を確認します。

Answer: (解答を表示する**)**

Encrypted Traffic Insights は、SRX シリーズ ファイアウォールと ATP クラウドが、暗号化されたトラフィックに隠れている悪意のある脅威を、トラフィックを復号化することなく検出できるようにする機能です。これは、暗号化されたセッションのメタデータと接続パターンを分析することによって行われます。Encrypted Traffic Insights がトラフィックの脅威を評価する 2 つの方法は次のとおりです。

使用される証明書を検証します。SRX シリーズ ファイアウォールは、暗号化されたセッションからサーバー証明書を抽出し、その署名を ATP クラウドによって提供される既知の悪意のある証明書のブロックリストと比較します。一致する場合、セッションはブロックされ、脅威として報告されます。

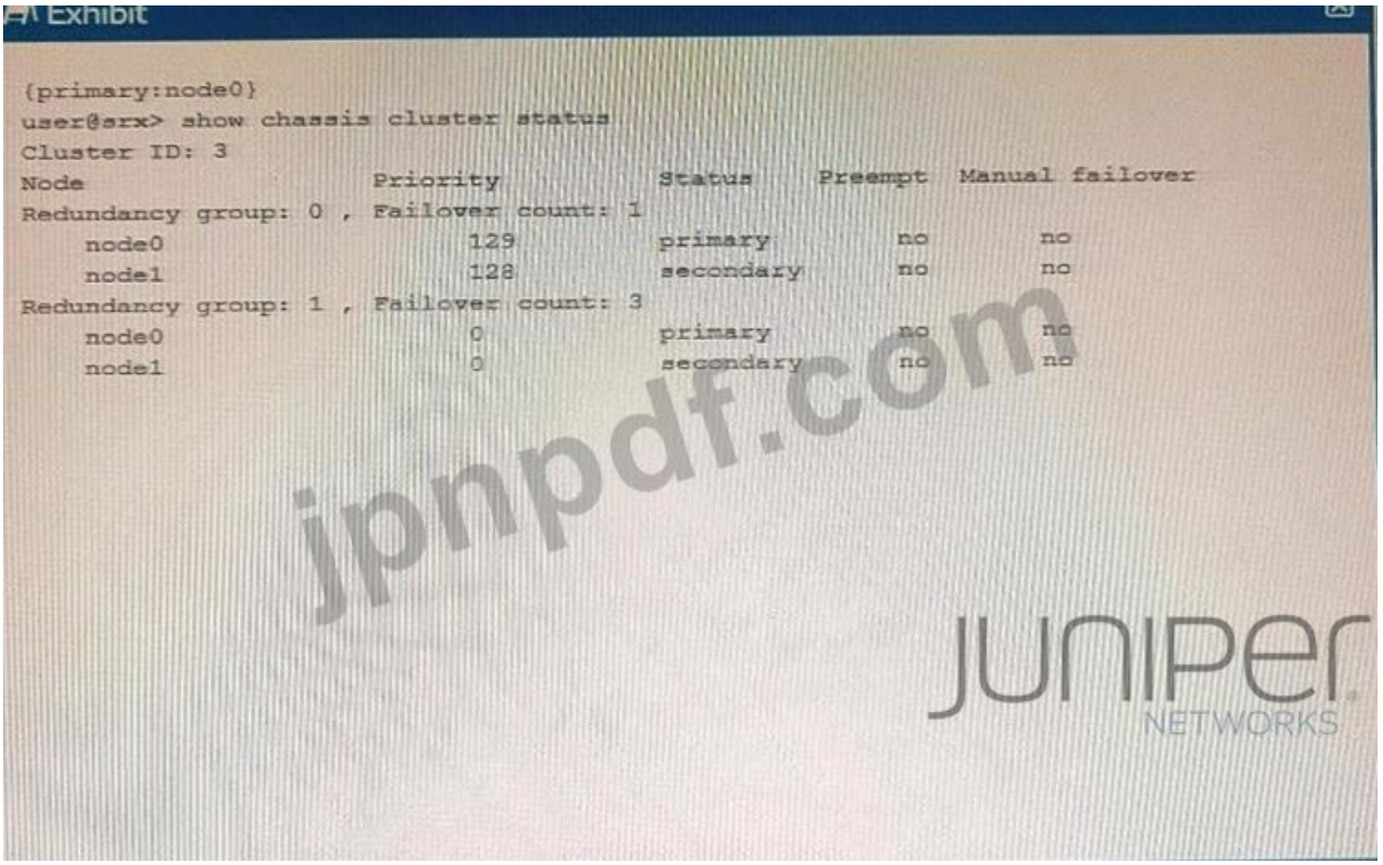
接続のタイミングと頻度を確認します。SRX シリーズ ファイアウォールは、送信元および宛先の IP アドレス、ポート、プロトコル、タイムスタンプなどの接続の詳細を ATP クラウドに送信します。ATP クラウドは、動作分析と機械学習アルゴリズムを適用して、高頻度、短い継続時間、異常なタイミングなどの異常または疑わしい接続パターンを検出します。

最新問題: **30**
AppSecure の AppQoE モジュールはどの機能を提供しますか?
A. AppQoE モジュールは、アプリケーションベースのルーティングを提供します。
B. AppQoE モジュールは、ネットワーク状態に基づいてルーティングを提供します。
C. AppQoE モジュールは、危険なアプリケーションへのアクセスをブロックします。
D. AppQoE モジュールは重要なアプリケーションを優先します。
Answer: (解答を表示する**)**

最新問題: **31**
AppQoE を有効にするための 2 つの要件は何ですか? (2つお選びください。)
A. 2 つの SRX シリーズ デバイス エンドポイントが必要です。
B. 2 つの SRX シリーズまたは MX シリーズ デバイス エンドポイントが必要です。
C. APPID 機能ライセンスが必要です。
D. 逆トラフィック用に AppQoE を構成する必要があります。
Answer: (解答を表示する**)**
AppQoE は、ネットワーク上のアプリケーションのエクスペリエンスの品質を監視し、最適化できる機能です。アプリケーション認識ルーティングと動的パス選択を使用して、事前定義またはカスタムの SLA プロファイルに基づいて各アプリケーションに最適なパスを選択します。AppQoE は、アプリケーションのパフォーマンスとネットワークの状態に関する可視性とレポートも提供します。AppQoE を有効にするための 2 つの要件は次のとおりです。
2 つの SRX シリーズまたは MX シリーズ デバイス エンドポイントが必要です。AppQoE は、2 つの SRX シリーズ デバイス エンドポイント間、またはハブ アンド スポークまたはフル メッシュトポロジの SRX シリーズ デバイスと MX シリーズ デバイス間で構成できます。デバイスは同じバージョンの Junos OS を実行し、同じ AppQoE 構成を持つ必要があります。
APPID 機能ライセンスが必要です: AppQoE では、SRX シリーズ デバイスに APPID 機能ライセンスがインストールされている必要があります。APPID 機能ライセンスにより、AppQoE が機能するために不可欠なアプリケーションの識別と分類が可能になります。

最新問題: 32

展示する



展示品からの情報を使用して、どの記述が正しいでしょうか?

A. 冗長グループ 1 は不適格な状態です。

B. Node1 はコントロール プレーンのアクティブ ノードです

C. クラスターに問題はありません。

D. 冗長グループ 0 は不適格な状態です。

Answer: B (メーッセージを残す)

説明

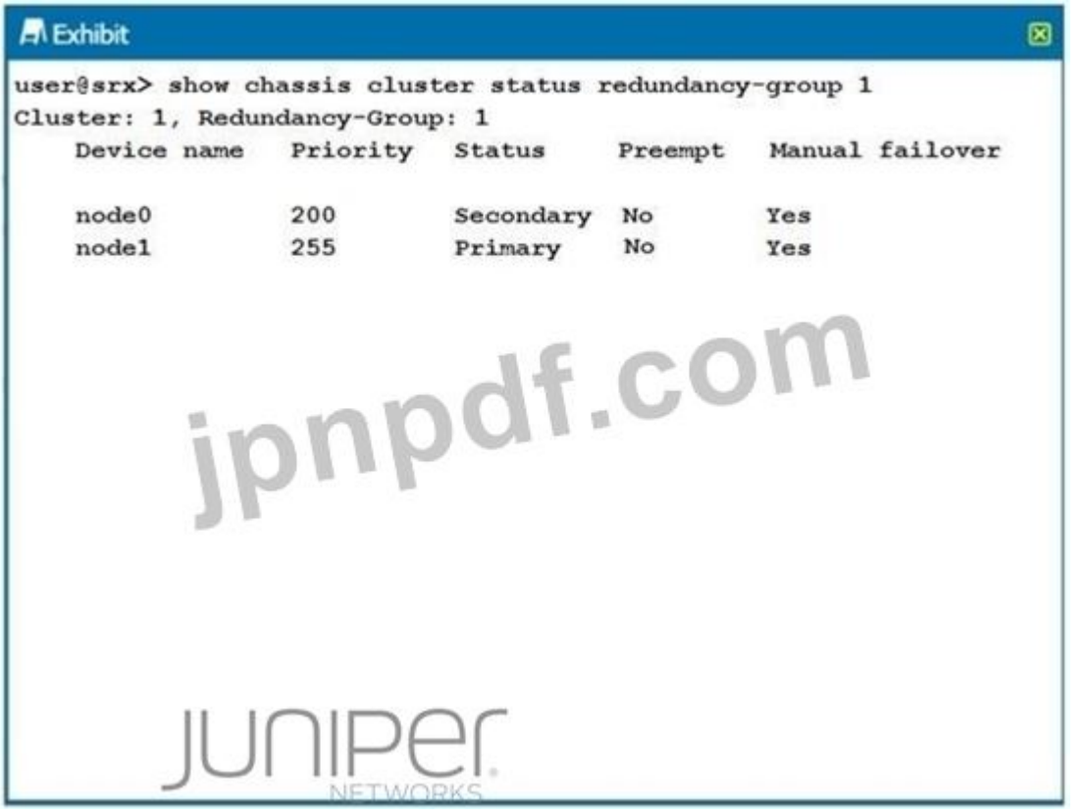
展示の情報によると、node0 は冗長グループ 0 (RG0) と冗長グループ 1 (RG1) の両方のプライマリ ノードです。RG0 は、ルーティング エンジンと管理インターフェイスを含むコントロール プレーンを担当します。RG1 は、インターフェイスとサービスを含むデータ プレーンを担当します。したがって、node0 がデータ プレーンのアクティブ ノードとなり、node1 がコントロール プレーンのアクティブ ノードになります34。

シャーシ クラスタ冗長グループ | Junos OS | ジュニパーネットワークス

SRX シャーシ クラスターでフェールオーバーしない冗長グループのトラブルシューティング | Junos OS | ジュニパーネットワークス シャーシ クラスター冗長性グループ 0 について: ルーティング エンジン | ジュニパーネットワークス Junos OS | ジュニパーネットワークス シャーシ クラスター冗長グループ 1 ～ 128 について | Junos OS | ジュニパーネットワークス

最新問題: **33**
セッション テーブル上のスペースを管理するために使用される 2 つのセッション パラメーターはどれですか? (2つお選びください。)
A. TCP RST
B. 最低水準点
C. 最高水準点
D. TCP MSS
Answer: B,C (メーッセージを残す**)**

最新問題: **34**
展示に示されている出力を説明する 2 つのステートメントはどれですか? (2つお選びください。)



A. 冗長グループ 1 は管理上フェイルオーバーされました。
B. 冗長グループ 1 で動作障害が発生しました。
C. ノード 0 は冗長グループ 1 のトラフィックを渡しています。
D. ノード 1 は冗長グループ 1 のトラフィックを渡しています。
Answer: (解答を表示する**)**

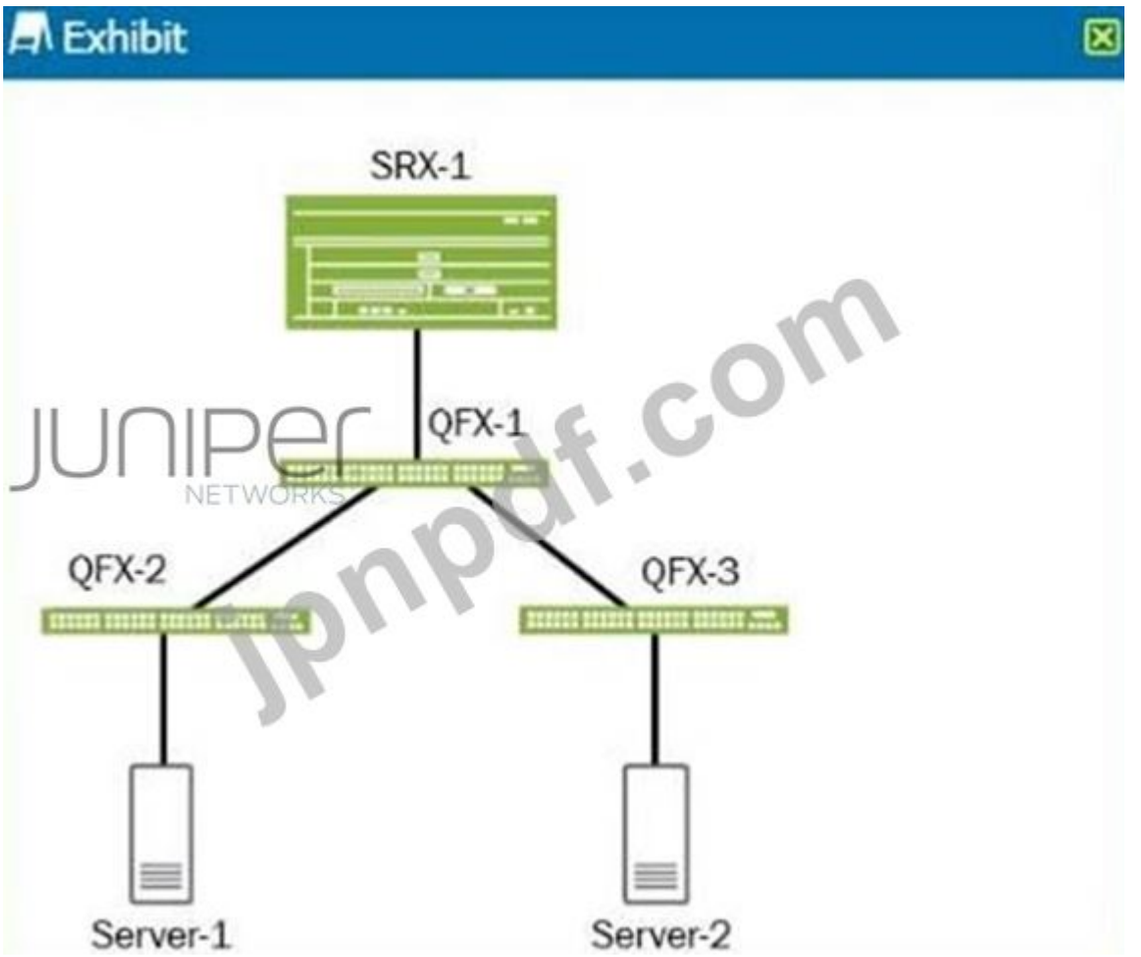
最新問題: **35**
これで、出力インターフェイスと同じサブネット内のアドレスのプールを使用してソース NAT が構成されました。プール内のアドレスを使用できるようにするには、他に何を構成する必要がありますか?
A. アドレスの永続性

B. 宛先 NAT
C. プロキシ ARP
D. 静的 NAT
Answer: C (メーッセージを残す**)**

最新問題**: 36**
AppSecure の AppTrack モジュールについて説明しているのはどれですか?
A. AppTrack モジュールは、特定のアプリケーションに基づいてトラフィックをブロックする機能を提供します。
B. AppTrack モジュールは、アプリケーションに基づいてトラフィックのルーティングによる制御を提供します。
C. AppTrack モジュールは、ネットワーク上のアプリケーションの使用状況を可視化し、ボリュームレポートを提供します。
D. AppTrack モジュールは、ネットワーク トラフィックに存在するアプリケーションを識別します。
Answer: (解答を表示する**)**

最新問題**: 37**
IoT セキュリティ機能は、IoT デバイスからのトラフィックを識別するためにどの方法を使用しますか?
A. SRX シリーズ デバイスは、LOT デバイスのトランジット トラフィックからジュニパー ATP クラウドにメタデータをストリーミングします。
B. SRX シリーズ デバイスは、IoT デバイスから受信したトランジット トラフィックをジュニパー ATP クラウドにストリーミングします。
C. SRX シリーズ デバイスは、MAC アドレスを使用して LOT デバイスを識別します。
D. SRX シリーズ デバイスは、トランジット トラフィックから抽出されたメタデータから LOT デバイスを識別します。
Answer: A (メーッセージを残す**)**
説明
https://www.juniper.net/documentation/us/en/software/junos/security-iot/topics/topic-map/security-iot-overview。
SRX は IoT デバイスを識別しません。メタデータが Juniper ATP クラウドにストリーミングされ、Junipe ATP クラウドがデバイスを識別します。

最新問題**: 38**
「展示」ボタンをクリックします。



展示物を参照すると、Policy Enforcer を備えたセキュア ファブリック サイトの一部とみなされる 2 つのデバイスはどれですか? (2つお選びください。)

A. サーバー-2

B. サーバー-1

C. QFX-1

D. SRX-1

Answer: C,D (メーッセージを残す**)**

最新問題**: 39**

新しい出力インターフェイスの選択を伴うルーティング変更が SRX シリーズ デバイスで発生します。

このシナリオでは、影響を受けるすべての現在のセッションに当てはまるのはどれですか?

A. 現在のセッションは、対応するセキュリティ ポリシーに基づいて変更される可能性があります。

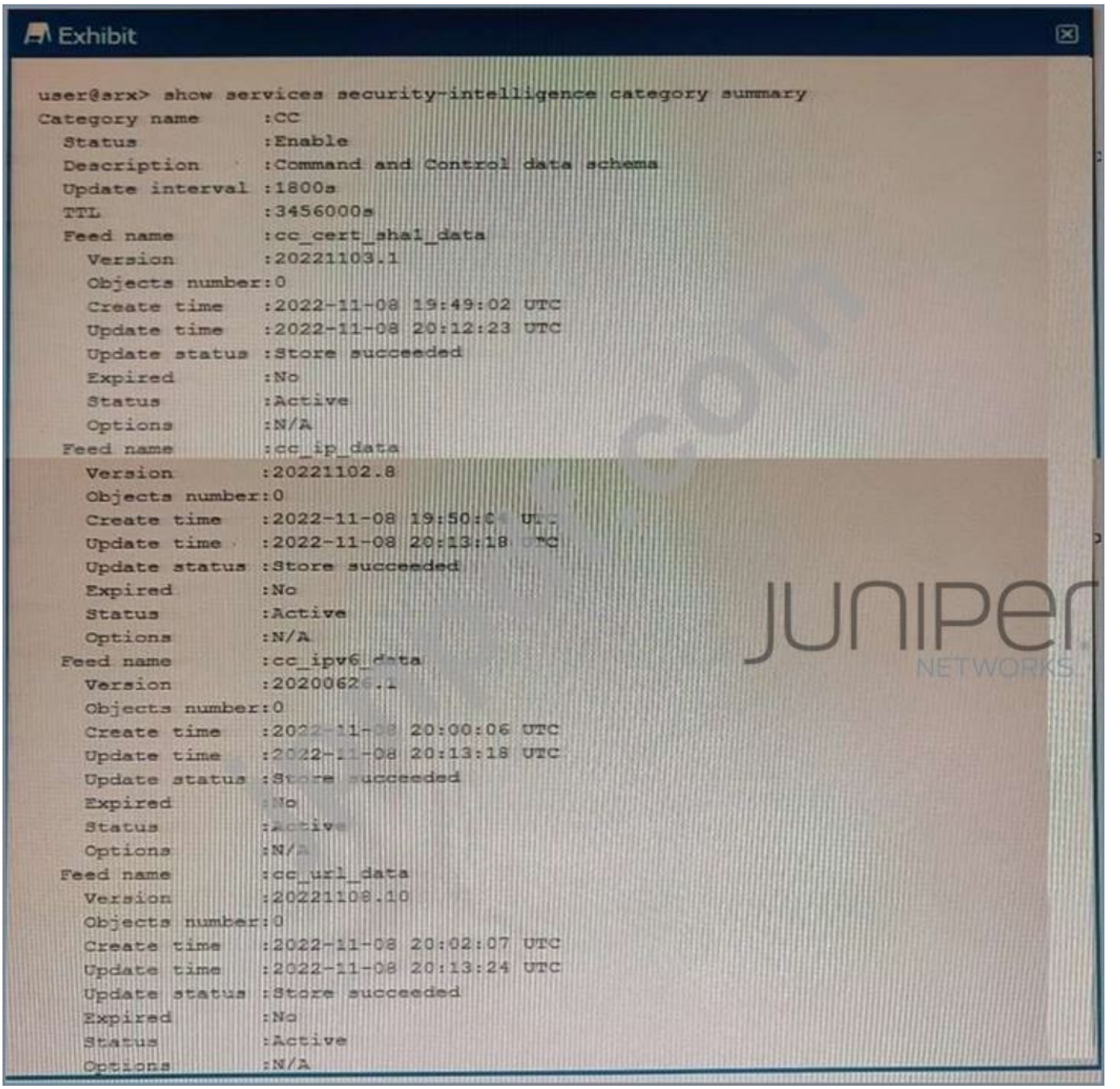
B. 現在のセッションは変更されません。

C. 現在のセッションは、ポリシー再照合オプションが有効になっている場合にのみ破棄されます。

D. 現在のセッションは破棄され、新しいルートに基づいて最初のパス処理が行われます。

Answer: (解答を表示する**)**

最新問題: **40**
展示する



Juniper ATP Cloud を使用したコマンド アンド コントロール (C&C) カテゴリのセットアップが完了しました。すべてのフィードにオブジェクトが含まれていないことがわかります。
このシナリオではどの記述が正しいでしょうか?

A. セキュリティ インテリジェンス ポリシーを構成する必要があります。統一されたセキュリティポリシーについて

B. commit full コマンドを使用してダウンロードを開始します。

C. アクションは必要ありません。フィードのダウンロードには数分かかります。

D. Juniper ATP Cloud GUI 内で最大 C&C エントリを設定します。

Answer: C (メーッセージを残す**)**

Juniper Networks JNCIS-SEC Study Guide によると、Juniper ATP Cloud でコマンド アンド コントロール (C&C) カテゴリを設定すると、最初はすべてのフィードにオブジェクトが含まれません。フィードのダウンロードには数分かかる場合があるため、これは正常な動作です。このシナリオではアクションは必要ありません。ダウンロードが完了すると、フィードにオブジェクトが取り込まれ始めることがわかります。

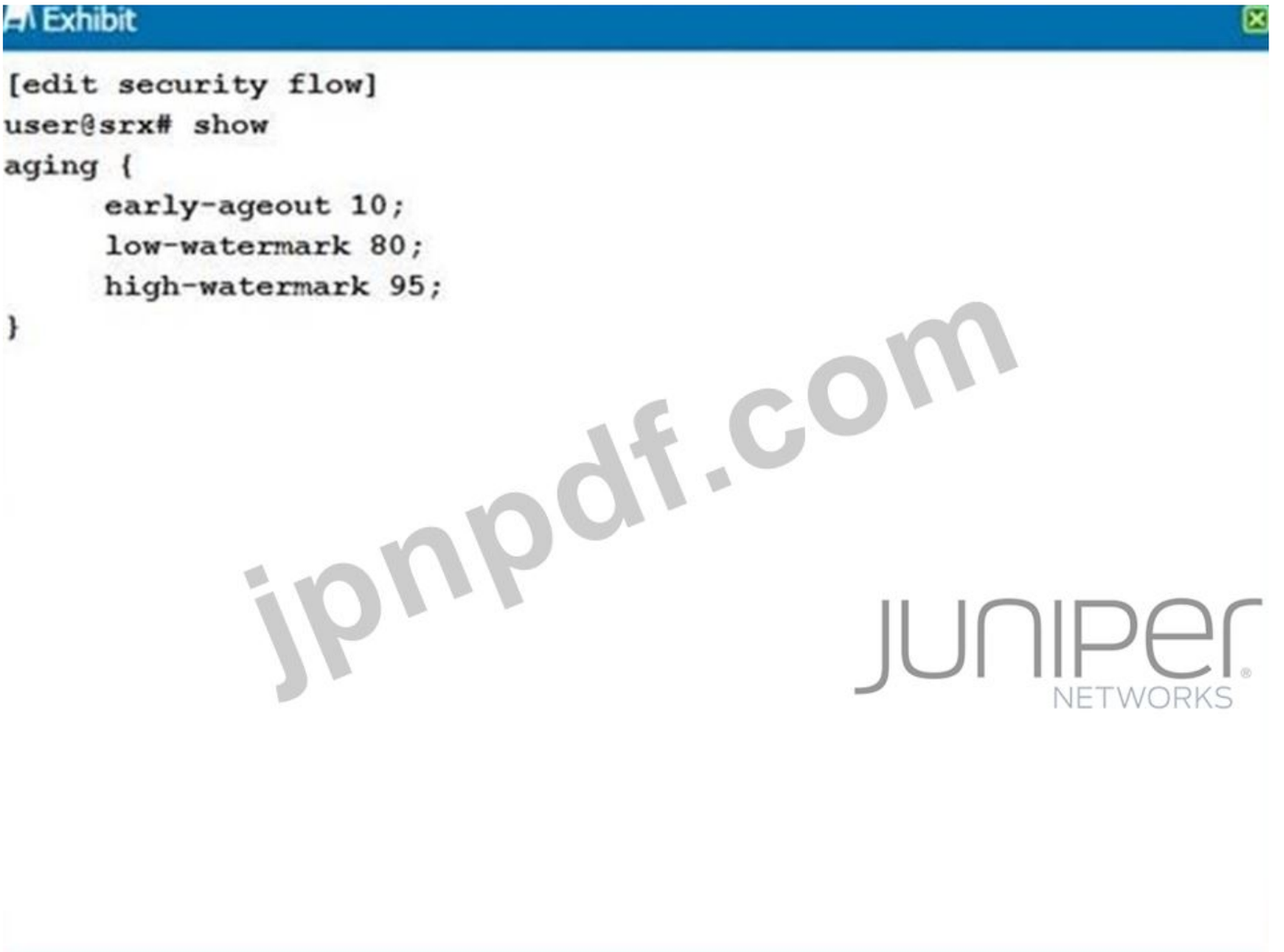
最新問題: **41**
管理対象セッションを考慮する場合、早期エージアウト機能を実装するためにセッション テーブルがどの程度満たされていなければならないかを決定する設定パラメータはどれですか?
A. 高いウェアマーク
B. 最低水準点
C. ポリシーの再照合
D. セッションサービスタイムアウト
Answer: A (メーッセージを残す**)**

最新問題: **42**
JIMS サーバーがユーザーに与える負荷を軽減するように求められます。この状況ではどのアクションを実行する必要がありますか?
A. JIMS を RADIUS サーバーに接続します
B. JIMS をドメイン Exchange サーバーに接続します
C. JIMS をドメイン SQL サーバーに接続します。
D. JIMS を別の SRX シリーズ デバイスに接続します。
Answer: (解答を表示する**)**
説明
JIMS は、ドメイン コントローラーまたは Exchange サーバー上のイベント ログを使用して、ログオン イベントを判断します。したがって、ドメイン コントローラーの負荷を軽減するには、Exchange サーバーを使用してログを読み取ることができます。
参考文献:
Juniper Identity Management サービス (JIMS) のドキュメント
Juniper Identity Management サービス ユーザー ガイド
概要 | ジム | ジュニパーネットワークス
ジュニパー - 試験ブースト
Juniper Identity Management サービスの概要

最新問題: **43**
クライアント保護 SSL プロキシ プロファイルを構成しています。
このシナリオではどの記述が正しいでしょうか?
A. サーバー証明書とルート認証局は使用されません。
B. サーバー証明書が使用されますが、ルート認証局は使用されません。
C. サーバー証明書は使用されませんが、ルート認証局が使用されます。

D. サーバー証明書とルート認証局の両方が使用されます。
Answer: D (メーッセージを残す**)**

最新問題**: 44**
展示」ボタンをクリックします。



展示品に示されている構成に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. セッション テーブルの容量が 80% に達すると、積極的なエージングがトリガーされます。
B. セッションは、非アクティブ状態が 10 秒続くとセッション テーブルから削除されます。
C. セッションは、非アクティブ状態が 10 ミリ秒続いた後にセッション テーブルから削除されます。
D. セッション テーブルの容量が 95% に達すると、積極的なエージングがトリガーされます。
Answer: B,D (メーッセージを残す**)**

最新問題**: 45**
ソフトウェア デファインド ネットワークで vSRX を使用する 2 つの利点は何ですか? (2つお選びください。)
A. スケーラビリティ
B. ソフトウェア ライセンスは必要ありません

C. きめ細かいセキュリティ
D. インターフェースの数は無限です
Answer: A,C (メーッセージを残す**)**
説明
= vSRX は、物理 SRX シリーズ ファイアウォールと同じ機能を提供する仮想ファイアウォールですが、ネットワーク需要に合わせて拡張するセキュリティ サービスを提供するための仮想化フォーム ファクターを備えています。vSRX は、Juniper Contrail Networking とサードパーティの Software-Defined Networking (SDN) ソリューションをサポートしており、動的で自動化されたネットワーク プロビジョニングと管理を可能にします。vSRX は、OpenStack などのクラウド オーケストレーション ツールとも統合されており、仮想マシンとネットワークの柔軟な導入と構成が可能になります。vSRX は、パブリック クラウドまたはプライベート クラウド上の仮想ネットワーク内で実行されるワークロードに対してきめ細かいセキュリティを提供します。アプリケーション セキュリティ、侵入防止、ユーザー ID、ロールベースのアクセス制御などの次世代ファイアウォール機能をサポートします。また、マルウェア サンドボックス、脅威インテリジェンス フィード、暗号化トラフィック検査などの高度な脅威防御機能もサポートしています。
vSRX は、内部と外部の両方の脅威からネットワークを保護し、ネットワーク全体に一貫したセキュリティ ポリシーを適用できます。参考文献:
vSRX 仮想ファイアウォール | ジュニパーネットワークス米国
vSRX ドキュメント | ジュニパーネットワークス
Microsoft Azure クラウドを使用した vSRX 仮想ファイアウォールを理解する

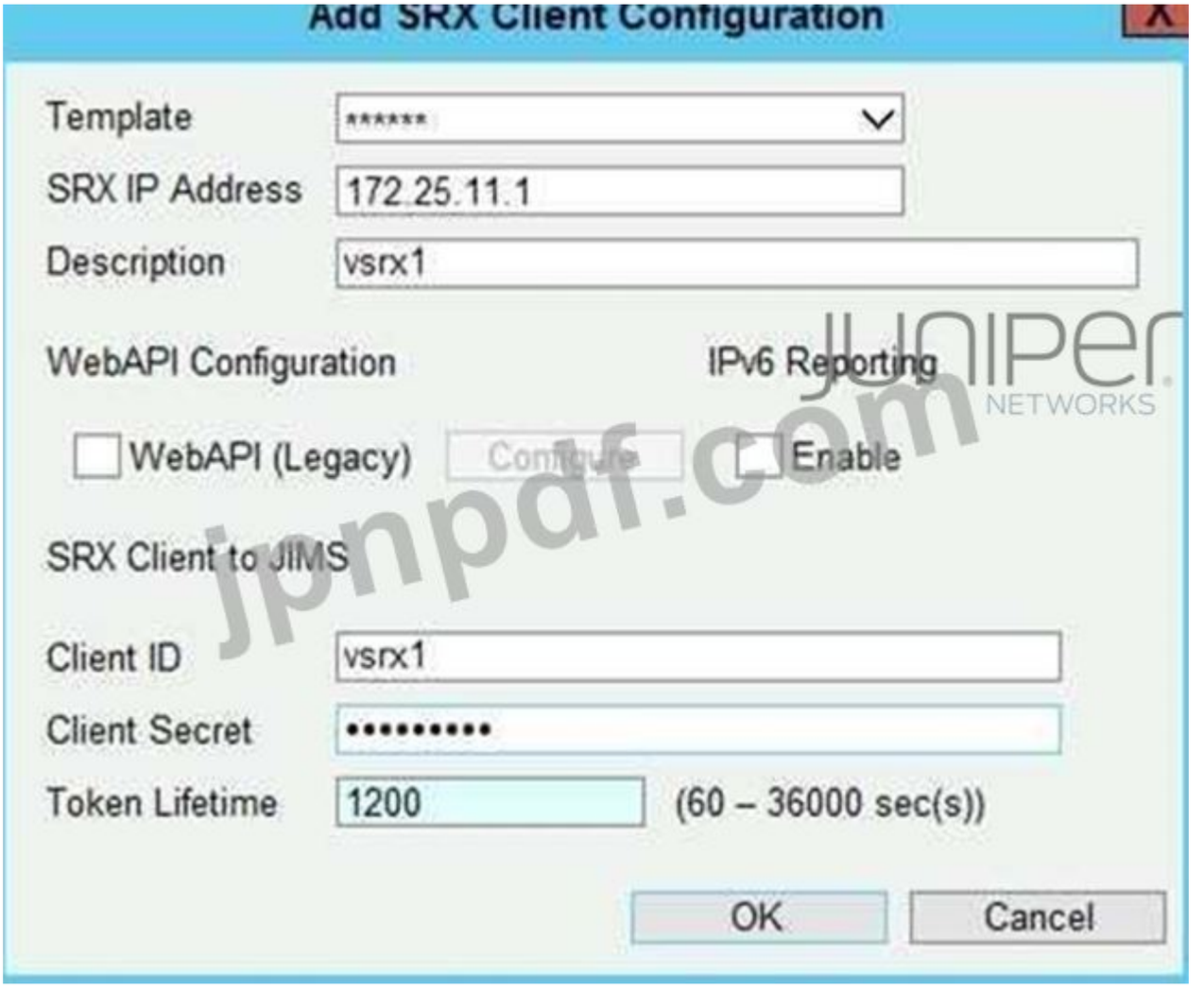
最新問題**: 46**
JIMS サーバーはイベント ログを表示できません。
この問題を解決するには、どの 2 つのアクションを取りますか? (2つお選びください。)
A. SRX シリーズ デバイスで正しいホスト受信トラフィック ルールを有効にします。
B. 必要な Exchange サーバー上の Windows ファイアウォール内でリモート イベント ログ管理を有効にします。
C. 必要なドメイン コントローラー上の Windows ファイアウォール内でリモート イベント ログ管理を有効にします。
D. JIMS サーバー上の Windows ファイアウォール内でリモート イベント ログ管理を有効にします。
Answer: C,D (メーッセージを残す**)**
説明
JIMS サーバーは、Active Directory ドメインまたは syslog ソースからユーザー、デバイス、およびグループの情報を収集して維持する Windows サービス アプリケーションです。JIMS サーバーは、Windows イベント ログを使用して、ドメイン コントローラーおよび Exchange サーバーからユーザーのログイン情報とログアウト情報を取得します。したがって、JIMS サーバーがイベントログを表示できるようにするには、次のアクションを実行する必要があります。
必要なドメイン コントローラーおよび Exchange サーバー上の Windows ファイアウォール内でリモート イベント ログ管理を有効にします。これにより、JIMS サーバーはこれらのサーバー上

のイベント ログにリモートでアクセスできるようになります。これを行うには、セキュリティが強化された Windows ファイアウォール スナップインを使用するか、netsh コマンドを使用します。
たとえば、ドメイン コントローラーでリモート イベント ログ管理を有効にするには、次のコマンドを使用できます。
netsh advfirewall firewall set rules group="リモート イベント ログ管理" new enable=yes JIMS サーバー上の Windows ファイアウォール内でリモート イベント ログ管理を有効にします。これにより、JIMS サーバーはドメイン コントローラーおよび Exchange サーバーからイベント ログを受信できるようになります。これは、上記と同じ方法を使用して行うことができます。たとえば、JIMS サーバー上でリモート イベント ログ管理を有効にするには、次のコマンドを使用できます。
netsh advfirewall firewall set rules group="リモート イベント ログ管理" new enable=yes オプション C およびオプション D は、この問題を解決するための正しいアクションを示しています。オプション A とオプション B は、JIMS サーバーのイベント ログを表示する機能に関連していないため、不正解です。ホスト受信トラフィック ルールは、JIMS サーバーではなく、SRX シリーズ デバイスへの到達が許可されるトラフィックを制御するために使用されます。JIMS サーバーが Exchange サーバーからユーザー情報を収集する必要がない場合、Exchange サーバー上でリモート イベント ログ管理を有効にする必要はありません。
参考資料: Juniper Security, Specialist (JNCIS-SEC) 参考資料および Juniper Security, Professional (JNCIP-SEC) 参考資料

最新問題: **47**
ネットワーク上のリスクを増大させるアプリケーションを実行しているシステムを見つけるように求められます。マルウェアやウイルスから保護するために、これらのシステムが IPS および Juniper ATP Cloud を通じて処理されていることを確認する必要があります。
このタスクを達成できるジュニパーネットワークスのソリューションはどれですか?
A. 暗号化されたトラフィックの分析情報
B. ジム
C. UTM
D. 適応型脅威プロファイリング
Answer: (解答を表示する**)**

Adaptive Threat Profiling (ATP) は、組織がネットワーク上の悪意のあるアクティビティを検出し、IPS および Juniper ATP Cloud を通じて処理してマルウェアやウイルスを保護できるようにするジュニパーネットワークスのソリューションです。ATP はジュニパーの高度な機械学習および人工知能 (AI) 機能を活用しており、悪意のあるアクティビティをリアルタイムで検出してブロックできます。
ATP はジュニパーの統合脅威管理 (UTM) および暗号化トラフィック インサイト (ETI) ソリューションと統合されており、エンドツーエンドのネットワーク保護ソリューションを提供します。

最新問題: **48**
「展示」ボタンをクリックします。



展示を参照すると、JIMS SRX クライアント設定の 2 つの値が SRX クライアントで設定された値と一致する必要があるのはどれですか? (2つお選びください。)
A. IPv6 レポート
B. クライアント ID
C. クライアント シークレット
D. トークンの有効期間
Answer: B,C (メーッセージを残す)

https://www.juniper.net/documentation/en_US/jims/topics/task/configuration/jims-srx-cconfiguration.html

最新問題: **49**
Juniper Secure Analytics デバイスでネットワーク イベントを操作する場合、フロー レコードはどのソースから取得されますか?
A. タップポート
B. スパン
C. スイッチ
D. ミラー
Answer: (解答を表示する**)**
https://www.juniper.net/documentation/en_US/jsa7.3.1/jsa-arch-deployment-guide/topics/concept/jsa-ad-jsa-events-and-flows.html

最新問題: **50**
AppQoS の 3 つの機能とは何ですか? 3つお選びください。)
A. DSCP 値を書き換えます
B. 転送クラスを割り当てます
C. TTL を書き換えます
D. レート制限トラフィック
E. 予約帯域幅
Answer: A,B,E (メーッセージを残す**)**
AppQoS (Application Quality of Service) は、アプリケーション トラフィックの高度な制御と優先順位付けを提供する Junos OS の機能です。AppQoS を使用すると、アプリケーション トラフィックを分類し、トラフィックに転送クラスを割り当て、トラフィックにサービス品質 (QoS) ポリシーを適用できます。DSCP 値を書き換えて、重要なアプリケーション用に帯域幅を予約することもできます。ただし、AppQoS は TTL またはレート制限トラフィックを書き換えません。

最新問題: **51**
展示」ボタンをクリックします。

展示物に示されている構成を参照して、次の 2 つの記述が真実ですか? (2つお選びください。)

A. syslog はユーザー機能用に構成されています。

B. syslog は情報機能用に構成されています。

C. ログはローカル ルーティング エンジンに保存されています。

D. ログはリモート サーバーに送信されています。

Answer: A,D (メーッセージを残す**)**

最新問題**: 52**

あなたは、vSRX 導入に関して次の要件を提出した新規顧客向けの提案を準備しています。

-- 世界中に分散されており、

-- 迅速なプロビジョニング、

-- 需要に基づいたスケール、

-- そして設備投資も低い。

これらの要件を満たすソリューションはどれですか?

A. AWS

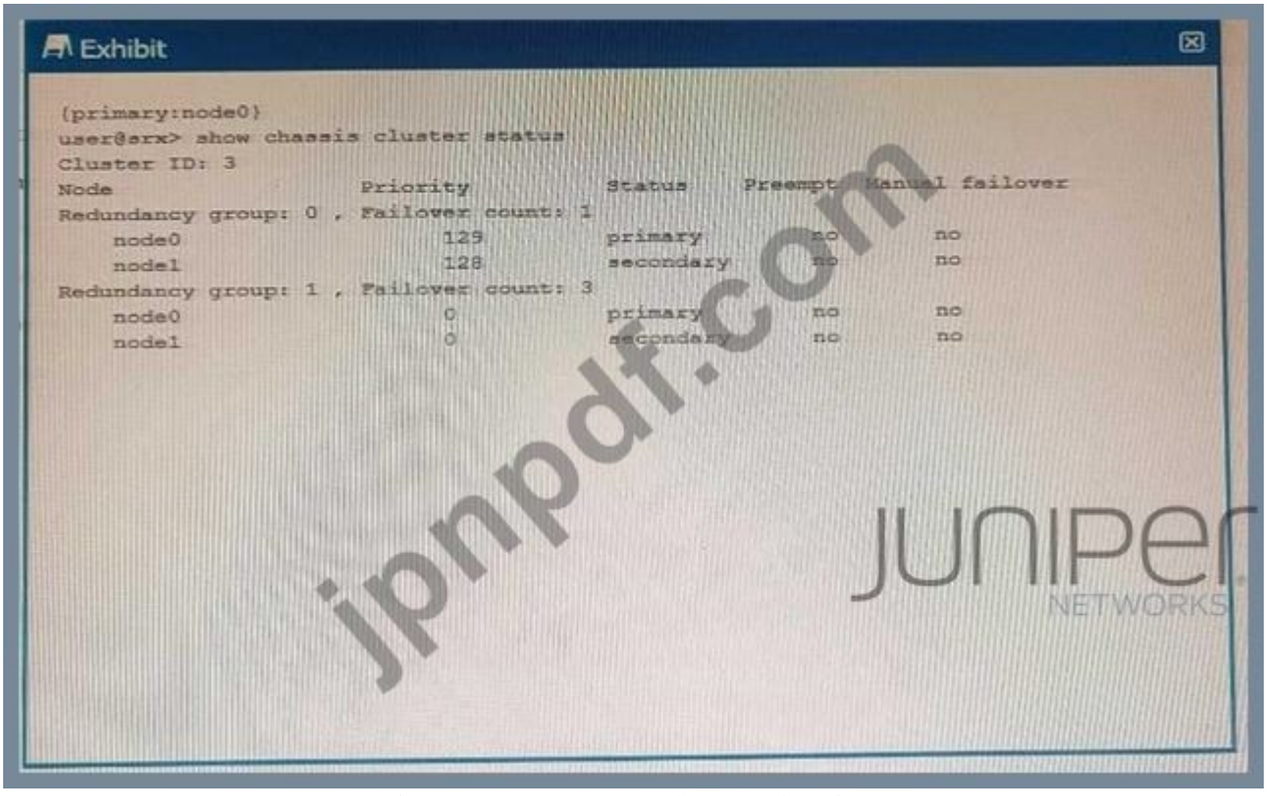
B. ネットワーク ディレクター

C. ジュニパー ATP クラウド

D. VMWare ESXi

Answer: A (メーッセージを残す**)**
vSRX 導入の要件を満たすソリューションは AWS です。AWS (アマゾン ウェブ サービス) は、インフラストラクチャ、プラットフォーム、ソフトウェア、データベースなどのオンデマンド サービスをサービスとして提供するクラウド コンピューティング プラットフォームです。AWS は世界中に分散されており、世界中の複数の地域にデータセンターがあります。AWS では迅速なプロビジョニングも可能です。つまり、事前構成された Amazon Machine Image (AMI) またはカスタム テンプレートを使用して、vSRX インスタンスを数分で起動できます。AWS では、デマンドに基づいたスケーリングも可能です。つまり、ネットワーク トラフィックとパフォーマンスのニーズに応じて vSRX インスタンスの数とサイズを調整できます。AWS は CapEx (資本支出) も低いため、使用した分だけ支払い、ハードウェアやメンテナンスのコストに投資する必要がありません。

最新問題: **53**
展示品からの情報を使用して、どの記述が正しいでしょうか?



A. Node1 はコントロール プレーンのアクティブ ノードです
B. クラスターに問題はありません。
C. 冗長グループ 1 は不適格な状態です。
D. 冗長グループ 0 は不適格な状態です。
Answer: C (メーッセージを残す**)**

最新問題: **54**
あなたは、帯域幅が狭く、すべてのトラフィックを許可する送信ポリシーを持つクラウドベースの VoIP ソリューションを使用しているブランチ オフィスに SRX シリーズ デバイスを実装しています。

このシナリオで VoIP トラフィックを優先するには、どのサービスをエッジ デバイスに実装しますか?
A. AppFW
B. SIP ALG
C. AppQoE
D. アプリの QoS
Answer: (解答を表示する**)**
説明
AppQoS は、SRX シリーズ デバイス上のさまざまな種類のアプリケーションのサービス品質 (QoS) に優先順位を付けて管理できるサービスです。AppQoS は、アプリケーション シグネチャを使用してトラフィックを識別および分類し、QoS ポリシーを適用して帯域幅、優先順位、およびスケジューリング パラメータをトラフィックに割り当てます。AppQoS は、VoIP などの重要なアプリケーションのパフォーマンスを最適化し、混雑したネットワークで必要な帯域幅と遅延を確保するのに役立ちます12。このシナリオでは、AppQoS を使用して VoIP トラフィックを他のトラフィックよりも優先し、ブランチ オフィスの SRX シリーズ デバイス上でその QoS を保証できます。参考文献:
アプリケーションのサービス品質について
アプリケーションのサービス品質の構成

最新問題**: 55**
シャーシのクラスタリングに関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. ノード ID 値の範囲は 1 ～ 255 です。
B. ノード ID は、シャーシ クラスタ内の各デバイスを識別するために使用されます。
C. クラスターへの変更を有効にするには、システムの再起動が必要です。
D. クラスター ID は、シャーシ クラスター内の各デバイスを識別するために使用されます。
Answer: (解答を表示する**)**
ノード ID 値の範囲は 1 ～ 255 で、シャーシ クラスタ内の各デバイスを識別するために使用されます。クラスター ID は各デバイスを識別するためにも使用されますが、ノード ID 構成の一部ではありません。クラスターへの変更を有効にするためにシステムを再起動する必要はありませんが、すべての変更が適切に適用されていることを確認することをお勧めします。

最新問題**: 56**
シャーシ クラスタのファブ インターフェイスに関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. リアルタイム オブジェクト (RTO) は、セッションの同期を維持するためにファブ インターフェイス上で交換されます。
B. アクティブ/アクティブ構成では、シャーシ間の転送トラフィックはファブ インターフェイス経由で送信されます。
C. ファブ インターフェイスにより構成の同期が可能になります。

D. ファブ インターフェイス上で送信されるハートビート信号は、コントロール プレーン リンクの状態を監視します。
Answer: A,B (メーッセージを残す**)**
ファブ インターフェイスは、シャーシ クラスタ内の 2 つのノードを接続するファブリック リンクです。シャーシ クラスターは、2 つの同一の SRX シリーズ デバイスを単一のデバイスとして機能するクラスターにグループ化する高可用性機能です。ファブ インターフェイスには 2 つの機能があります。
リアルタイム オブジェクト (RTO) は、セッションの同期を維持するためにファブ インターフェイス上で交換されます。RTO は、送信元および宛先の IP アドレス、ポート、プロトコル、セキュリティ ポリシーなど、アクティブなセッションに関する情報を保存するデータ構造です。RTO はファブ インターフェイス上のノード間で交換され、両方のノードが同じセッション情報を持ち、フェールオーバーの場合にトラフィックを引き継げるようにします。
アクティブ/アクティブ構成では、シャーシ間の転送トラフィックはファブ インターフェイス経由で送信されます。アクティブ/アクティブ構成では、クラスター内の両方のノードが異なる冗長グループ (RG) のトラフィックを処理できます。RG は、あるノードから別のノードに一緒にフェールオーバーするインターフェイスまたはサービスの集合です。トラフィックをある RG から別のノードでアクティブな別の RG に転送する必要がある場合、トラフィックはファブ インターフェイス経由で送信されます。

最新問題**: 57**
仮想化された SRX を環境に展開したいと考えています。
このシナリオでは、なぜ cSRX ではなく vSRX を使用するのでしょうか? (2つお選びください。)
A. vSRX はレイヤー 2 およびレイヤー 3 構成をサポートします。
B. vSRX のみがクラスタリングを提供します。
C. vSRX の起動時間は速くなります。
D. vSRX のみが NAT、IPS、および UTM サービスを提供します
Answer: A,B (メーッセージを残す**)**
説明
vSRX は、物理 SRX シリーズ ファイアウォールと同じ機能を提供する仮想ファイアウォールですが、ネットワークの需要に合わせて拡張するセキュリティ サービスを提供するための仮想化フォーム ファクターを備えています。コア ファイアウォール、堅牢なネットワーキング、完全な次世代機能、自動化されたライフサイクル管理など、SRX アプライアンスと同じ機能を提供します1。vSRX はレイヤー 2 およびレイヤー 3 構成をサポートします。つまり、透過的またはルーティングされた構成として動作できます。ネットワーク トポロジと要件に応じてファイアウォールを設定します。また、vSRX は、仮想ルーター、仮想スイッチ、論理システムなどの複数のルーティング インスタンスをサポートし、トラフィックの論理的な分離と分離を実現します2。vSRX はクラスタリングを提供し、2 つ以上の vSRX インスタンスが単一の論理デバイスとして機能できるようにします。高可用性、負荷分散、およびスケーラビリティを提供します。vSRX クラスターは、構成情報とセッション情報を同期し、ステートフル フェイルオーバーと冗長グループを

サポートできます3。cSRX は、仮想化環境およびクラウド環境に高密度ファイアウォールを備えたコンパクトなフットプリントを提供するコンテナ化ファイアウォールです。マイクロサービスとコンテナ化されたアプリケーションを保護し、ネットワークの可視性と脅威の防御を提供するように設計されています4。cSRX は、動的ルーティングやネットワーク機能を実行しない軽量で機敏なファイアウォールを目的としているため、レイヤー 2 およびレイヤー 3 構成をサポートしません。cSRX は、Kubernetes や Docker などの基盤となるコンテナ オーケストレーション プラットフォームに依存して、ネットワーク接続と管理を提供します4。cSRX は、コンテナ オーケストレーション プラットフォームのネイティブな復元力とスケーラビリティ機能を活用するように設計されているため、クラスタリングは提供しません。cSRX は、スタンドアロンのファイアウォールまたはサービス チェーンの一部として導入でき、需要に応じて動的にスケールアップまたはスケールダウンできます4。cSRX は、数分ではなく数秒でインスタンス化できるため、vSRX よりも起動時間が短くなります。vSRX の場合。cSRX は、コンテナ化された環境向けに最適化されているため、vSRX よりもイメージ サイズとメモリ要件が小さくなっています4。cSRX は、vSRX と同様の NAT、IPS、および UTM サービスを提供しますが、いくつかの制限があります。cSRX は、IPSec VPN、アプリケーション ID、ユーザー ファイアウォール、または SSL プロキシをサポートしません。また、cSRX は、コンテナ リソースとオーケストレーション プラットフォームによって制約を受けるため、vSRX よりもパフォーマンスとスループットが低くなります4。ジュニパーネットワークス US 2: VMware 用 vSRX 仮想ファイアウォール - TechLibrary - ジュニパーネットワークス 3: vSRX クラスターの概要 - TechLibrary - ジュニパーネットワークス 4: Juniper vSRX と cSRX の比較 - TechLibrary - ジュニパーネットワークス
https://www.juniper.net/documentation/us/en/software/csrx/csrx-linux-deployment/topics/concept/security-csrx-d

最新問題**: 58**
セキュリティ ポリシーが変更された場合、そのポリシーで許可されているアクティブ セッションのデフォルトの動作について正しいのはどれですか?
A. ポリシーで許可されているアクティブなセッションは削除されます。
B. アクション フィールドの変更を伴うポリシー変更のみが、変更の影響を受けるアクティブ セッションをドロップします。
C. アプリケーションの変更を伴うポリシー変更のみが、変更の影響を受けるアクティブなセッションをドロップします。
D. ポリシーによって許可されているアクティブなセッションは変更されずに継続されます。
Answer: D (メーッセージを残す**)**
SRX シリーズ デバイスのセキュリティ ポリシーを変更すると、デフォルトの動作では、ポリシーに一致する既存のセッションが変更されずに継続されます。これは、ポリシーの変更は、変更後に開始された新しいセッションにのみ影響することを意味します。ただし、clear-policy-session コマンドを使用すると、この動作を変更できます。これにより、変更されたポリシーに一致するすべてのセッションがクリアされ、新しいポリシーの再評価が強制されます。参考 := JNCIS-SEC 認

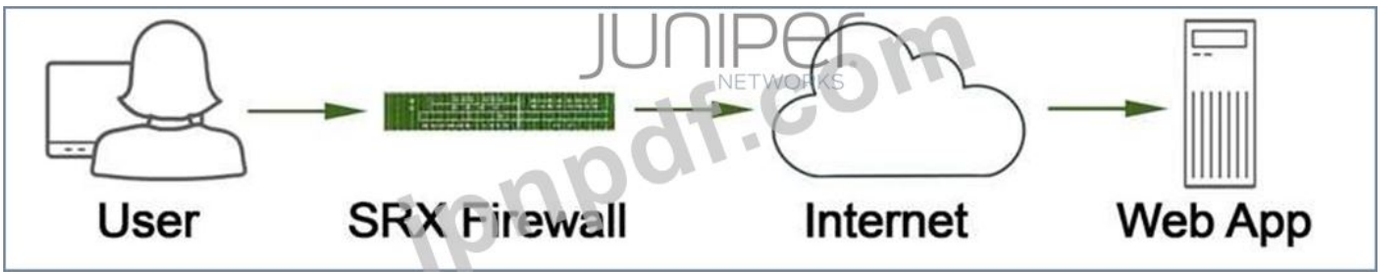
定、オープン ラーニング - セキュリティ、スペシャリスト (JNCIS-SEC)、セキュリティ ポリシー (上級)

最新問題: **59**
cSRX について正しい 2 つの記述はどれですか? (2つお選びください。)
A. cSRX は、ファイアウォール、NAT、IPS、および UTM サービスをサポートします。
B. cSRX は、レイヤ 2 の 『バンプインザワイヤ』展開のみをサポートします。
C. cSRX は BGP、OSPF をサポートします。IS-IS ルーティング サービス。
D. cSRX には、trust、untrust、および Management の 3 つのデフォルト ゾーンがあります。
Answer: B,C (メーッセージを残す)
説明
cSRX は、SRX シリーズ ファイアウォールのコンテナ化されたバージョンで、コンテンツ セキュリティ、AppSecure、統合脅威管理 (UTM) などの高度なセキュリティ サービスをコンテナの形式で提供します1。cSRX は、アプリケーション保護、マイクロセグメンテーション、または Docker コンテナ管理ソリューション 2 を介したセキュアな IoT 導入のためのエッジ ゲートウェイなど、さまざまな顧客のユース ケースをカバーする、簡単、柔軟、および拡張性の高い導入オプションをサポートします。cSRX は、Contrail Enterprise Multicloud、OpenContrail、およびその他のサードパーティ ソリューションを介した SDN もサポートします2。cSRX は、Kubernetes3 などの他の次世代クラウド オーケストレーション ツールとも統合します。
cSRX はファイアウォール、NAT、IPS、および UTM サービスをサポートしているため、オプション A は誤りです1。cSRX は、レイヤ 2 の 『バンプインザワイヤ』展開だけでなく、BGP、OSPF、IS-IS などのルーティング プロトコルを使用したレイヤ 3 展開もサポートしているため、オプション B は正解です4。cSRX は BGP、OSPF、および IS-IS ルーティング サービスをサポートしているため、選択肢 C は正解です4。cSRX には 3 つのデフォルト ゾーンがありませんが、代わりにホスト SRX シリーズ デバイスからゾーンを継承するため、オプション D は正しくありません5。参考文献:
1: cSRX コンテナ ファイアウォール | ジュニパーネットワークス米国
2: cSRX コンテナ ファイアウォール データシート | ジュニパーネットワークス米国
3: Kubernetes を使用した cSRX を理解する - ジュニパーネットワークス
4: すべての接続ポイントにセキュリティを拡張: コンテナ化されたセキュリティ ...
5: cSRX コンテナ ファイアウォール | ジュニパーネットワークス UK&I

最新問題: **60**
SRX シリーズ デバイス上の IPS によって使用される 2 種類の攻撃オブジェクトは何ですか? (2つお選びください。)
A. プロトコル異常ベースの攻撃
B. DDoS ベースの攻撃
C. スパムベースの攻撃
D. シグネチャベースの攻撃
Answer: A,D (メーッセージを残す)

最新問題: **61**
IPS シグネチャを使用してトラフィックを監視したいと考えています。
AppSecure スイートのどのモジュールがこのタスクに役立ちますか?
A. AppTrack
B. アプリの QoS
C. AppFW
D. APPID
Answer: A (メーッセージを残す**)**
説明
AppTrack: 通過するアプリケーションを追跡およびレポートします。
デバイス。
* 侵入検知および防御 (IDP): 適用
実行中のアプリケーションに対する適切な攻撃オブジェクト
標準外のポート。アプリケーション識別により IDP が向上
攻撃シグネチャの範囲を狭めることによるパフォーマンス
デコーダのないアプリケーション向け。
* AppFW: を使用してアプリケーション ファイアウォールを実装します。
アプリケーションベースのルール。
* AppQoS: サービス品質 (QoS) の優先順位付けを提供します。
アプリケーション認識に基づく
AppSecure AppTrack サービス モジュールは、アプリケーションの可視性に関する情報を共有するために使用されるログ記録およびレポート ツールです。AppID によってアプリケーションが識別されると、AppTrack はその使用状況を監視して記録するだけでなく、定期的にアプリケーションのアクティビティ更新メッセージも送信します。これらのメッセージは syslog によって送信されるため、ジュニパーネットワークス JSA シリーズ Secure Analytics アプライアンスや Contrail Service Orchestration などの互換性のあるサードパーティ デバイスで読み取ることができます。https://www.juniper.net/content/dam/www/assets /solution-briefs/us/en/appsecure-application-visib

最新問題: **62**
展示する



展示物を参照して、使用されるプロキシのタイプを説明している 2 つの記述はどれですか? (2つお選びください。)

A. クライアント保護プロキシ

B. フォワードプロキシ

C. サーバー保護プロキシ

D. リバースプロキシ

Answer: (解答を表示する**)**

最新問題**: 63**

2 つの SRX シリーズ デバイス間に VPN トンネルを構築しています。送信するトラフィックがない場合でも、トンネルが常に確立されるようにしたいとします。この目標を達成するにはどのアクションを使用しますか?

A. トンネル インターフェイスで OSPF デマンド回路機能を設定します。

B. 即時パラメータを使用して確立トンネルを構成します。

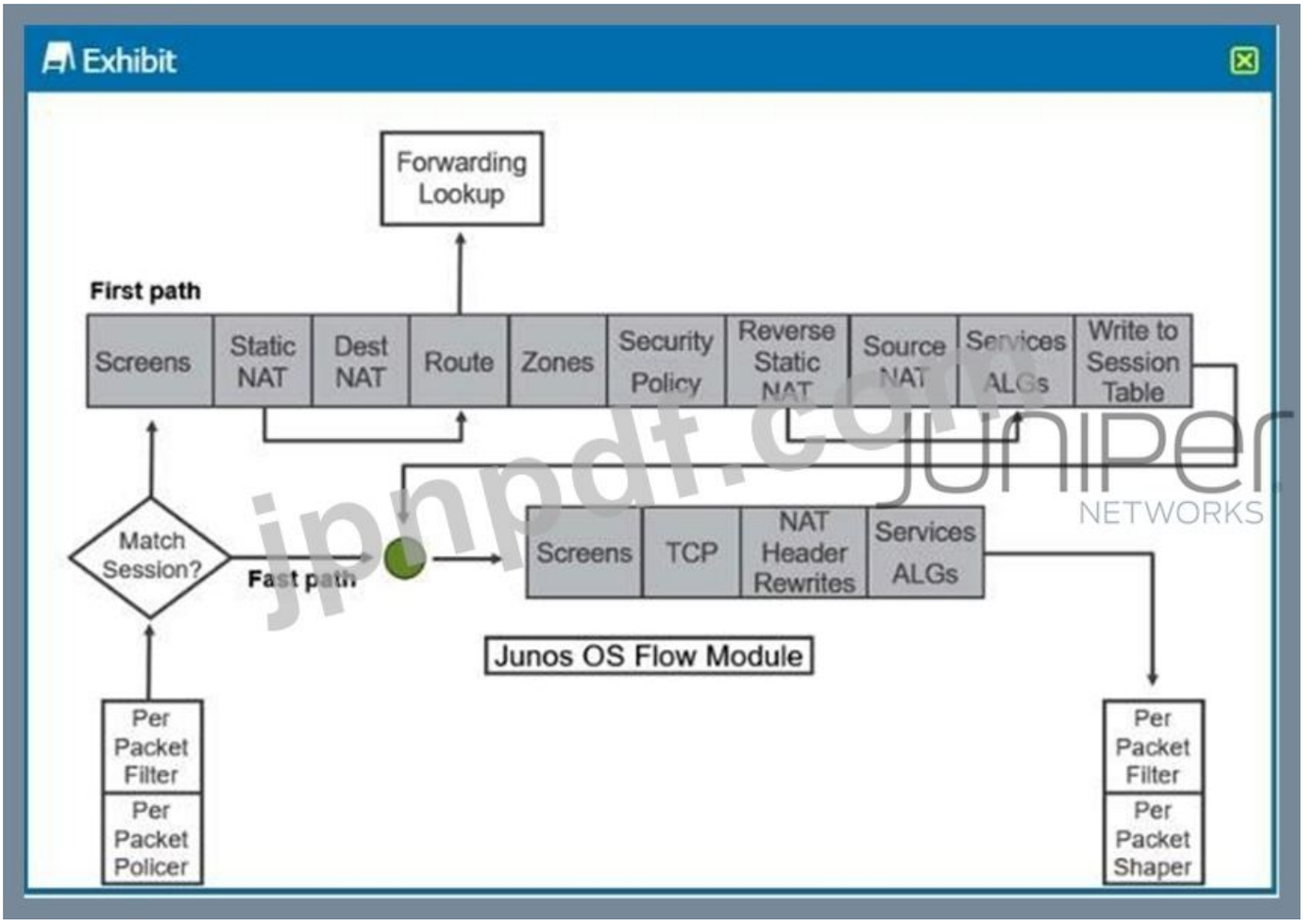
C. トンネル上で最適化されたパラメータを使用して vpn-monitor を構成します。

D. リンク全体で継続的に ping を実行するように RPM プローブを構成します。

Answer: (解答を表示する**)**

最新問題**: 64**

展示品にある SRX シリーズのフロー モジュール図を参照すると、IDP/IPS はどこで処理されますか?



A. 転送ルックアップ
B. セキュリティ ポリシー
C. サービス ALG
D. 画面
Answer: C (メーッセージを残す**)**

最新問題**: 65**
ポリシーのスケジュールに適用される 2 つのステートメントはどれですか? (2つお選びください。)
A. ポリシーは 1 つのスケジュールを参照します。
B. ポリシーは多くのスケジュールを参照します。
C. スケジュールがいつアクティブになるかに関係なく、ポリシーはアクティブのままです。
D. 複数のポリシーが同じスケジュールを参照できます。
Answer: (解答を表示する**)**

最新問題**: 66**
動作モードコマンドの表形式のデータを表示したいと考えています。
このシナリオでは、どのログ パラメータがこの機能を提供しますか?
A. 許可する
B. カウント

C. セッション初期化
D. セッション終了
Answer: B (メーッセージを残す**)**
説明
count ログ パラメータは、ファイアウォール フィルタ条件に一致するパケットの数を表形式で表示します。count パラメータは、show firewall コマンドで表示できるカウンタも作成します。他のロギング パラメータ (permit、session-init、session-close) は表形式のデータを表示せず、用語に一致するパケットをシステム ログ ファイルまたはユーザー指定のファイルに記録します。参考文献:
ファイアウォールフィルターカウンターについて
ファイアウォールフィルターカウンターの構成
ファイアウォールを表示

最新問題**: 67**
reth LAG に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. リンクの速度とデュプレックス設定は同じである必要があります。
B. リンクは同じケーブル タイプを使用する必要があります
C. 「minimum-links」ステートメントの値は 2 でなければなりません。
D. 2 つ以上のインターフェイスが必要です。
Answer: (解答を表示する**)**
説明
reth LAG は、シャーシ クラスタの各ノードからの 1 つ以上の物理インターフェイスを含む冗長イーサネット インターフェイスです。reth LAG により、クラスターの帯域幅とリンクの可用性が向上します。reth LAG を構成するには、次の手順に従う必要があります。
各ノードの物理インターフェイスを、同じ速度とデュプレックス設定を持つ集約イーサネット インターフェイスとして構成します。これは、リンクが LAG を形成し、トラフィックを正しく通過できるようにするために必要です。
リンクには異なるタイプのケーブル (銅線や光ファイバーなど) を使用できますが、速度は同じである必要があります。
redundant-ether-options ステートメントを使用して reth インターフェイスを構成し、集約されたイーサネット インターフェイスを子リンクとして指定します。reth LAG には少なくとも 2 つのインターフェイス (各ノードに 1 つ) が必要ですが、冗長性と負荷分散のためにさらにインターフェイスを追加できます。また、minimum-links ステートメントを指定して、reth インターフェイスが起動するために起動する必要がある子リンクの最小数を設定することもできます。デフォルト値は 1 ですが、必要に応じてより大きな値に変更できます。
必要に応じて、適切な IP アドレス、セキュリティ ゾーン、その他の設定を使用して reth インターフェイスを構成します。
reth インターフェイスで LACP を有効にして、ピア デバイスと LAG パラメータを動的にネゴシエートすることもできます。

参考文献:
[シャーシクラスタ内の集約イーサネットインターフェイス] 1
[シャーシ クラスタ冗長イーサネット インターフェイス] 2
[シャーシ クラスタ上の LACP / LAG - インターフェイスの監視?] 3
[緊急 (LAG - RETH 相互接続)] 4

最新問題: **68**
データ プレーンのロギングはどの 2 つのモードで動作しますか? (2つお選びください。)
A. syslog
B. バイナリ
C. イベント
D. ストリーム
Answer: C,D (メーッセージを残す**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/system-logging-for-a-security-device.html

最新問題: **69**
アプリケーションの識別に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. アプリケーション識別により、レイヤー 7 内にあるネストされたアプリケーションを識別できます。
B. アプリケーション識別では、レイヤー 7 内にあるネストされたアプリケーションを識別できません。
C. アプリケーション署名は IDP 署名と同じです。
D. アプリケーション署名は IDP 署名と同じではありません。
Answer: A,C (メーッセージを残す**)**
説明
https://www.juniper.net/documentation/us/en/software/junos/application-identification/topics/topic-map/security

最新問題: **70**
あなたの会社では、Juniper ATP Cloud の無料モデルを使用しています。現在の検査プロファイルは 10 MB に設定されています。他のファイル タイプのスキャン時間の変化を最小限に抑えながら、最大 30 MB の実行可能ファイルをスキャンできるように ATP クラウドを構成するように求められます。
このシナリオではどの構成を使用する必要がありますか?
A. CLI を使用してカスタム プロファイルを作成し、スキャン制限を増やします。
B. ATP Cloud UI を使用してデフォルトのプロファイルを変更し、すべてのファイルのスキャン制限を 30 MB に増やします。
C. CLI を使用してデフォルトのプロファイルを変更し、すべてのファイルのスキャン制限を 30 MB に増やします。

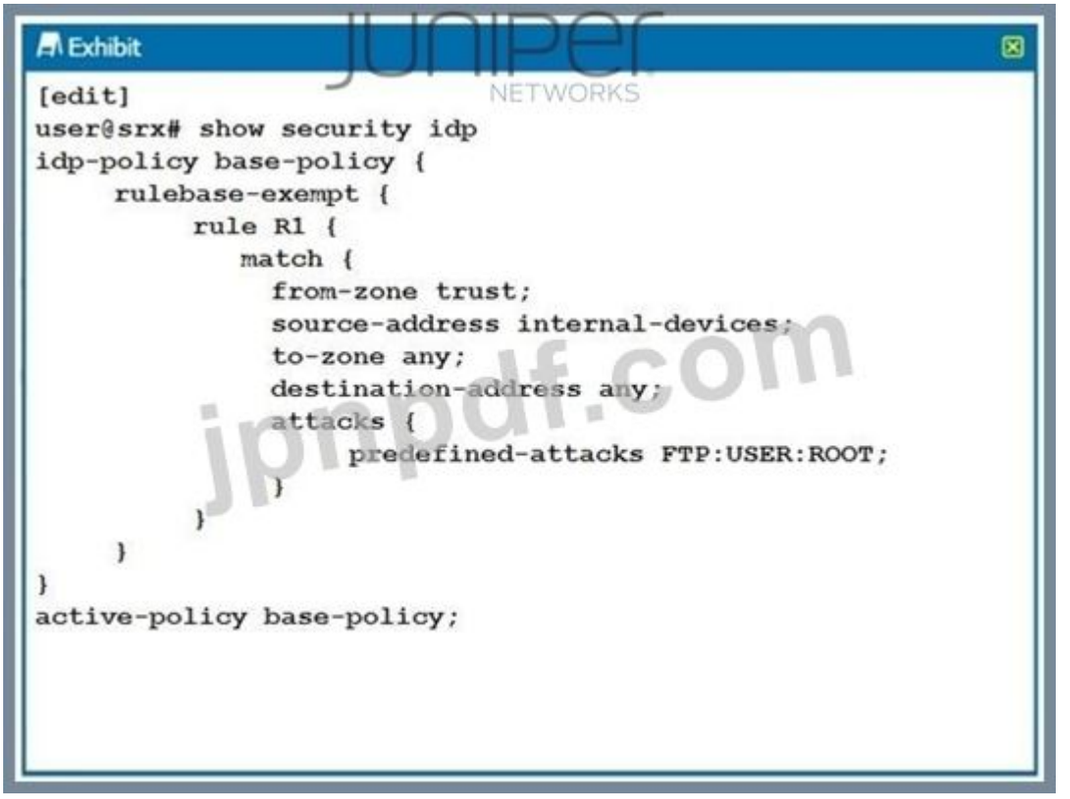
D. ATP Cloud UI を使用してカスタム プロファイルを更新し、実行可能ファイルのスキャン制限を 30 MB に増やします。

Answer: (解答を表示する**)**

このシナリオでは、ATP Cloud UI を使用してカスタム プロファイルを作成し、実行可能ファイルのスキャン制限を 30 MB に更新する必要があります。これにより、最大 30 MB の実行可能ファイルを確実にスキャンできると同時に、他のファイル タイプのスキャン時間の変化を最小限に抑えることができます。これを行うには、ATP Cloud UI にログインし、[プロファイル] タブに移動します。[作成] ボタンをクリックして新しいプロファイルを作成し、実行可能ファイルのスキャン制限を 30 MB に調整します。カスタム プロファイルを保存したら、それを目的のシステムに適用すると、新しいスキャン制限が有効になります。

最新問題: **71**

展示物に関して、どの記述が真実ですか?



Exhibit

```
[edit]
user@srx# show security idp
idp-policy base-policy {
     rulebase-exempt {
          rule R1 {
             match {
               from-zone trust;
               source-address internal-devices;
               to-zone any;
               destination-address any;
               attacks {
                  predefined-attacks FTP:USER:ROOT;
               }
             }
     }
}
active-policy base-policy;
```

A. IDP はすべてのユーザーをブロックします。

B. IDP は、一致したセッションの接続を閉じます。

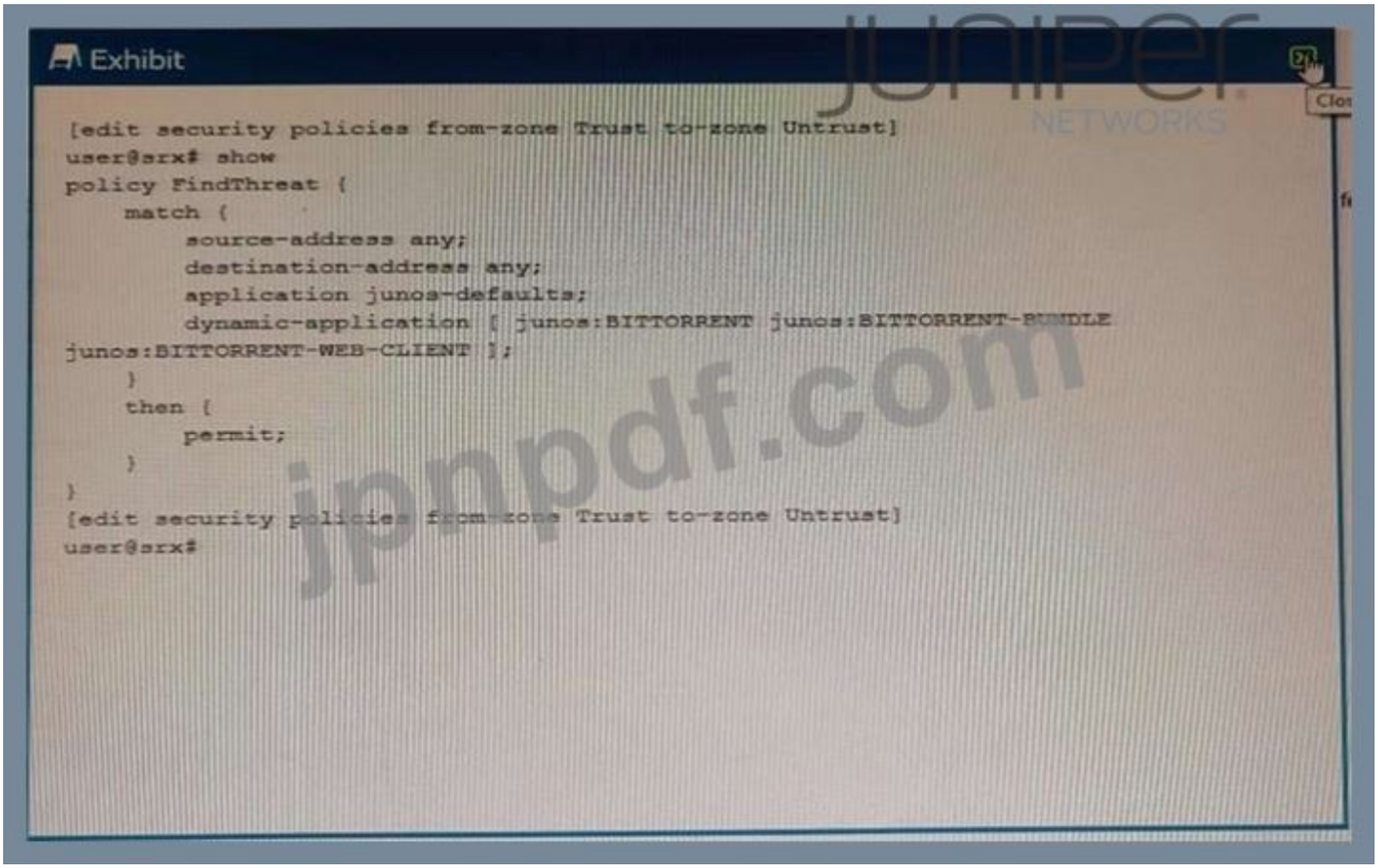
C. IDP は、一致したセッションの接続を無視します。

D. IDP は root ユーザーをブロックします。

Answer: C (メーッセージを残す**)**

最新問題: **72**

展示する



ネットワーク上の BitTorrent トラフィックを追跡するように求められます。将来の脅威を軽減するには、ワークステーションを High_Risk_Workstations フィードに、サーバーを BitTorrent_Servers フィードに自動的に追加する必要があります。
この機能を FindThreat ポリシーに追加する 2 つのコマンドはどれですか? (2つお選びください。)

A.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-identity-to-feed High_Risk_Workstations
```

B.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-ip-to-feed High_Risk_Workstations
```

C.

D.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-identity-to-feed BitTorrent_Servers
```

Answer: D (メーッセージを残す)

最新問題: **73**
JSA データ収集に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. Event Collector は、BGP FlowSpec を使用して情報を収集します。
B. フロー コレクターは統計サンプリングを使用できます。
C. フロー コレクターはログを解析します。
D. Event Collector はログを解析します
Answer: (解答を表示する)

フロー コレクターは、統計サンプリングを使用してネットワーク フロー データを収集し、JSA データベースに保存できます。イベント コレクターは、syslog、SNMP、NetFlow、BGP FlowSpec などのさまざまなソースから情報を収集します。フロー コレクターとイベント コレクターは両方ともログを解析し、ログから有用な情報を抽出します。

最新問題: **74**
アプリケーション層ゲートウェイ (ALG) の機能を定義するステートメントはどれですか?
A. ALG は、特定の IP アドレス範囲を許可または禁止するソフトウェア プロセスを使用します。
B. ALG は、アプリケーションと同じポート番号を使用する単一の TCP セッションで使用されるソフトウェアを使用します。
C. ALG には、TCP セッションごとに 1 つのアプリケーション セッションを使用するプロトコルが含まれています。
D. ALG は、特定のプロトコルを管理するためにソフトウェア プロセスを使用します。
Answer: D (メーッセージを残す**)**
アプリケーション層ゲートウェイ (ALG) の機能を定義するステートメントは次のとおりです。ALG は、特定のプロトコルを管理するためにソフトウェア プロセスを使用します。ALG は、OSI モデルのアプリケーション層 (層 7) で動作し、SIP、FTP、RTSP などの特定のアプリケーション プロトコルに関連付けられたデータを処理するセキュリティ コンポーネントです。ALG は、クライアント間のプロキシまたは仲介者として機能します。とサーバー アプリケーションを統合し、アドレスとポートの変換、リソースの割り当て、アプリケーションの応答制御、データと制御トラフィックの同期などのさまざまな機能を実行します。ALG は、アプリケーション ペイロードを検査および変更して、ファイアウォールまたは NAT トラバーサルを有効にしたり、スプーフィングや DoS 攻撃を防止したり、アプリケーション固有のコマンドに基づいて詳細なセキュリティ ポリシーを適用したりすることもできます。参考 := アプリケーション レベル ゲートウェイ - Wikipedia、アプリケーション層ゲートウェイ (ALG) とは何ですか? | F5、ALG ** アプリケーション層ゲートウェイとは | 3CX

最新問題: **75**
展示する

展示物を参照して、使用されるプロキシのタイプを説明している 2 つの記述はどれですか? (2つお選びください。)

A. フォワードプロキシ

B. クライアント保護プロキシ

C. サーバー保護プロキシ

D. リバースプロキシ

Answer: (解答を表示する**)**

B) クライアント保護プロキシ: フォワード プロキシはユーザーの ID とコンピュータ情報を Web サーバーから保護するため、クライアント保護プロキシとも呼ばれるため、この記述は正しいです4。

C) サーバー保護プロキシ: リバース プロキシは Web サーバーの ID と場所をユーザーから保護するため、サーバー保護プロキシとも呼ばれるため、この記述は正しいです4。

最新問題: **76**

2 つのデバイスでシャーシ クラスタリングを有効にし、各デバイスにクラスタ ID とノード ID を割り当てます。

このシナリオでは、デバイスを再起動する正しい順序は何ですか?

A. セカンダリ デバイスを再起動し、次にプライマリ デバイスを再起動します。

B. プライマリ デバイス自体に正しいクラスターとノード ID が割り当てられるため、セカンダリ デバイスのみを再起動します。

C. プライマリ デバイスを再起動し、次にセカンダリ デバイスを再起動します。

D. セカンダリ デバイス自体に正しいクラスターとノード ID が割り当てられるため、プライマリ デバイスのみを再起動します。

Answer: (解答を表示する**)**

説明

ジュニパーネットワークスのシャーシ クラスタリング設定で、2 つのデバイスでシャーシ クラスタリングを有効にし、クラスタ ID とノード ID を各デバイスに割り当てる場合、デバイスを再起

動する正しい順序は次のとおりです。C. プライマリ デバイス、次にセカンダリ デバイスを再起動します。
説明: クラスター ID とノード ID を各デバイスに割り当てた後、最初にプライマリ デバイスを再起動することをお勧めします。これにより、プライマリ デバイスが指定されたクラスター ID とノード ID で確実にオンラインになります。プライマリ デバイスが起動して実行されたら、セカンダリ デバイスを再起動できます。セカンダリ デバイスは、プライマリ デバイスに割り当てられている既存のクラスタ ID とノード ID を認識し、それに応じてクラスタに参加します。

最新問題: **77**
クライアントが既知のコマンドアンドコントロール サーバーとの通信を試みましたが、設定された脅威レベルのしきい値に達しました。
この状況では、クライアントの IP アドレスはどのフィードに自動的に追加されますか?
A. コマンド アンド コントロール クラウド フィード
B. ホワイトリストとブロックリストのフィード
C. カスタム クラウド フィード
D. 感染したホストのクラウド フィード
Answer: D (メーッセージを残す)
説明
感染したホストのクラウド フィードは、マルウェアによる侵害または感染が確認された IP アドレスのリストです。フィードは、既知のコマンド アンド コントロール サーバーへの接続など、ホストからの悪意のあるアクティビティの検出に基づいて、ジュニパー ATP クラウドによって更新されます。ネットワーク上のホストが設定された脅威レベルのしきい値に達すると、その IP アドレスが感染したホストのクラウド フィードに自動的に追加され、インターネット上の他のホストとの通信がブロックされます。他のフィードはこの状況には関係ありません。コマンド アンド コントロール クラウド フィードは、マルウェアがリモート コントロールと通信に使用することがわかっている IP アドレスのリストです。ホワイトリストおよびブロックリスト フィードは、SRX シリーズ デバイスによって許可または拒否される IP アドレスのユーザー定義リストです。カスタム クラウド フィードは、特定のカテゴリまたは脅威レベルに関連付けられた IP アドレスのユーザー定義のリストです。参考文献:
感染したホスト: 詳細情報
ジュニパーの攻撃者 IP フィードが SecIntel で脅威保護を強化
ATP アプライアンスと SRX シリーズの脅威レベルの比較表

最新問題: **78**
仮想化された SRX シリーズ デバイスに関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. vSRX はトランスペアレント モードで導入できます。
B. cSRX はルーテッド モードで展開できます。
C. vSRX はトランスペアレント モードでは展開できません。
D. cSRX はルーテッド モードで展開できません。
Answer: (解答を表示する**)**

最新問題: **79**
2 台のスタンドアロン SRX シリーズ デバイスをシャーシ クラスタ展開に変換するように求められます。
IPsec トンネルが新しい展開と互換性があることを確認する必要があります。
このシナリオでは、トンネル エンドポイントをバインドするときにどの 2 つのインターフェイスを使用する必要がありますか?
(2つお選びください。)
A. lo0
B. レス
C. pp0
D. げ
Answer: B,D (メーッセージを残す**)**

最新問題: **80**
JIMS の高可用性について正しい 2 つの記述はどれですか? (2つお選びください。)
A. SRX クライアントは、JIMS サーバーの共有仮想 IP (VIP) アドレスを使用して構成されます。
B. SRX クライアントは、認証テーブルをプライマリ JIMS サーバーとセカンダリ JIMS サーバーの両方と同期します。
C. JIMS は、プライマリ JIMS サーバーとセカンダリ JIMS サーバーのインストールを通じて高可用性をサポートします。
D. SRX クライアントは、プライマリおよびセカンダリ JIMS サーバーの一意の IP アドレスを使用して構成されます。
Answer: C,D (メーッセージを残す**)**

最新問題: **81**
IoT セキュリティ機能は、IoT デバイスからのトラフィックを識別するためにどの方法を使用しますか?
A. SRX シリーズ デバイスは、IoT デバイスのトランジット トラフィックから Juniper ATP Cloud Juniper ATP Cloud にメタデータをストリーミングします。

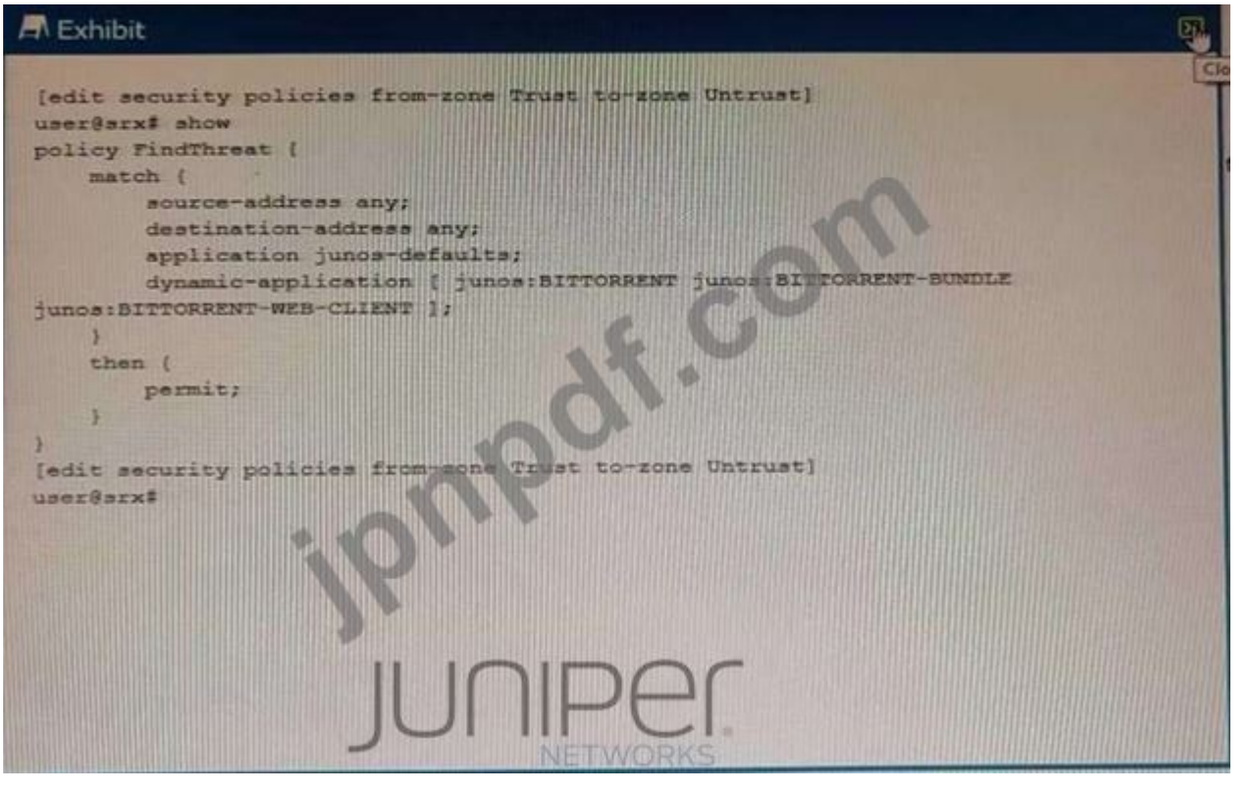
B. SRX シリーズ デバイスは、IoT デバイスから受信したトランジット トラフィックをジュニパー ATP クラウドにストリーミングします。
C. SRX シリーズ デバイスは、MAC アドレスを使用して LOT デバイスを識別します。
D. SRX シリーズ デバイスは、トランジット トラフィックから抽出されたメタデータから LOT デバイスを識別します。
Answer: D (メーッセージを残す**)**
メタデータは、デバイスのタイプ、それに関連するアクティビティ、およびその脅威プロファイルを識別するために使用されます。この情報は、デバイスに適切なセキュリティ ポリシーを決定するために使用されます。IoT セキュリティの詳細については、ジュニパー セキュリティ スペシャリスト (JNCIS-SEC) スタディ ガイドを参照してください。

最新問題**: 82**
危険なアプリケーションをブロックするには、ネットワークに AppSecure を導入する必要があります。
このシナリオでは、どの 2 つの AppSecure 機能が必要ですか? (2つお選びください。)
A. AppTrack
B. APBR
C. AppFW
D. アプリID
Answer: A,D (メーッセージを残す**)**

最新問題**: 83**
SRX シリーズ デバイス シャーシ クラスタに関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
A. 冗長グループ 0 はクラスター バックアップ ノード上でのみアクティブです。
B. 各シャーシ クラスタ メンバーには一意のクラスタ ID 値が必要です。
C. 各シャーシ クラスタ メンバー デバイスは、アクティブな冗長グループをホストできます。
D. シャーシ クラスタ メンバー デバイスは同じモデルである必要があります。
Answer: C,D (メーッセージを残す**)**
説明
シャーシ クラスタは、単一ノードとして動作するように接続および構成された 1 組の SRX シリーズ デバイスであり、トラフィック フローの高可用性と負荷分散を実現します1。シャーシ クラスタは 2 つのノードで構成されます。
1 つはプライマリ、もう 1 つはセカンダリです。各ノードは 1 つ以上の冗長グループをホストできます。冗長グループは、ノード障害の場合に一緒にフェールオーバーする必要があるインターフェイスとサービスをグループ化する論理エンティティです2。冗長グループ 0 は、ルーティング エンジンや制御リンクなど、クラスターのコントロール プレーンを監視する特別なグループです。冗長グループ 0 は常にプライマリ ノードでアクティブになり、セカンダリ ノードでスタンバイになります3。

したがって、選択肢 A は false です。各シャーシ クラスタ メンバーには一意のノード ID 値が必要です。これは次のいずれかになります。
0 または 1。クラスタ内で自身を識別します4。ただし、クラスター ID 値は両方のノードで同じであり、クラスター全体を識別するために使用されます。したがって、選択肢 B は false です。各シャーシ クラスタ メンバー デバイスは、ノードの構成とステータスに応じて、アクティブな冗長グループをホストできます。デフォルトでは、プライマリ ノードはすべての冗長グループをホストしますが、優先順位が高い場合はセカンダリ ノードによって一部のグループがプリエンプトされるように、または優先順位が同じ場合はノード間で負荷共有されるように構成できます。
したがって、選択肢 C は true です。モデルが異なるとハードウェアおよびソフトウェアの仕様が異なり、クラスタ内で相互に互換性がない可能性があるため、シャーシ クラスタ メンバー デバイスは同じモデルである必要があります。
したがって、選択肢 D は true です。参考文献:
SRX シリーズ デバイス用シャーシ クラスター ユーザー ガイド
シャーシクラスタ冗長グループについて
冗長グループ 0 について
シャーシクラスタのノードIDについて
[シャーシクラスタのクラスタIDについて]
【シャーシクラスタ冗長グループの設定】
[SRX シリーズ デバイスのシャーシ クラスター機能ガイド]

最新問題: **84**
ネットワーク上の BitTorrent トラフィックを追跡するように求められます。将来の脅威を軽減するには、ワークステーションを High_Risk_Workstations フィードに、サーバーを BitTorrent_Servers フィードに自動的に追加する必要があります。



この機能を FindThreat ポリシーに追加する 2 つのコマンドはどれですか? (2つお選びください。)

A.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-identity-to-feed High_Risk_Workstations
```

B.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-source-ip-to-feed High_Risk_Workstations
```

C.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-ip-to-feed BitTorrent_Servers
```

D.

```
[edit security policies from-zone Trust to-zone Untrust policy FindThreat then permit application-
services security-intelligence]
user@srx# set add-destination-identity-to-feed BitTorrent_Servers
```

Answer: D (メーッセージを残す)

最新問題: **85**

あなたの会社では、Juniper ATP Cloud の無料モデルを使用しています。現在の検査プロファイルは 10 MB に設定されています。他のファイル タイプのスキャン時間の変化を最小限に抑えながら、最大 30 MB の実行可能ファイルをスキャンできるように ATP クラウドを構成するように求められます。

このシナリオではどの構成を使用する必要がありますか?

A. CLI を使用してカスタム プロファイルを作成し、スキャン制限を増やします。

B. ATP Cloud UI を使用してデフォルトのプロファイルを変更し、すべてのファイルのスキャン制限を 30 MB に増やします。

C. CLI を使用してデフォルトのプロファイルを変更し、すべてのファイルのスキャン制限を 30 MB に増やします。

D. ATP Cloud UI を使用してカスタム プロファイルを更新し、実行可能ファイルのスキャン制限を 30 MB に増やします。

Answer: D (メーッセージを残す)

説明

Juniper ATP Cloud プロファイルを使用すると、検査のためにクラウドに送信するファイルを定義できます。スキャンするファイルの種類 (.tar、.exe、.java など) を共通の名前でグループ化し、スキャンするコンテンツに基づいて複数のプロファイルを作成できます。次に、対象となる SRX シリーズ デバイスにプロファイル名を入力して適用します1。カスタム プロファイルを更新するには、ATP Cloud UI を使用し、[構成] > [ファイル検査管理] > [プロファイル] に移動します。そこで既存のプロファイルを編集し、他のファイルのスキャン制限を 10 MB に維持したまま、実行可能ファイルのスキャン制限を 30 MB に変更できます。こうすることで、他のファイル タイプのスキャン時間を増やすことなく、より大きな実行可能ファイルをスキャンできます。参考資料: ファイル検査プロファイルの概要

最新問題: **86**

2 つのデバイスでシャーシ クラスタリングを有効にし、各デバイスにクラスタ ID とノード ID を割り当てます。このシナリオでは、デバイスを再起動する正しい順序は何ですか?
A. セカンダリ デバイスを再起動し、次にプライマリ デバイスを再起動します。
B. プライマリ デバイス自体に正しいクラスターとノード ID が割り当てられるため、セカンダリ デバイスのみを再起動します。
C. プライマリ デバイスを再起動し、次にセカンダリ デバイスを再起動します。
D. セカンダリ デバイス自体に正しいクラスターとノード ID が割り当てられるため、プライマリ デバイスのみを再起動します。
Answer: C (メーッセージを残す)
2 つのデバイスでシャーシ クラスタリングを有効にする場合、それらを再起動する正しい順序は、最初にプライマリ デバイスを再起動し、次にセカンダリ デバイスを再起動することです。どちらのデバイスも正しいクラスターとノード ID を自分自身に割り当てることはできないため、両方のデバイスを再起動して、適切な構成が適用されていることを確認する必要があります。

最新問題: **87**
シャーシ クラスターで reth LAG インターフェイスをサポートしたいと考えています。
このタスクを実行するには、相互接続スイッチで何を有効にする必要がありますか?
A. LLDP
B. swfab
C. RSTP
D. 802.3ad
Answer: D (メーッセージを残す)

最新問題: **88**
使用されているポート番号に関係なく、悪意のあるアプリケーションをブロックするように求められます。
このシナリオでは、どの 2 つのアプリケーション セキュリティ機能を使用する必要がありますか? (2つお選びください。)
A. AppFW
B. AppQoE
C. APPID
D. AppTrack
Answer: A,C (メーッセージを残す)
ネットワーク アクセス ポリシー、ユーザーとそのジョブ ロール、時間、アプリケーション署名に基づいてアプリケーションとユーザーをブロックできます2。また、Juniper Advanced Threat Prevention (ATP) を使用して、ファイル、IP トラフィック、DNS リクエスト内の一般的なサイバー脅威やゼロデイ サイバー脅威を検出してブロックすることもできます1

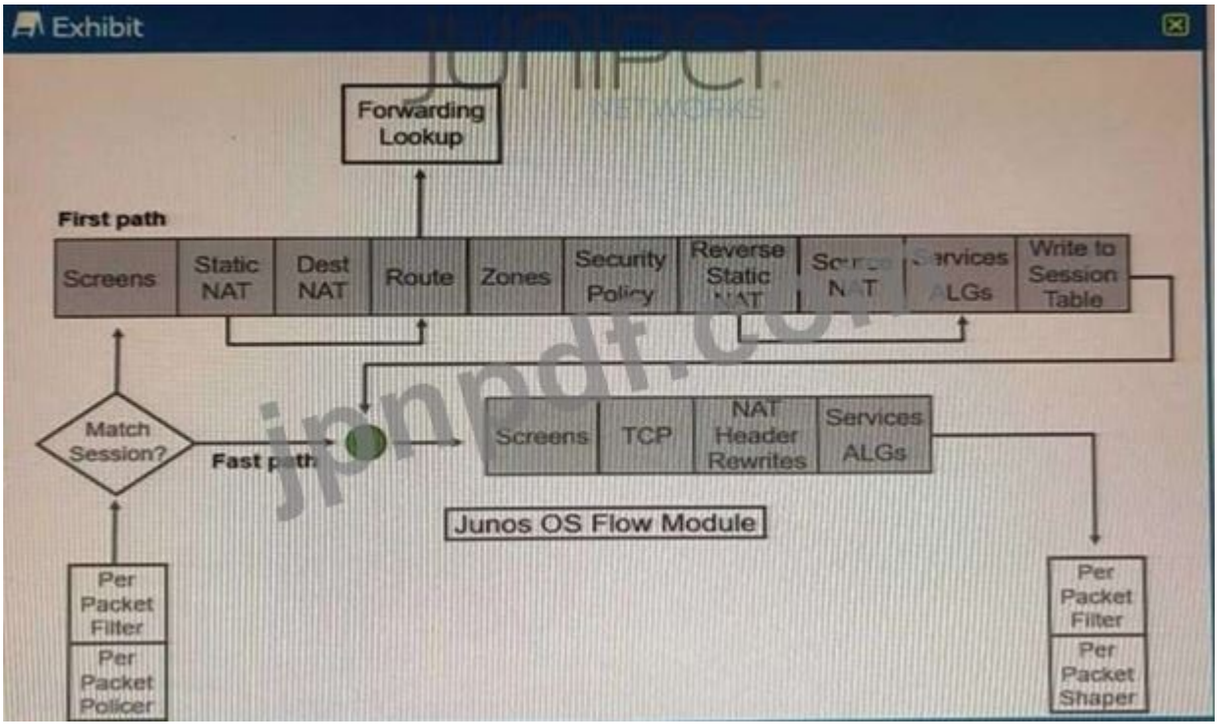
最新問題: **89**

特定の基準に一致したときにアラートが確実にトリガーされるようにするために、Juniper Secure Analytics (JSA) で構成可能な 2 つの機能はどれですか? (2つお選びください。)
A. 構成要素
B. アセット
C. イベント
D. テスト
Answer: C,D (メーッセージを残す**)**
Juniper Secure Analytics (JSA) の 2 つの構成可能な機能は、イベントとテストであり、特定の基準に一致したときにアラートを確実にトリガーするために使用できます。イベントはさまざまなソースからのデータの収集を指しますが、テストはアラートをトリガーする基準を定義するために使用されます。たとえば、イベントを使用してファイアウォールからデータを収集し、IP アドレス、ポート番号、トラフィックの種類などの基準を定義するテストを使用できます。

最新問題**: 90**
cSRX ベースの仮想セキュリティ展開と vSRX ベースの仮想セキュリティ展開の違いについて正しい 3 つの記述はどれですか? 3つお選びください。)
A. vSRX と cSRX は両方とも、レイヤ 2 ～ レイヤ 7 の安全なサービスを提供します。
B. vSRX はレイヤ 2 ～ レイヤ 7 のセキュア サービスを提供し、cSRX はレイヤ 4 ～ レイヤ 7 のセキュア サービスを提供します。
C. cSRX は、vSRX ベースのソリューションよりも特定の展開に必要なストレージとメモリのスペースが少なくなります。
D. cSRX ベースのソリューションは、vSRX ベースのソリューションよりもスケーラブルです。
E. vSRX は、cSRX と比較して、導入時間と再起動が高速になります。
Answer: B,C,D (メーッセージを残す**)**

最新問題**: 91**
SRX5800 シャーシ クラスタのソフトウェア アップグレード後、node1 がセカンダリである必要があるのに、node0 と node1 の両方がプライマリ状態になっていることがわかります。すべての制御リンクとファブリック リンクは正常に動作しています。
このシナリオでは、クラスターを回復するにはどの手順を実行する必要がありますか?
A. ノード 1 でシステム再起動要求コマンドを実行します。
B. ノード0でシステムソフトウェアロールバック要求コマンドを実行します。
C. ノード 1 でシステム ソフトウェア追加要求コマンドを実行します。
D. ノード0でシステム再起動要求コマンドを実行します。
Answer: (解答を表示する**)**

最新問題: **92**
展示品にある SRX シリーズのフロー モジュール図を参照すると、アプリケーションのセキュリティはどこで処理されますか?



A. 転送ルックアップ
B. セキュリティ ポリシー
C. サービス ALG
D. 画面
Answer: C (メーッセージを残す)

最新問題: **93**
cSRX ベースの仮想セキュリティ展開と vSRX ベースの仮想セキュリティ展開の違いについて正しい 3 つの記述はどれですか? 3つお選びください。)
A. vSRX はレイヤ 2 ～ レイヤ 7 のセキュア サービスを提供し、cSRX はレイヤ 4 ～ レイヤ 7 のセキュア サービスを提供します。
B. cSRX は、vSRX ベースのソリューションよりも特定の展開に必要なストレージとメモリのスペースが少なくなります。
C. cSRX ベースのソリューションは、vSRX ベースのソリューションよりもスケーラブルです。
D. vSRX と cSRX は両方とも、レイヤ 2 ～ レイヤ 7 の安全なサービスを提供します。
E. vSRX は、cSRX と比較して、導入時間と再起動が高速になります。
Answer: A,B,C (メーッセージを残す)

https://www.juniper.net/documentation/en_US/day-one-books/topics/concept/juniper-vsrx-versus-csrx.html

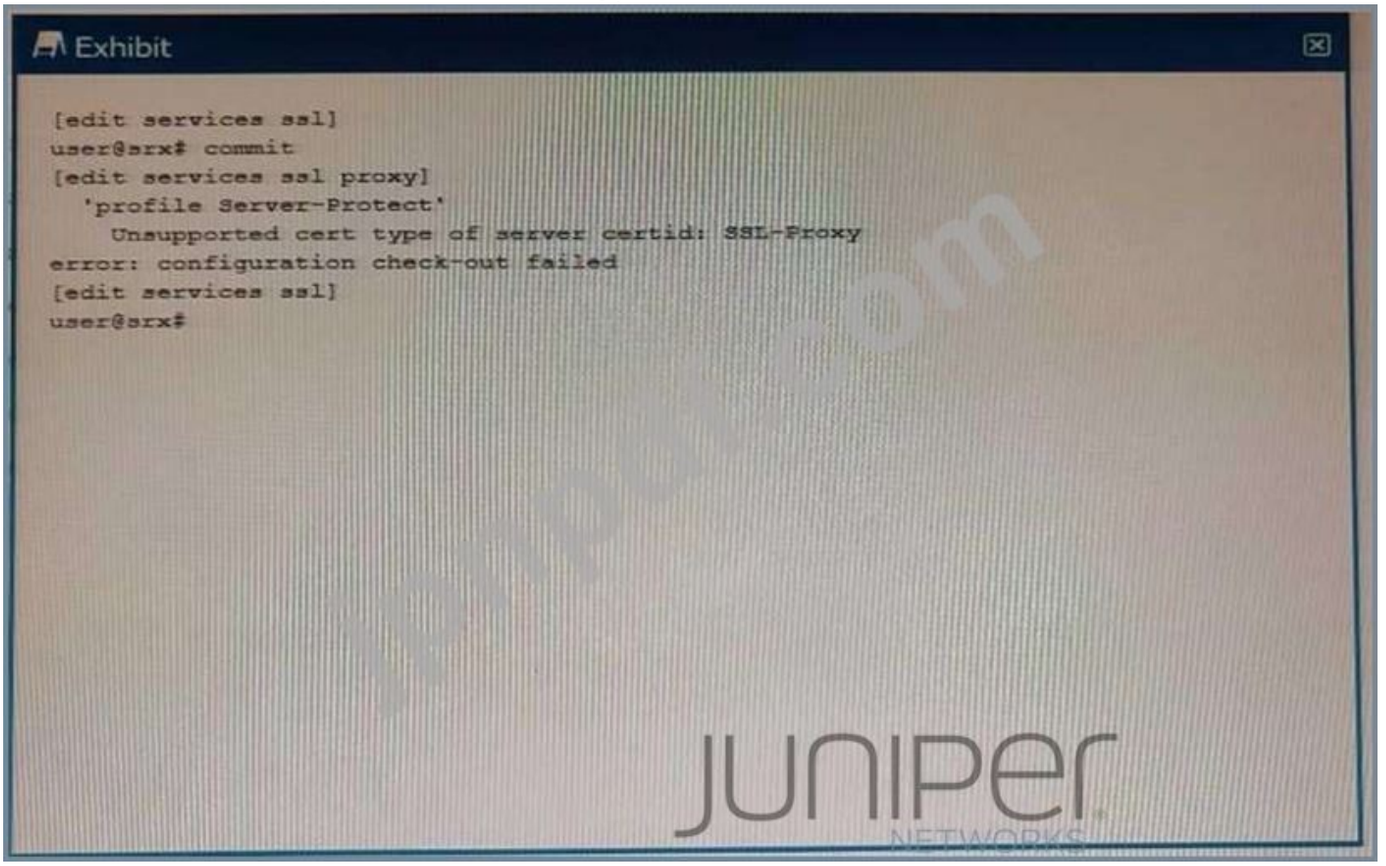
最新問題: **94**
Policy Enforcer による DDoS 保護に使用する 2 つのデバイスはどれですか? (2つお選びください。)
A. vQFX
B. MX
C. vMX
D. QFX
Answer: (解答を表示する**)**
MX および vMX デバイスは、Policy Enforcer による DDoS 保護に使用できます。Policy Enforcer は、DDoS 攻撃からのリアルタイム保護を提供するジュニパーネットワークスのソリューションです。これを使用すると、悪意のあるトラフィックを検出してブロックできるほか、ユーザー アクセスとポリシーの適用をきめ細かく制御することもできます。MX および vMX デバイスは、高性能ハードウェアと高度なセキュリティ機能により、Policy Enforcer での使用に最適です。

最新問題: **95**
Policy Enforcer による DDoS 保護に使用する 2 つのデバイスはどれですか? (2つお選びください。)
A. vQFX
B. MX
C. vMX
D. QFX
Answer: (解答を表示する**)**
説明
Policy Enforcer は、Junos Space Security Director コンポーネントであり、更新されたセキュリティ ポリシーを Juniper SRX シリーズ ファイアウォール、MX シリーズ 5G ユニバーサル ルーティング プラットフォーム、EX シリーズ イーサネット スイッチ、QFX シリーズ スイッチ、およびサードパーティ ネットワーク デバイス全体に展開できるようにします1。Policy Enforcer は、Juniper デバイスの DDoS 保護機能を利用して、ネットワーク上の DDoS 攻撃を検出および軽減できます。DDoS 保護機能は、2 つの主要なコンポーネントに基づいています。1 つはホスト宛のコントロール プレーン トラフィックの分類、もう 1 つは各プロトコル タイプがホストに送信できるコントロール プレーン トラフィックの量を制限する個別レベルおよび集約レベルのポリサーの階層セットです。処理用のルーティング エンジン (RE)2。DDoS 保護機能は、MX シリーズ ルーターや QFX シリーズ スイッチなどのデバイスでサポートされています3。したがって、Policy Enforcer による DDoS 保護に使用する正しいデバイスは MX および QFX です。
他のオプションは次の理由により正しくありません。
vQFX は、テストおよび開発目的で QFX シリーズ スイッチをエミュレートする仮想スイッチです。DDoS 保護機能はサポートしていません4。

vMX は、テストおよび開発目的で MX シリーズ ルーターをエミュレートする仮想ルーターです。DDoS 保護機能はサポートしていません。
参考資料: Policy Enforcer DDoS Protection Case Study 分散型サービス拒否 (DDoS) 攻撃に対する保護 vQFX10000 の概要 [vMX の概要]

最新問題: **96**
Junos アプリケーション ファイアウォール機能をネットワークに展開しています。
このシナリオでは、アプリケーション システム キャッシュ内のアプリケーションにマップされる 2 つの要素はどれですか?
(2つお選びください。)
A. 宛先 IP アドレス
B. 宛先ポート
C. 送信元 IP アドレス
D. 送信元ポート
Answer: A,B (メーッセージを残す**)**

最新問題: **97**
サーバー保護 SSL プロキシを設定しようとすると、次のエラーが表示されます。このエラーの理由は 2 つありますか? (2つお選びください。)



A. SSL プロキシ証明書 ID はブロックリストの一部です。
B. SSL プロキシ証明書 ID には正しい再ネゴシエーション オプション セットがありません。
C. SSL プロキシ証明書 ID は転送プロキシ用です。

D. SSL プロキシ証明書 ID が存在しません。
Answer: (解答を表示する**)**
このエラーの原因としては、SSL プロキシ証明書 ID が存在しないこと、または SSL プロキシ証明書 ID がブロックリストの一部であることが 2 つ考えられます。SSL プロキシ証明書 ID が存在しない場合は、新しい証明書を生成する必要があります。SSL プロキシ証明書 ID がブロックリストの一部である場合、ブロックリストのソースに連絡して削除する必要があります。さらに、サーバーを適切に保護するために必要なため、SSL プロキシ証明書 ID に正しい再ネゴシエーション オプションが設定されていることを確認する必要がある場合があります。

最新問題**: 98**
Juniper ATP Cloud について正しい 2 つの記述はどれですか? (2つお選びください。)
A. 目標のしきい値に達すると、Juniper ATP Cloud は 0 ～ 5 分間脅威を探し続けます。
B. 目標のしきい値に達すると、Juniper ATP Cloud は 0 ～ 10 分の範囲の脅威レベルを探し続けます。
C. 脅威レベルの範囲は 0 ～ 10 です。
D. 脅威レベルの範囲は 0 ～ 100 です。
Answer: A,C (メーッセージを残す**)**
Juniper Networks JNCIS-SEC Study Guide によると、Juniper ATP Cloud はセキュリティ イベントの目標しきい値を設定し、このしきい値を超えるアクティビティがないか環境を継続的にスキャンします。しきい値に達すると、Juniper ATP Cloud は 0 ～ 5 分間脅威の検索を続けます。脅威レベルの範囲は 0 ～ 10 で、0 が最低、10 が最高です。

最新問題**: 99**
SRX シリーズ デバイスに IPS を実装するように求められます。
このシナリオでは、構成が機能する前にどの 2 つのタスクを完了する必要がありますか? (2つお選びください。)
A. IPS シグネチャ データベースをダウンロードします。
B. SRX シリーズ デバイスを Juniper ATP Cloud に登録します。
C. IPS シグネチャ データベースをインストールします。
D. SRX シリーズ デバイスを再起動します。
Answer: (解答を表示する**)**
SRX シリーズ デバイス上の IPS の構成が機能する前に完了する必要がある 2 つのタスクは、IPS シグネチャ データベースのダウンロードと IPS シグネチャ データベースのインストールです。セキュリティ スペシャリスト (JNCIS-SEC) スタディ ガイドには、IPS シグネチャ データベースをダウンロードしてインストールする方法の詳細が記載されています。構成を機能させるために SRX シリーズ デバイスを Juniper ATP Cloud に登録する必要はなく、SRX シリーズ デバイスを再起動する必要もありません。

Valid JN0-335 Dumps shared by GoShiken.com for Helping Passing JN0-335 Exam! GoShiken.com now offer the **newest JN0-335 exam dumps**, the GoShiken.com JN0-335 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com JN0-335 dumps with Test Engine here: https://www.goshiken.com/Juniper/JN0-335-mondaishu.html (**200** Q&As Dumps, **30%OFF** **Special Discount:** **Freepdfdumps**)