Juniper.JN0-336.v2026-06-18.q38

試験コード：	JN0-336
試験名称：	Security, Specialist (JNCIS-SEC)
認証ベンダー：	Juniper
無料問題の数：	38
バージョン：	v2026-06-18
ページの閲覧量：	105
問題集の閲覧量：	403

https://www.jpnshiken.com/shiken/Juniper.JN0-336.v2026-06-18.q38.html

質問: **1**
SRXシリーズのデバイスシャーシクラスタに関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. シャーシクラスタデータプレーンは収益ポートに接続されています。
B. シャーシクラスタには最大3台のデバイスを搭載できます。
C. シャーシクラスタデータプレーンはSPCポートに接続されています。
D. シャーシクラスタには最大2台のデバイスを搭載できます。
正解: **A,D (**コメントを発表する**)**
SRXシリーズのデバイスシャーシクラスタに関して正しい記述は次の2つです。
シャーシクラスタのデータプレーンは収益ポートに接続されています。シャーシクラスタは、2台の同一のSRXシリーズデバイスをクラスタにグループ化し、単一のデバイスとして動作させる高可用性機能です。クラスタには、制御リンクとファブリックリンクの2種類のリンクがあります。制御リンクは、ノード間でハートビートメッセージの交換と構成の同期に使用されます。ファブリックリンクは、ノード間でデータトラフィックを転送するために使用されます。ファブリックリンクは収益ポートに接続されています。収益ポートは、クラスタモードでない場合は通常のトラフィックにも使用できる、通常のイーサネットインターフェイスです。
シャーシクラスタには最大2台のデバイスを収容できます。シャーシクラスタは、ノード0とノード1の2つのノードのみで構成されます。ノードは同じモデル、同じハードウェア構成、同じソフトウェアバージョン、同じライセンスキーを備えている必要があります。ノードは共通の構成を共有し、障害発生時には互いにバックアップとして機能します。
参考資料 :SRXシリーズデバイスでのシャーシクラスタリングの設定、SRXシリーズシャーシクラスタ構成の概要、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を作成する

質問: **2**
展示する

Exhibit

```
(primary:node0)
user@srx> show chassis cluster status
Cluster ID: 3
Node                  Priority          Status    Preempt  Manual failover
Redundancy group: 0 , Failover count: 1
    node0                   129         primary      no       no
    node1                   128         secondary    no       no
Redundancy group: 1 , Failover count: 3
    node0                   0           primary      no       no
    node1                   0           secondary    no       no
```

展示資料の情報に基づいて、正しい記述はどれですか？

A. 冗長グループ1は不適格状態です。

B. Node1は制御プレーンのアクティブノードです

C. 冗長グループ0は不適格な状態です。

D. クラスターに問題はありません。

正解: **(**正解を表示します**)**

質問: **3**

reth LAG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. リンクは同じ速度とデュプレックス設定である必要があります。

B. リンクには同じ種類のケーブル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である必要があります。

D. インターフェースは2つ以上必要です。

正解: **(**正解を表示します**)**

reth LAGは、シャーシクラスタ内で複数の物理インターフェイスを単一の論理インターフェイスに結合する冗長イーサネットリンクアグリゲーショングループです。reth LAGは、冗長グループ内または冗長グループ間のトラフィックに対して負荷分散と冗長性を提供します。reth LAGについて正しい記述は次の2つです。
リンクは同じ速度とデュプレックス設定である必要があります。reth LAGを形成するには、物理インターフェースは同じ速度とデュプレックス設定である必要があります。これにより、リンクが同じ容量で動作し、パフォーマンスの問題やエラーを回避できます。
インターフェースは2つ以上必要です。reth LAGを作成するには、少なくとも2つの物理インターフェースが必要です。1つのインターフェースはノード0に接続し、もう1つのインターフェースはノード1に接続する必要があります。帯域幅と冗長性を高めるために、reth LAGに2つ以上のインターフェースを含めることもできます。
参考資料：冗長イーサネットインターフェースの設定、[冗長イーサネットインターフェースの理解]

質問: **4**
Junosが生成するシステムログには、どのような種類がありますか？ 2つ選択してください。）
A. SQLログファイル
B. データプレーンログ
C. システムコアダンプファイル
D. コントロールプレーンログ
正解: **(**正解を表示します**)**
Junosが生成するシステムログには、コントロールプレーンログとデータプレーンログの2種類があります。コントロールプレーンログはJunosオペレーティングシステムによって生成され、システムの起動とシャットダウン、構成変更、システムアラームなどのシステムレベルのイベントが含まれます。データプレーンログはネットワークプロトコルプロセスによって生成され、ルーティング、ファイアウォール、NAT、IPSなどのネットワークとそのコンポーネントの状態に関するメッセージが含まれます。SQLログファイルとシステムコアダンプファイルは、Junosが生成するシステムログの種類ではありません。

質問: **5**
展示する

Exhibit

```
user@srx> show security flow session
Session ID: 61524, Policy name: Internet-access/9, Timeout: 48, Valid
  In: 10.10.12.37/37466 --> 10.111.111.254/80;tcp, Conn Tag: 0x0, If: ge-
0/0/0.0, Pkts: 3, Bytes: 1023,
  Out: 10.111.111.254/80 --> 10.10.12.37/9241;tcp, Conn Tag: 0x0, If: ge-
0/0/1.0, Pkts: 0, Bytes: 0,
user@srx> show services application-identification application-system-cache
Application System Cache Configurations:
  application-cache: on
    Cache lookup for security-services: off
    Cache lookup for miscellaneous-services: on
  cache-entry-timeout: 3600 seconds
pic: 0/0
Logical system name: root-logical-system
```


展示物に関して、次のうち正しい記述はどれですか？

A. SSLプロキシ機能はセッションを無視します。

B. SSLプロキシは試合前の結果を利用します

C. SSLプロキシは、最終的なマッチングが行われるまで戻りトラフィックを待つ必要があります。

D. SSLプロキシは試合後の結果を利用します。

正解: **(**正解を表示します**)**

質問: **6**

同一のデバイスで5分以内に3回以上誤ったパスワードが使用された場合に、アラートを受け取りたい。

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. 適応型脅威プロファイリング

B. Juniper Secure Analytics

C. Juniper Identity Management Service
D. 侵入防止システム
正解: **(**正解を表示します**)**
5分以内に1台のデバイスで誤ったパスワードが3回以上使用された場合にアラートを発するタスクを実行するJuniper Networksのソリューションは、Juniper Secure Analytics（JSA）です。JSAは、ファイアウォール、ルーター、スイッチ、サーバー、アプリケーションなど、さまざまなソースからネットワークデータを収集、分析、相関付けるセキュリティインテリジェンスプラットフォームです。JSAは、ルール、違反、レポート、ダッシュボードを使用して、脅威、異常、脆弱性をリアルタイムで検出して対応できます。また、JSAはJIMS（Juniper Identity Management Service）と統合して、Active DirectoryドメインまたはsyslogソースからユーザーID情報を取得することもできます。JSAはこの情報を使用して、ログイン失敗やパスワード変更などのユーザーの行動やアクティビティに基づいて違反やアラートをトリガーするカスタムルールを作成できます。
参考資料 :Juniper Secure Analyticsトラブルシューティングガイド、Juniper Identity Management Serviceユーザーガイド

質問: **7**
イベントログのタイムスタンプの順序が乱れているため、JIMSサーバーで予期せぬ問題が発生しており、トラブルシューティングを行っています。
この問題を解決するために、どのような行動を取るべきでしょうか？
A. クライアントデバイスで時刻同期を有効にします。
B. JIMSサーバーで時刻同期を有効にします。
C. ドメインコントローラで時刻同期を有効にします。
D. SRXシリーズ機器で時刻同期を有効にします。
正解: **(**正解を表示します**)**
JIMS サーバーでイベント ログのタイムスタンプの順序が乱れる問題を解決するには、ドメイン コントローラで時刻同期を有効にする必要があります。JIMS (Juniper Identity Management Service) は、Active Directory ドメインまたは syslog ソースからユーザー、デバイス、およびグループ情報を収集し、ID ベースのセキュリティ ポリシーのために SRX シリーズ デバイスと CSO に提供する Windows サービスです。JIMS は、ドメイン コントローラによって生成されたイベント ログのタイムスタンプを使用して、ユーザーのログイン、ログアウト、および IP アドレスの変更を追跡します。ドメイン コントローラのクロックが異なっていたり、不正確だったりすると、イベント ログのタイムスタンプの順序が乱れたり、誤ったタイムスタンプが記録されたりして、JIMS が一部のイベントを見逃したり、誤って解釈したりして、その精度とパフォーマンスに影響を与える可能性があります。そのため、ネットワーク内のすべてのドメイン コントローラが、NTP サーバーや Windows タイム サービスなどの信頼できる時刻ソースと同期されていることを確認してください。参照資料 :Juniper Identity Management Serviceユーザーガイド、Juniper Identity Management Service機能ガイド、JIMSコレクターによるMicrosoftイベントログの取得設定、集中ログプラットフォームにおけるタイムスタンプに関する考慮事項

質問: **8**
SSLプロキシサーバーの保護に関する記述として正しいものはどれですか？（2つ選択してください。）
A. SRXシリーズデバイスのSSLプロキシ機能を使用するためにサーバーを設定する必要はありません。
B. SRXシリーズデバイスにサーバー証明書をロードする必要があります。
C. サーバーは、SRXシリーズデバイスのSSLプロキシ機能を使用するように設定する必要があります。
D. サーバーにルートCAをインポートする必要があります。
正解: **(**正解を表示します**)**
SSLプロキシを使用する場合、サーバー側でSRXデバイスのSSLプロキシ機能を利用するための特別な設定は必要ありません。SSLプロキシは透過的に動作し、SSL/TLSトラフィックがサーバーに到達する前に傍受して復号化します。

SSLプロキシが効果的に機能するためには、特にサーバー保護モードでは、サーバーになりすましてクライアントに情報を伝えるため、サーバーの証明書をSRXデバイスにロードする必要があります。これにより、SRXはサーバーの認証情報を使用してクライアントとの信頼できる接続を確立できます。

質問: **9**
SRX5800では、シャーシクラスタの帯域外管理にはどのポートが使用されますか？
A. Txp0
B. ユーザー定義
C. fxp1
D. ge-0/0/0
正解: **(**正解を表示します**)**

質問: **10**
誤検知の発生をなくすために、IPS（侵入検知システム）の適用除外となるルールベースを作成するよう求められています。
トラフィックの検査対象から除外するために使用できる設定パラメータはどれですか？ 2つ選択してください。）
A. ソースポート
B. 送信元IPアドレス
C. 宛先IPアドレス
D. 目的地港
正解: **(**正解を表示します**)**
送信元IPアドレスまたはIPアドレス範囲を指定することで、特定のネットワークセグメントやデバイスからのトラフィックを除外できます。これは、既知の安全な送信元からのトラフィックをホワイトリストに登録し、それ以外の場合にIPSシステムで誤検知が発生するのを防ぐのに役立ちます。
同様に、宛先IPアドレスまたはアドレス範囲を指定することで、特定のネットワークホストまたはセグメント宛てのトラフィックを除外できます。これにより、信頼できる内部リソースや安全性が確認されている特定の外部サービス宛てのトラフィックに対する誤検知を減らすことができます。

質問: **11**
アプリケーション層ゲートウェイ（ALG）の機能を定義しているのは、次のうちどれですか？
A. ALGは、特定のIPアドレス範囲を許可または拒否するために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。
正解: **(**正解を表示します**)**
アプリケーション層ゲートウェイ（ALG）の機能を定義する記述は次のとおりです。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（レイヤー7）で動作するセキュリティコンポーネントであり、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します。ALGは、クライアントアプリケーションとサーバーアプリケーション間のプロキシまたは仲介役として機能し、アドレスとポートの変換、リソース割り当て、アプリケーション応答制御、データと制御トラフィックの同期など、さまざまな機能を実行します。ALGはまた、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、なりすましや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きめ細か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。参照 :=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？ | F5、ALGとは
** アプリケーション層ゲートウェイ | 3CX

質問: **12**
AppQoEを有効にするための要件を2つ挙げてください。（2つ選択してください。）
A. SRXシリーズのデバイスエンドポイントが2つ必要です。
B. SRXシリーズまたはMXシリーズのデバイスエンドポイントが2台必要です。
C. APPID機能ライセンスが必要です。
D. 逆方向トラフィック用にAppQoEを設定する必要があります。
正解: **(正解を表示します)**
AppQoEは、ネットワーク上のアプリケーションのユーザーエクスペリエンス品質を監視および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機能も提供します。
AppQoEを有効にするための2つの要件は以下のとおりです。
SRXシリーズまたはMXシリーズのデバイスエンドポイントが2台必要です。AppQoEは、2台の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構成もしくはフルメッシュ構成のSRXシリーズデバイスとMXシリーズデバイス間で設定できます。デバイスは同じバージョンのJunos OSを実行し、同じAppQoE構成になっている必要があります。
APPID機能ライセンスが必要です。AppQoEを使用するには、SRXシリーズ端末に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機能ライセンスは、AppQoEの動作に不可欠なアプリケーションの識別と分類を可能にします。
参考資料 :アプリケーション品質エクスペリエンスの概要、アプリケーション品質エクスペリエンスの概要 - Juniper Networks、アプリケーション品質エクスペリエンス | Junos OS | Juniper Networks

質問: **13**
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なセッションのデフォルトの動作について、正しい記述はどれですか？
A. ポリシーで許可されているアクティブ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なセッションを破棄します。
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切断します。
D. ポリシーで許可されているアクティブセッションは変更されません。
正解: **(正解を表示します)**
SRXシリーズデバイスでセキュリティポリシーを変更すると、デフォルトでは、ポリシーに一致する既存のセッションは変更されずに継続されます。つまり、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。このコマンドは、変更されたポリシーに一致するすべてのセッションをクリアし、新しいポリシーを再評価するように強制します。参照 :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）

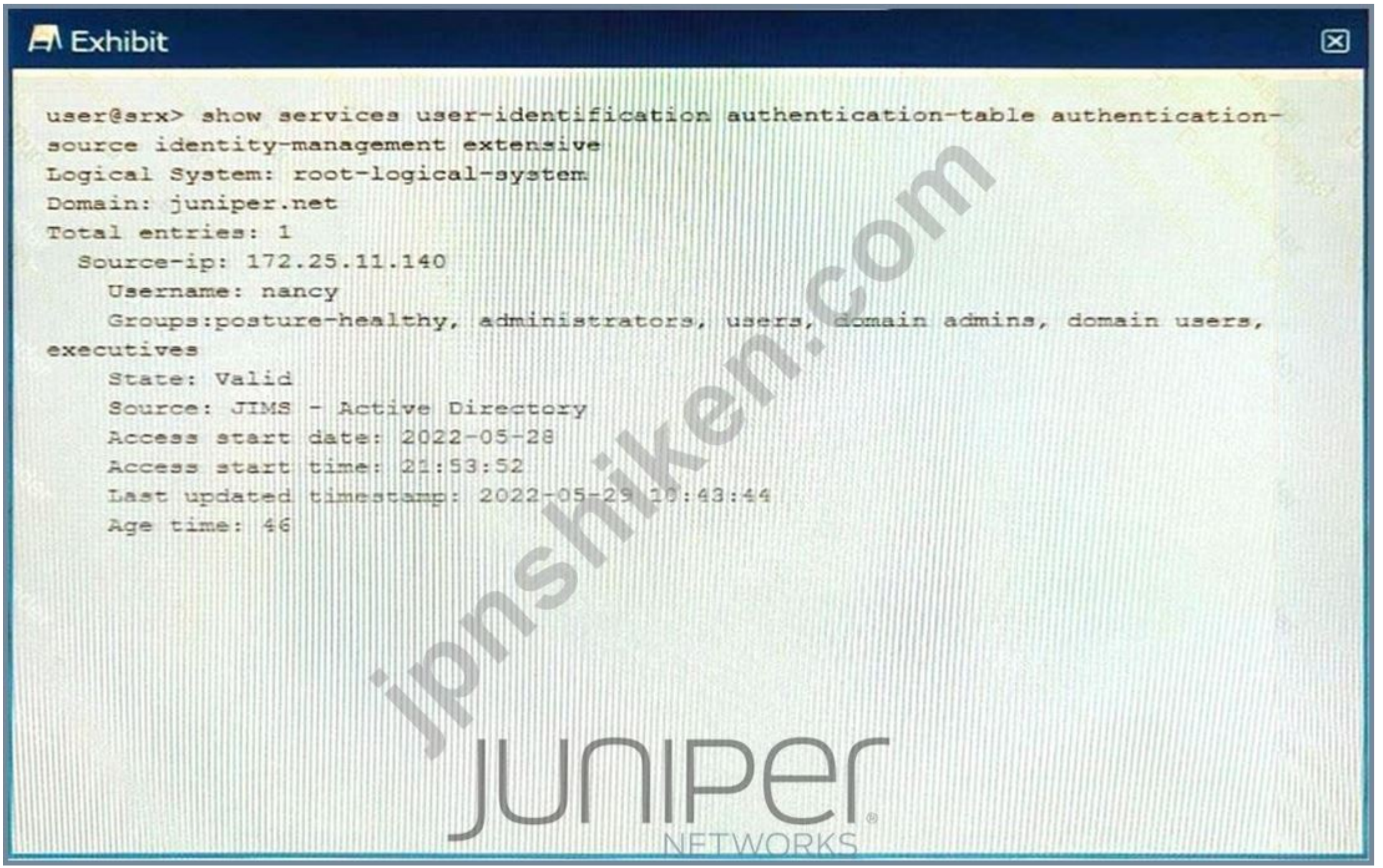
質問: **14**
お使いのJIMSサーバーはイベントログを表示できません。
この問題を解決するために、あなたはどのような行動を2つ取りますか？ （2つ選択してください。）
A. SRXシリーズデバイスで正しいホスト受信トラフィックルールを有効にします。
B. 必要なExchangeサーバー上のWindowsファイアウォールでリモートイベントログ管理を有効にします。
C. 必要なドメインコントローラーで、Windowsファイアウォール内のリモートイベントログ管理を有効にします。
D. JIMSサーバー上のWindowsファイアウォールでリモートイベントログ管理を有効にします。

正解: **(**正解を表示します**)**
JIMSは、ネットワーク全体でのユーザーおよびデバイスのアクティビティを追跡するために、ドメインコントローラーのイベントログにアクセスする必要があります。ドメインコントローラーのWindowsファイアウォールがこのアクセスをブロックしている場合は、リモートイベントログ管理を有効にすることで、JIMSが必要な情報を取得できるようになります。
あまり一般的ではありませんが、JIMSサーバー自体のファイアウォール設定が、イベントログ管理に関連する送信リクエストやレスポンスをブロックしないようにすることも非常に重要です。これにより、JIMSは自身のファイアウォールによる妨害を受けることなく、リクエストを送信し、レスポンスを受信できるようになります。

質問: **15**
Juniper Identity Management Service (JIMS) ドメイン PC プローブに関する記述として正しいのはどれですか？
A. JIMSドメインPCプローブは、デフォルトで60分間隔でドメインコントローラのセキュリティイベントログを分析します。
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、SRXシリーズデバイスによって開始され、認証テーブル情報を検証します。
正解: **(**正解を表示します**)**
Juniper Identity Management Service (JIMS) ドメイン PC プローブは、ドメイン セキュリティ イベント ログ内でユーザー名と IP アドレスをマッピングするために使用されます。これにより、SRX シリーズ デバイスはグループ メンバーシップなどの認証テーブル情報を検証できます。プローブは、ドメイン セキュリティ イベント ログ内でユーザー名と IP アドレスのマッピングが見つからない場合にトリガーされます。デフォルトでは、プローブは 60 分間隔で実行されます。

質問: **16**
帯域幅が狭く、かつ発信ポリシーが全てのトラフィックを許可するクラウドベースのVoIPソリューションを使用している支店に、SRXシリーズのデバイスを導入しようとしています。
このシナリオにおいて、VoIPトラフィックを優先させるために、エッジデバイスにどのサービスを実装しますか？
A. AppFW
B. SIP ALG
C. AppQoE
D. AppQoS
正解: **(**正解を表示します**)**
このシナリオでエッジデバイスに実装してVoIPトラフィックを優先させるサービスはAppQoSです。AppQoSは、アプリケーションシグネチャまたはカスタムルールに基づいて帯域幅を割り当て、トラフィックを優先できる機能です。AppQoSは、VoIPなどの重要度の高いアプリケーションやレイテンシに敏感なアプリケーションのサービス品質とユーザーエクスペリエンスを向上させることができます。AppQoSポリシーを設定することで、異なるアプリケーションやトラフィックフローに異なるサービスクラス（CoS）値またはキュー番号を割り当てることができます。また、各クラスまたはキューに対して帯域幅制限、保証、またはバーストを定義することもできます。参照：
[アプリケーションサービス品質の概要]、[アプリケーションサービス品質の設定]

質問: **17**
展示する



展示物に関して、正しい記述は次のうちどれですか？ 2つ選択してください。）

A. ナンシーはActive Directoryの営業グループのメンバーです。
B. ナンシーはjuniper.net Active Directoryドメインにログインしました。
C. ナンシーのクライアント PC の IP アドレスは 172.25.11 です。
D. 認証ドメインコントローラのIPアドレスは172.25.11.140です。

正解: **(**正解を表示します**)**

質問: **18**
ポリシー再マッチング機能を使用する際のセキュリティポリシーの変更に関して、正しい記述を2つ選択してください。
A. ポリシー変更にポリシーのアクションを許可から拒否に変更することが含まれる場合、既存のセッションはすべて維持されます
B. ポリシーの変更に、ポリシーの送信元または宛先アドレスの一致条件の変更が含まれる場合、既存のセッションはすべて破棄されます。
C. ポリシーの変更に、ポリシーのアクションを許可から拒否に変更することが含まれる場合、既存のセッションはすべて破棄されます。
D. ポリシーの変更に、ポリシーの送信元または宛先アドレスの一致条件の変更が含まれる場合、既存のすべてのセッションが再評価されます。
正解: **C,D (**コメントを発表する**)**
ポリシー再マッチングは、関連付けられたセキュリティポリシーが変更された際に、デバイスがアクティブなセッションを再評価できるようにする機能です。セッションは、最初にセッションを許可したポリシーに引き続き一致する場合は開いたままになります。関連付けられたポリシーの名前が変更されたり、無効化されたり、削除されたりした場合は、セッションは閉じられます。

質問: **19**
SRXシリーズデバイスにIPSを実装するよう依頼されています。
このシナリオでは、設定が正しく機能するために完了しなければならないタスクはどれですか？ 2つ選択してください。）
A. IPS署名データベースをダウンロードしてください。
B. SRXシリーズデバイスをJuniper ATP Cloudに登録します。
C. IPS署名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。
正解: **A,C (**コメントを発表する**)**
SRXシリーズデバイスでIPSの設定を有効にするには、IPSシグネチャデータベースのダウンロードとインストールという2つの作業を完了する必要があります。セキュリティスペシャリスト（JNCIS-SEC）の学習ガイドには、IPSシグネチャデータベースのダウンロードとインストール方法の詳細が記載されています。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。

質問: **20**
vSRX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. VMXNET3 vNICはサポートされていません。
B. VMXNET3 vNICをサポートしています。
C. UNIXが基本OSです。
D. LinuxがベースOSです。
正解: **(**正解を表示します**)**
参考資料 :Juniper Networks Security, Specialist (JNCIS-SEC) 学習ガイド、第 1 章 :Junos Security の概要、1-8 ページ。
vSRXは、仮想マシン上で動作する仮想セキュリティアプライアンスです。仮想化環境において、ファイアウォール、VPN、その他のセキュリティサービスを提供します。
vSRXは、仮想化に最適化されたJunos OSのバージョンをベースとしています。Linuxカーネル上で動作し、KVMハイパーバイザーを使用します。VMware ESXiとKVMハイパーバイザーをサポートしています。
vSRXは、VMwareが提供する高性能仮想ネットワークインターフェイスであるVMXNET3 vNICをサポートしています。これらのインターフェイスは、他の仮想NICタイプよりも高いスループットと低いCPU使用率を実現できます。

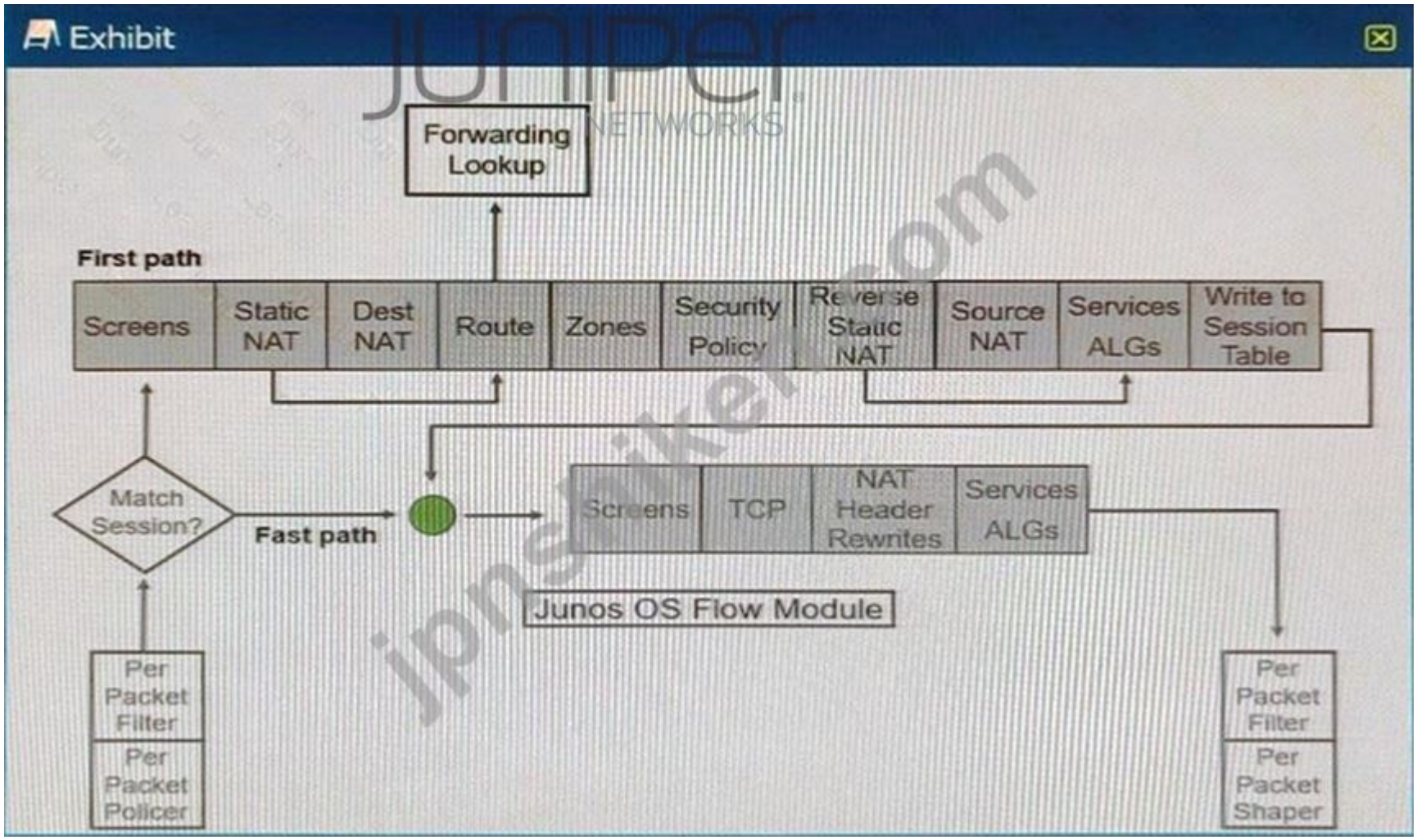
質問: **21**
JSAが外部イベントとフローを受信した後、どの2つのステップが実行されますか？ 2つ選択してください。）
A. データのフォーマット後、データは資産データベースに保存されます。
B. データのフォーマットを行う前に、関連情報についてデータを分析します。
C. 情報がフィルタリングされる前に、情報はフォーマットされます
D. 情報がフィルタリングされた後、JSAは積極的な対策で対応します。
正解: **(**正解を表示します**)**
JSA（Juniper Secure Analytics）が外部イベントとフローを受信すると、一般的な処理手順は次のようになります。
選択肢C：情報がフィルタリングされる前に、情報はフォーマットされます。
データフォーマットは、イベントやフローからの生データを、JSAがより容易に処理および分析できる標準フォーマットに変換するプロセスの最初のステップです。
オプションA :データのフォーマット後、データは資産データベースに保存されます。
データがフォーマットされると、資産データベースに保存されます。このデータベースは、フォーマットされたすべてのデータの保管場所として機能し、JSAがさらなる分析や相関分析を行い、最終的にはネットワーク資産と活動の包括的なビューを維持できるようにします。
これらの手順は、JSAの包括的なセキュリティイベント管理アプローチの一環であり、潜在的なセキュリティ上の脅威や脆弱性を効率的に特定するために、データの収集、正規化、分析を行うものです。

質問: **22**
SRXファイアウォールで作業しているときに、show security policies policy-name <name> detail コマンドを実行します。
このコマンドはどのような機能を果たしますか？
A. デフォルトのセキュリティポリシーの詳細を表示します。
B. 有効になっているさまざまなカスタムポリシーを識別します。
C. ローカルのSRXシリーズデバイスのシステムログファイルを表示します。
D. 設定済みのポリシーのポリシーカウンターを表示します。
正解: **(**正解を表示します**)**
show security policies policy-name <name> detail コマンドの機能は、設定済みのポリシーのポリシーカウンタを表示することです。ポリシーカウンタは、トラフィックによってポリシーが一致した回数と、ポリシーによって実行されたアクションを示す統計情報です。ポリシーカウンタは、セキュリティポリシーのパフォーマンスと有効性を監視およびトラブルシューティングするのに役立ちます。show security policies policy-name <name> detail コマンドは、特定のポリシーのソースゾーン、宛先ゾーン、説明、状態、ヒット数、バイト数、パケット数、アクション数、セッション数などの詳細情報を表示します。
参照: = セキュリティ ポリシーの表示、セキュリティ ポリシー情報の表示、[SRX] データが渡されないセキュリティ ポリシーのトラブルシューティング方法

質問: **23**
シャーシクラスタ内のファブインターフェースについて、正しい記述を2つ選択してください。
A. セッション同期を維持するために、ファブインターフェース上でリアルタイムオブジェクト（RTO）が交換されます。
B. アクティブ/アクティブ構成では、シャーシ間のトランジットトラフィックはファブインターフェースを介して送信されます。
C. ファブインターフェースにより、構成の同期が可能になります。

D. ファブインターフェースで送信されるハートビート信号は、制御プレーンリンクの状態を監視します。
正解: **(**正解を表示します**)**
ファブインターフェースは、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。シャーシクラスタは、2つの同一のSRXシリーズデバイスをクラスタにグループ化し、単一のデバイスとして動作させる高可用性機能です。
ファブインターフェースには2つの機能があります。
リアルタイムオブジェクト（RTO）は、セッション同期を維持するためにファブインターフェース上で交換されます。RTOは、送信元および宛先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格納するデータ構造です。RTOはファブインターフェー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、フェイルオーバーが発生した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、シャーシ間のトランジット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へ同時にフェイ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。トラフィックが1つのRGから別のノードでアクティブな別のRGへ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。
参考資料：SRXシリーズデバイスでのシャーシクラスタリングの設定、シャーシクラスタ冗長グループ、シャーシクラスタデータプレーン

質問: **24**
展示する



図に示されているSRXシリーズのフローモジュール図を参照すると、アプリケーションセキュリティはどこで処理されますか？
A. サービスALG
B. 転送ルックアップ

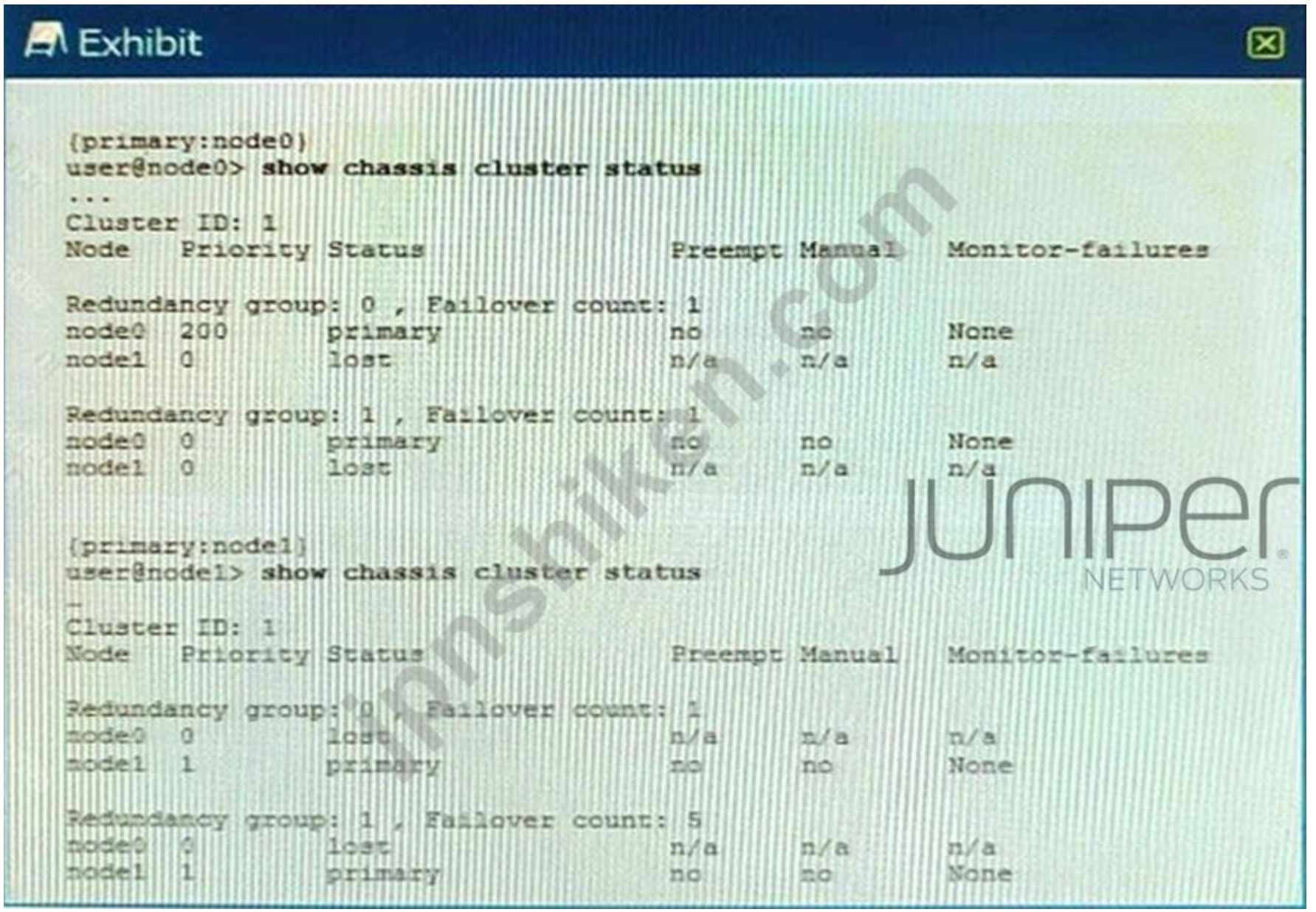
C. スクリーン
D. セキュリティポリシー
正解: **(**正解を表示します**)**

質問: **25**
JIMSサーバーがあなたのシステムにかける負荷を軽減するようにお願いします。
このような状況では、どのような行動を取るべきでしょうか？
A. JIMSをRADIUSサーバーに接続します
B. JIMSをドメインのExchangeサーバーに接続する
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。
正解: **D (**コメントを発表する**)**
JIMSサーバーは、SRXシリーズデバイス12のさまざまな認証ソースからユーザーID情報を収集するJuniper Identity Management Serviceです。ネットワーク内のSRXシリーズデバイスおよびCSOプラットフォームに接続できます1。

質問: **26**
運用モードコマンドの表形式データを表示したいのですね。
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
正解: **(**正解を表示します**)**
運用モードコマンドの表形式データを表示する機能を提供するログパラメータは count です。count パラメータは、セキュリティポリシーに一致するパケット数とバイト数、およびポリシーによって実行されたアクションを表示します。count パラメータは、show security policies hit-count コマンドと組み合わせて使用することで、ポリシーカウンタを表形式で表示できます。また、count パラメータは、show security flow session コマンドと組み合わせて使用することで、セッションカウンタを表形式で表示することもできます。参照: show security policies hit-count、show security flow session

質問: **27**
SRXシリーズのデバイスシャーシクラスタに関する記述のうち、正しいものはどれですか？ 2つ選択してください。）
A. 各シャーシクラスタメンバデバイスはアクティブ冗長グループをホストできます
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. 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。
D. 冗長グループ0はクラスタバックアップノードでのみ有効です。
正解: **A,C (**コメントを発表する**)**
シャーシクラスタでは、両方のノードがアクティブな冗長グループをホストできます。アクティブな冗長グループは、構成とフェイルオーバーの状態に応じて2つのノード間で分散され、各ノードが異なるサービスまたはインターフェイスのトラフィックを処理できるようになります。
シャーシクラスタリングが正しく機能するためには、クラスタ内の両方のノードが同じモデルである必要があります。
この要件は、処理能力やインターフェースの互換性といったハードウェア機能が同一であることを保証するものであり、クラスタノード間で一貫したパフォーマンスと動作を維持するために不可欠です。

質問: **28**
展示する



展示物を参照して、そのクラスターの状態についてどのようなことが分かりますか？
A. クラスターに問題はありません。
B. 両方のノードがプライマリ状態にあると判断します。
C. ノード2がダウンしています。
D. ノード1がダウンしています
正解: **(**正解を表示します**)**

質問: **29**
App Track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. App Trackは、SRXシリーズデバイス上の任意の定義済み論理システムに対して構成できます。
B. App Trackは、使用されているポートに関係なく、悪意のある可能性のあるトラフィックフローを識別してブロックします。
C. App Trackは、バイト、パケット、および期間の統計情報を含むトラフィックフロー情報を収集します。

D. App Trackは、SRXシリーズデバイスのメイン論理システムでのみ設定できます。
正解: **(**正解を表示します**)**
AppTrackは、SRXシリーズデバイス上のアプリケーショントラフィックを監視および分析できる機能です。物理デバイス内の仮想ルーターまたはスイッチである、定義済みの任意の論理システムに対して構成できます。AppTrackは、各アプリケーションフローのバイト数、パケット数、期間などの統計情報を収集し、レポートまたはログに表示します。AppTrackは悪意のあるトラフィックを識別またはブロックしません。これはAppSecureまたはIDP/IPSの機能です。参照 := 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)、アプリケーションセキュリティ理論

質問: **30**
展示する

Exhibit

```
user@srx> show services security-intelligence category summary
Category name      :CC
  Status           :Enable
  Description      :Command and Control data schema
  Update interval  :1800s
  TTL              :3456000s
  Feed name        :cc_cert_sha1_data
    Version        :20221103.1
    Objects number:0
    Create time    :2022-11-08 19:49:02 UTC
    Update time    :2022-11-08 20:12:23 UTC
    Update status  :Store succeeded
    Expired        :No
    Status         :Active
    Options        :N/A
  Feed name        :cc_ip_data
    Version        :20221102.8
    Objects number:0
    Create time    :2022-11-08 19:50:04 UTC
    Update time    :2022-11-08 20:13:18 UTC
    Update status  :Store succeeded
    Expired        :No
    Status         :Active
    Options        :N/A
  Feed name        :cc_ipv6_data
    Version        :20200626.1
    Objects number:0
    Create time    :2022-11-08 20:00:06 UTC
    Update time    :2022-11-08 20:13:18 UTC
    Update status  :Store succeeded
    Expired        :No
    Status         :Active
    Options        :N/A
  Feed name        :cc_url_data
    Version        :20221108.10
    Objects number:0
    Create time    :2022-11-08 20:02:07 UTC
    Update time    :2022-11-08 20:13:24 UTC
    Update status  :Store succeeded
    Expired        :No
    Status         :Active
    Options        :N/A
```

Juniper ATP Cloudでコマンド＆コントロール（C&C）カテゴリの設定が完了しました。すべてのフィードにオブジェクトがゼロ個含まれていることに気付きました。
この状況において、正しい記述はどれですか？
A. セキュリティインテリジェンスポリシーを設定する必要があります。統一セキュリティポリシー
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. 特に操作は必要ありません。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 エントリ数を設定します。
正解: **(**正解を表示します**)**
Juniper NetworksのJNCIS-SEC学習ガイドによると、Juniper ATP Cloudでコマンド＆コントロール（C&C）カテゴリを設定すると、すべてのフィードには最初はオブジェクトがゼロ個含まれています。
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。この場合、特に操作は必要ありません。ダウンロードが完了すると、フィードにオブジェクトが表示され始めます。

質問: **31**
仮想環境にSRXシリーズデバイスを導入する必要があります。このシナリオにおいて、CSRXを使用するメリットを2つ挙げてください。（2つ選択してください。）
A. cSRXはレイヤ2およびレイヤ3の展開をサポートしています。
B. cSRXのデフォルト設定には、トラスト、アントラスト、管理の3つのデフォルトゾーンが含まれています。
C. cSRXはファイアウォール、NAT、IPS、UTMサービスをサポートします。
D. cSRXはメモリ要件が低い。
正解: **(**正解を表示します**)**
仮想環境でcSRXを使用する2つの利点は次のとおりです。
cSRXは、ファイアウォール、NAT、IPS、UTMサービスをサポートします。cSRXは、Linuxホスト上でDockerコンテナとして動作するSRXシリーズファイアウォールのコンテナ版です。ファイアウォール、NAT、IPS、UTMサービスなど、SRXシリーズの物理ファイアウォールと同じ機能を提供します。cSRXは、仮想ワークロードとアプリケーションをさまざまな脅威や攻撃から保護します。
cSRXはメモリ要件が低い :cSRXは軽量かつ効率的で、メモリとCPUの要件が低いように設計されています。cSRXは最小1GBのRAMと1つのvCPUで動作できるため、リソースが限られた環境に適しています。参照 :cSRX概要、cSRXコンテナファイアウォールデータシート

質問: **32**
仮想化されたSRXを自社環境に導入したいと考えている。
このシナリオでは、cSRXではなくvSRXを使用する理由は何ですか？ （2つ選択してください。）
A. vSRXはレイヤ2とレイヤ3の構成をサポートしています。
B. クラスタリング機能を提供するのはvSRXのみです。
C. vSRXは起動時間が速い。

D. vSRXのみがNAT、IPS、およびUTMサービスを提供します。
正解: **A,B (**コメントを発表する**)**
vSRXは、レイヤ2（データリンク）とレイヤ3（ネットワーク）の両方の構成をサポートする柔軟なネットワーク機能を提供します。これにより、仮想環境内でさまざまなルーティングおよびスイッチングタスクを処理することが可能になります。
クラスタリング機能は、複数のvSRXインスタンスをグループ化して単一のエンティティとして動作させることで冗長性と高可用性を実現する、vSRX固有の機能です。これは、継続的な稼働時間と耐障害性が求められる環境において非常に重要です。

質問: **33**
クライアントが既知のコマンド&コントロールサーバーとの通信を試み、設定された脅威レベルのしきい値に達しました。
この場合、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. 指揮統制クラウドフィード
B. 許可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
正解: **(**正解を表示します**)**
感染ホストとは、マルウェアによって侵害され、外部のC&Cサーバーと通信している内部ホストのことです3。Juniper ATP Cloudは、感染ホストの内部IPアドレスまたはサブネットと脅威レベルを一覧表示する感染ホストフィードを提供します3。感染ホストのJuniper ATP Cloudグローバルしきい値に達すると、そのホストは感染ホストフィードに追加され、クラウドによって脅威レベル10が割り当てられます4。また、セキュリティポリシーを使用して、これらのIPアドレスからのトラフィックをブロックするようにSRXシリーズデバイスを設定することもできます4。

質問: **34**
「展示」ボタンをクリックしてください。

SSLクライアント保護プロキシを実装しました。従業員は図に示すエラーメッセージを受け取っています。
この問題をどう解決しますか？
A. 有効期限切れの既知の有効なCA証明書をSRXシリーズデバイスにロードします。

B. クライアントプロキシとして機能する新しいSRXシリーズデバイスをインストールします。
C. SRXシリーズデバイスを再起動します。
D. 既存の証明書を各クライアントデバイスにインポートします。
正解: **(**正解を表示します**)**
SSLクライアント保護プロキシは、クライアントからサーバーへのSSLトラフィックを復号化して検査できる機能です。これを行うには、SRXシリーズデバイスに認証局（CA）証明書をインストールし、同じ証明書を各クライアントデバイスにインポートする必要があります。これにより、SRXシリーズデバイスはクライアントとサーバー間のプロキシとして機能し、復号化されたトラフィックに対してセキュリティチェックを実行できます。クライアントデバイスに証明書がインストールされていない場合、図に示すようなエラーメッセージが表示されます。参照：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）、SSLプロキシ構成

質問: **35**
お使いのネットワークは単一のJSAホストを使用していますが、クラスタを実装したいと考えています。
このシナリオにおいて、正しい記述はどれですか？（2つ選択してください。）
A. プライマリホストとセカンダリホスト両方のソフトウェアバージョン
B. セカンダリホストは複数のJSAプライマリホストのバックアップを行うことができます。
C. プライマリホストとセカンダリホストは、同じストレージデバイスで構成する必要があります。
D. クラスタ仮想IPには、未使用のIPアドレスを割り当てる必要があります。
正解: **A,D (**コメントを発表する**)**
Juniper NetworksのJNCIP-SEC学習ガイドによると、単一のJSAホストでクラスタをセットアップする場合、プライマリホストとセカンダリホストの両方に同じソフトウェアバージョンがインストールされている必要があります。さらに、未使用のIPアドレスをクラスタの仮想IPアドレスに割り当てる必要があります。プライマリホストとセカンダリホストに同じストレージデバイスを設定する必要はなく、セカンダリホストを複数のJSAプライマリホストのバックアップに使用することはできません。

質問: **36**
Policy Enforcerを使ったDDoS攻撃対策には、どの2つのデバイスを使用しますか？（2つ選択してください。）
A. vQFX
B. MX
C. vMX
D. QFX
正解: **B,C (**コメントを発表する**)**
MXおよびvMXデバイスは、Policy Enforcerを使用してDDoS攻撃対策に利用できます。Policy Enforcerは、DDoS攻撃からリアルタイムで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。悪意のあるトラフィックを検出してブロックできるだけでなく、ユーザーアクセスとポリシー適用をきめ細かく制御することも可能です。
MXおよびvMXデバイスは、高性能なハードウェアと高度なセキュリティ機能を備えているため、Policy Enforcerとの併用に最適です。

質問: **37**
シャーシクラスタ内のファブインターフェースについて、正しい記述を2つ選択してください。
A. Fabリンクはフラグメンテーションをサポートしていません。
B. ファブリンクの物理インターフェースは構成で指定する必要があります。
C. ファブリンクは従来のインターフェース機能をサポートしています。

D. Junos OS は 1 つの Fab リンクのみをサポートします。
正解: **(**正解を表示します**)**
クラスタノード間のデータトラフィック同期に使用されるファブリックリンクは、フルサイズのパケットを処理するように設計されています。パケットの断片化はサポートされていないため、ファブリックインターフェースのパケットサイズ制限に関連する問題を回避するには、パケットサイズを適切に設定する必要があります。
シャーシクラスタリングの場合、ファブリックリンク（ファブリンク）として使用される特定の物理インターフェースを構成ファイルで明示的に定義する必要があります。この仕様は、状態同期やその他のクラスタリング機能において、ノード間の適切なデータフローを確保するために不可欠です。

質問: **38**
現在、サードパーティ製の脅威アナライザーを使用しています。SRXシリーズデバイスから復号化されたSSEトラフィックを.....に送信したいと考えています。
このシナリオでは、SRXデバイスでどの機能を設定する必要がありますか？
A. フェーズ2プロキシID
B. SSL復号ミラーリング
C. IPS IPanotifyアクション
D. JSA脆弱性評価
正解: **C,D (**コメントを発表する**)**