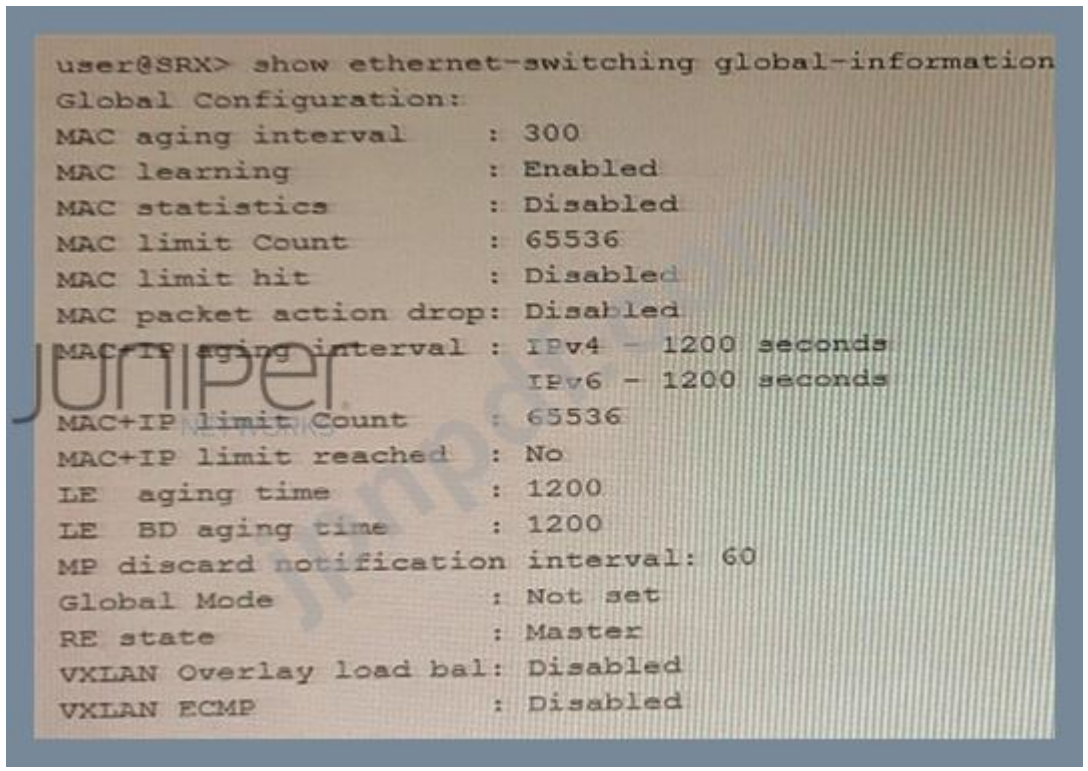
Juniper.JN0-636.v2023-12-28.q82

試験コード:	JN0-636
試験名称:	Security, Professional (JNCIP-SEC)
認定資格:	Juniper
無料問題数:	82
バージョン:	v2023-12-28
アクセス数:	461
ページビュー数:	820
https://www.jpnpdf.com/Juniper.JN0-636.v2023-12-28.q82-mondaishu.html	

最新問題: **1**
示す



同じブロードキャスト ドメイン内にある直接接続された複数のホストのパケットをスイッチングするように SRX シリーズ デバイスを設定しました。ただし、同じブロードキャスト ドメイン内の 2 つのホスト間のトラフィックがどのセキュリティ ポリシーにも一致しません。展示を参照すると、次のことを行う必要があります。この問題を解決します？

A. グローバルモードをセキュリティ切り替えモードに変更する必要があります。
B. グローバル モードをセキュリティ ブリッジ モードに変更する必要があります。
C. グローバルモードをスイッチングモードに変更する必要があります。
D. グローバル モードをトランスペアレント ブリッジ モードに変更する必要があります。

Answer: (解答を表示する)

最新問題: **2**

展示」ボタンをクリックします。

```
user@srx> show security flow session
Session ID: 11232, Policy name: Allow-ipv6-Telnet/11, Timeout: 1788, Valid
  In: 2001:db8::1/57707 --> 2001:db8::8/23;tcp, Conn Tag: 0x0, If: vlan.101,
Pkts: 9, Bytes: 799,
  Out: 10.8.8.8/23 --> 10.7.7.5/21868;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 8, Bytes: 589,
Total sessions: 1
```

展示されている NAT のタイプはどれですか?

A. DS-Lite

B. NAT64

C. 永続的 NAT

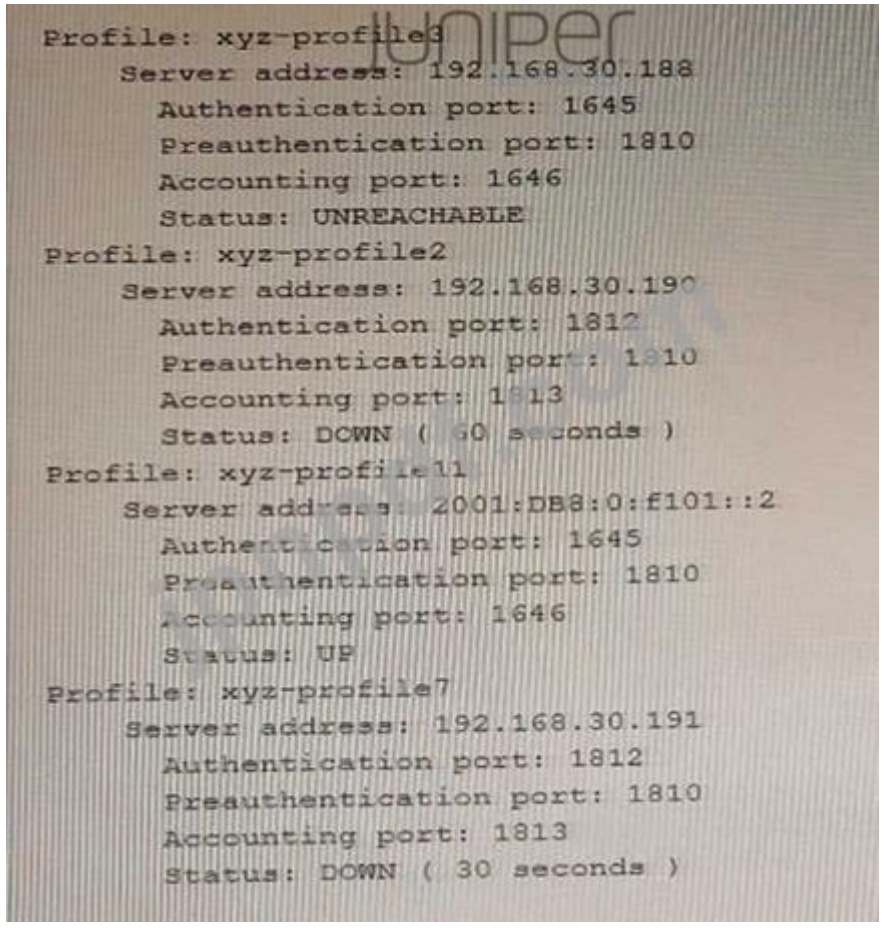
D. NAT46

Answer: (解答を表示する**)**

最新問題: **3**

show network-access aaa radius-servers コマンドは、認証の問題を解決するために発行されました。

展示品を参照すると、SRX シリーズ デバイスはどの 2 つの認証サーバーにリクエストを送信し続けるのでしょうか? (2つお選びください。)

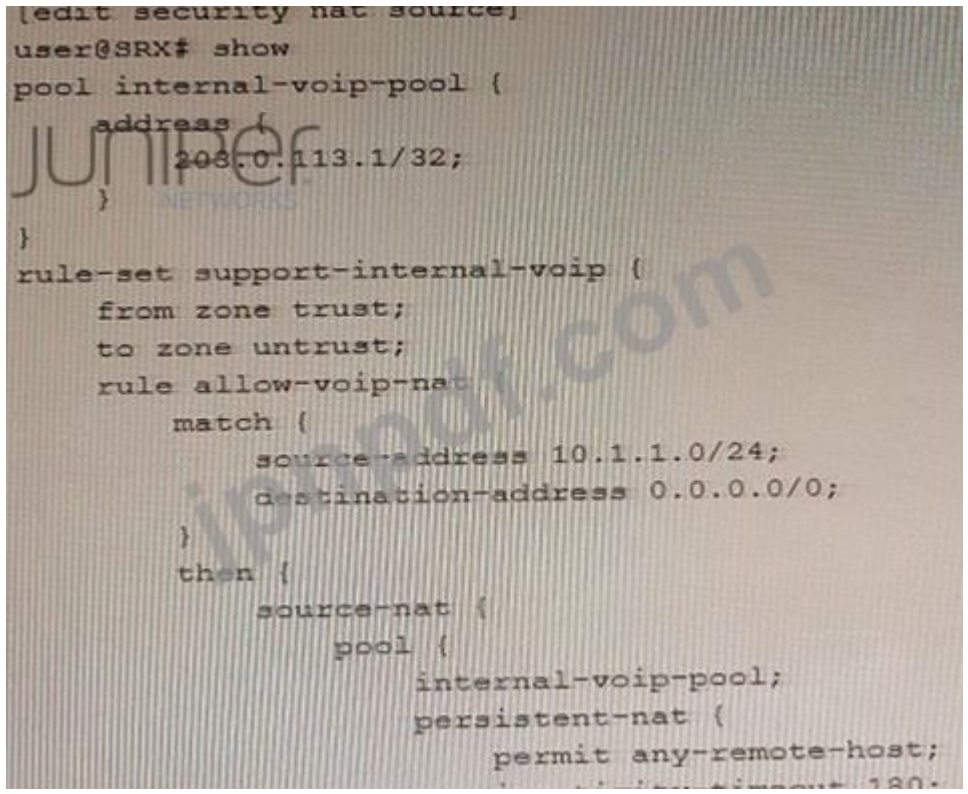


A. 192.168.30.190

B. 200l:DB8:0:f101::2

C. 192.168.30.191
D. 192.168.30.188
Answer: C,D (メーッセージを残す)

最新問題: **4**
示す



展示物を参照すると、内部ホストは、送信元ポート 54311 の再帰アドレス 203.0.113.1 を使用して、インターネット ホストにトラフィックを送信しています。
この状況で正しいのはどれですか?
A. インターネット上の任意のホストは、203.0.113.1 アドレス、ランダムな送信元ポート、および宛先ポート 54311 を使用して、内部ホストに到達するトラフィックを開始できます。
B. 内部ホストが最初に通信していたインターネット ホストのみが、203.0 113.1 アドレス、ランダムな送信元ポート、および宛先ポート 54311 を使用して内部ホストに到達するトラフィックを開始できます。
C. インターネット上の任意のホストは、アドレス 203.0.113.1、送信元ポート 54311、およびランダムな宛先ポートを使用して、内部ホストに到達するトラフィックを開始できます。
D. 内部ホストが最初に通信していたインターネット ホストのみが、203.0.113.1 アドレス、送信元ポート 54311、およびランダムな宛先ポートを使用して内部ホストに到達するトラフィックを開始できます。
Answer: (解答を表示する)

最新問題: **5**
コレクターのトラフィック フィードの 1 つが 100 kbps を下回った場合に通知を設定するように求められます。
このタスクを実行するには、どの 2 つの構成パラメータを設定する必要がありますか? (2つお選びください。)
A. JATP アプライアンスにトラフィック SNMP トラップを設定します。
B. JATP アプライアンスで一般的なトリガー通知を設定します。

C. JATP アプライアンスに交通システム アラートを設定します。
D. JATP アプライアンスでログ通知を設定します。
Answer: (解答を表示する**)**

最新問題**: 6**
Traceoptions を使用して、SRX シリーズ デバイスの NAT セッション情報を確認しています。
展示物に関して、正しいのは次のうちどれですか? (2つお選びください。)

Exhibit

```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

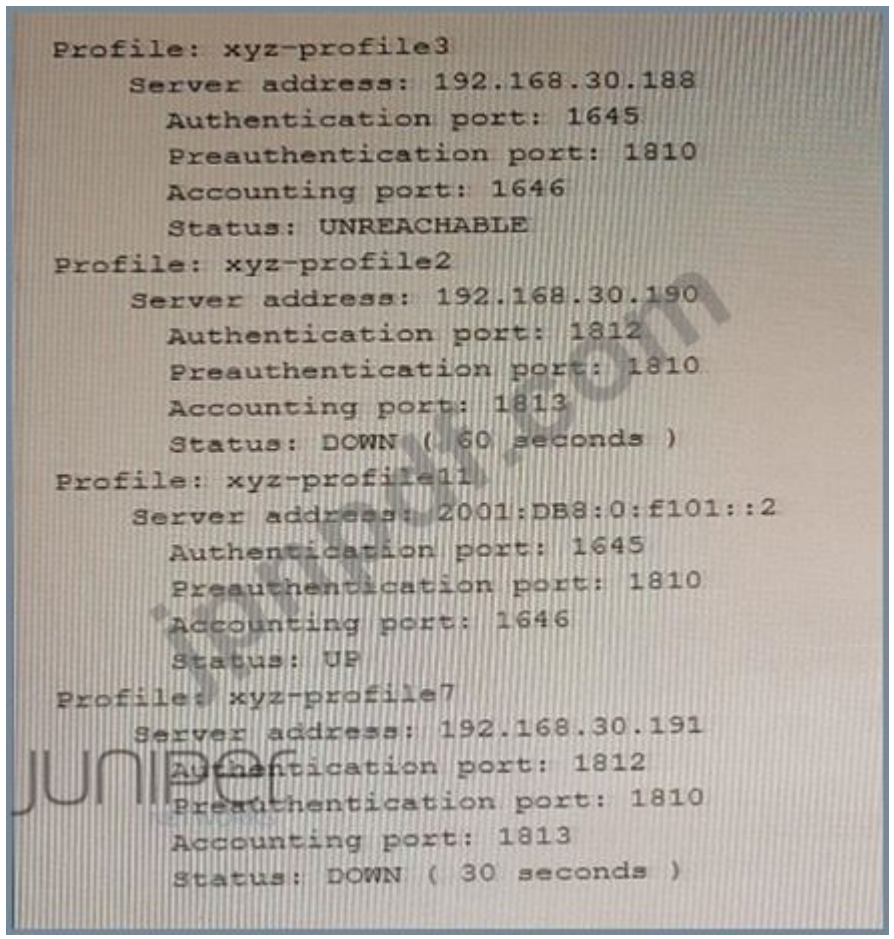
A. これはセッションの最後のパケットです。
B. SRX シリーズ デバイスは、このセッションで送信元 NAT と宛先 NAT の両方を実行しています。
C. これはセッションの最初のパケットです。
D. SRX シリーズ デバイスは、このセッションではソース NAT のみを実行しています。
Answer: A,B (メーッセージを残す)

最新問題**: 7**
宛先 NAT を使用して、HTTPS サーバーのアドレスを SRX シリーズ デバイス上のプライベート アドレスに変換しています。IDP SSL 復号化を実装することにしました。
復号化を有効にしても、セッションが復号化されていないことがわかります。
どのアクションで問題が解決しますか?
A. パブリック アドレスを使用するようにサーバーの SSL 証明書を置き換えます。
B. IDPsensor-configurationdetector を有効にしてアドレス変換を検出します。
C. SRX シリーズデバイスを再起動します。
D. SSLsession-id-cache-timeout 値を 5000 秒を超える任意の値に増やします。
Answer: (解答を表示する)

最新問題**: 8**
port-overloading-factor 1 設定を使用するのはどのような場合ですか?
A. ポートのオーバーロードを有効にします。
B. ポートのオーバーロードを無効にします。
C. ポートの過負荷のためにポートを 1:1 の比率でマッピングします。
D. 最大ポート過負荷容量を 65,536 に設定します。
Answer: B (メーッセージを残す)
https://www.juniper.net/documentation/en_US/junos/topics/reference/configuration-statement/security-edit-port-overloading-interface-source-nat.html

最新問題**: 9**
ソース NAT 実装では、複数の IPv4 アドレスを含むアドレス プールを使用します。
ユーザーは、外部アプリケーションと複数のセッションを確立すると、認証を複数回要求されると報告しています。外部ホストは内部ネットワーク ホストとのセッションを確立できません。
何がこの問題を解決するのでしょうか？
A. アドレスの永続性を有効にします。
B. 永続的 NAT を有効にする
C. PATを無効にします。
D. 宛先 NAT を有効にします。
Answer: (解答を表示する)

最新問題**: 10**
示す



show network-access aaa radius-servers コマンドは、認証の問題を解決するために発行されました。
展示品を参照すると、SRX シリーズ デバイスはどの 2 つの認証サーバーにリクエストを送信し続けるのでしょうか? (2つ選択してください)

A. 192.168.30.190
B. 192.168.30.191
C. 192.168.30.188
D. 200l:DB8:0:f101;:2
Answer: (解答を表示する**)**

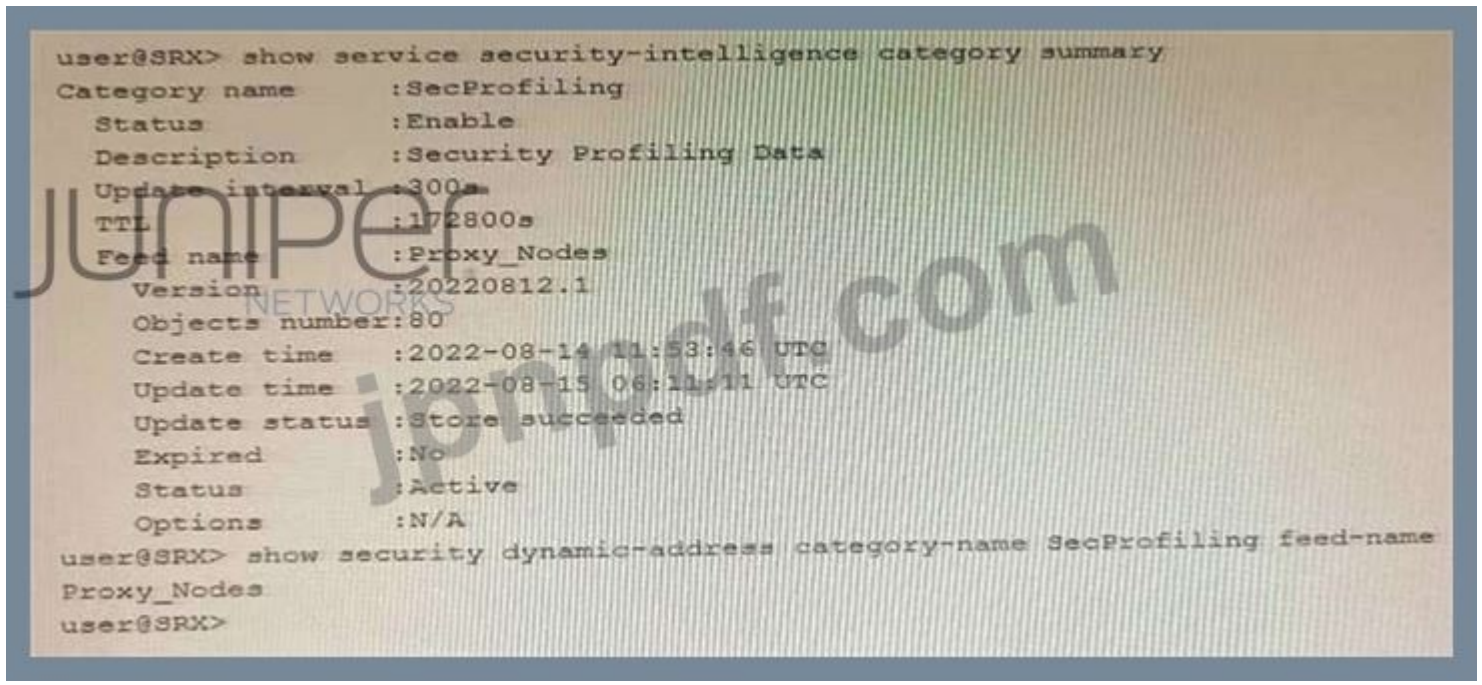
最新問題**: 11**
SRX シリーズ デバイス上でレイヤー 2 トラフィックがトランスペアレント モードで保護されていることを確認する必要があります。
このタスクを実行する際には何を考慮する必要がありますか?

A. トランスペアレント モードを構成した後、デバイスを再起動する必要があります。
B. トランスペアレント モードで動作している場合、セキュリティ ポリシーはサポートされません。
C. レイヤ 2 インターフェイスはイーサネット スイッチング プロトコル ファミリを使用する必要があります。
D. 透過モードのセキュリティ ゾーンでは画面がサポートされていません。
Answer: (解答を表示する**)**

最新問題**: 12**
SRX シリーズ デバイスを Juniper ATP Cloud に登録するように要求されます。
このシナリオではどの記述が正しいでしょうか?

A. SRX シリーズ デバイスを登録する唯一の方法は、Juniper ATP Cloud Web ポータルと対話することです。
B. ライセンスの有効期限が切れると、SRX シリーズ デバイスは猶予期間なしでジュニパー ATP クラウドから登録解除されます。
C. Juniper ATP Cloud は Junos OS op スクリプトを使用して、SRX シリーズ デバイスを Juniper ATP Cloud サービスに接続するように構成します。
D. デバイスがすでにレルムに登録されており、それを新しいレルムに登録すると、デバイス データまたは構成情報が新しいレルムに伝播されます。
Answer: (解答を表示する**)**

最新問題**: 13**
最近、適応型脅威プロファイリングを構成しましたが、図に示すように、ジュニパー ATP クラウド ポータルの監視セクションに 20 個の IP アドレス エントリがローカルの SRX シリーズ デバイス上のエントリ数と一致しないことに気づきました。
SRX デバイスでこの問題を解決するための正しいアクション は何ですか?



A. ATP クラウドのフィードを更新します。
B. Proxy__Nodes フィードの手動ダウンロードを強制します。
C. SRX デバイスのセキュリティ ポリシーで DAE を構成する必要があります。
D. SRX デバイスの DNS キャッシュをフラッシュします。
Answer: D (メーッセージを残す**)**

最新問題**: 14**
展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)

A. ge-070/0 インターフェイスを通過するデータは、誰でも傍受して読み取ることができます。
B. ge-O/0/0 インターフェイスを通過するデータは、接続関連付けキーによって保護されます。
C. ge-070/0 インターフェイスを通過するデータは、誰にも傍受されたり読み取られたりすることはできません。
D. ge-0/070 インターフェイスを通過するデータは、安全な関連付けキーによって保護されます。
Answer: (解答を表示する**)**

最新問題: **15**
示す

展示に示されている出力に関して正しい 2 つの記述はどれですか。(2つお選びください。)

A. 宛先アドレスが変換されます。

B. パケットはユーザー設定のポリシーに一致します。

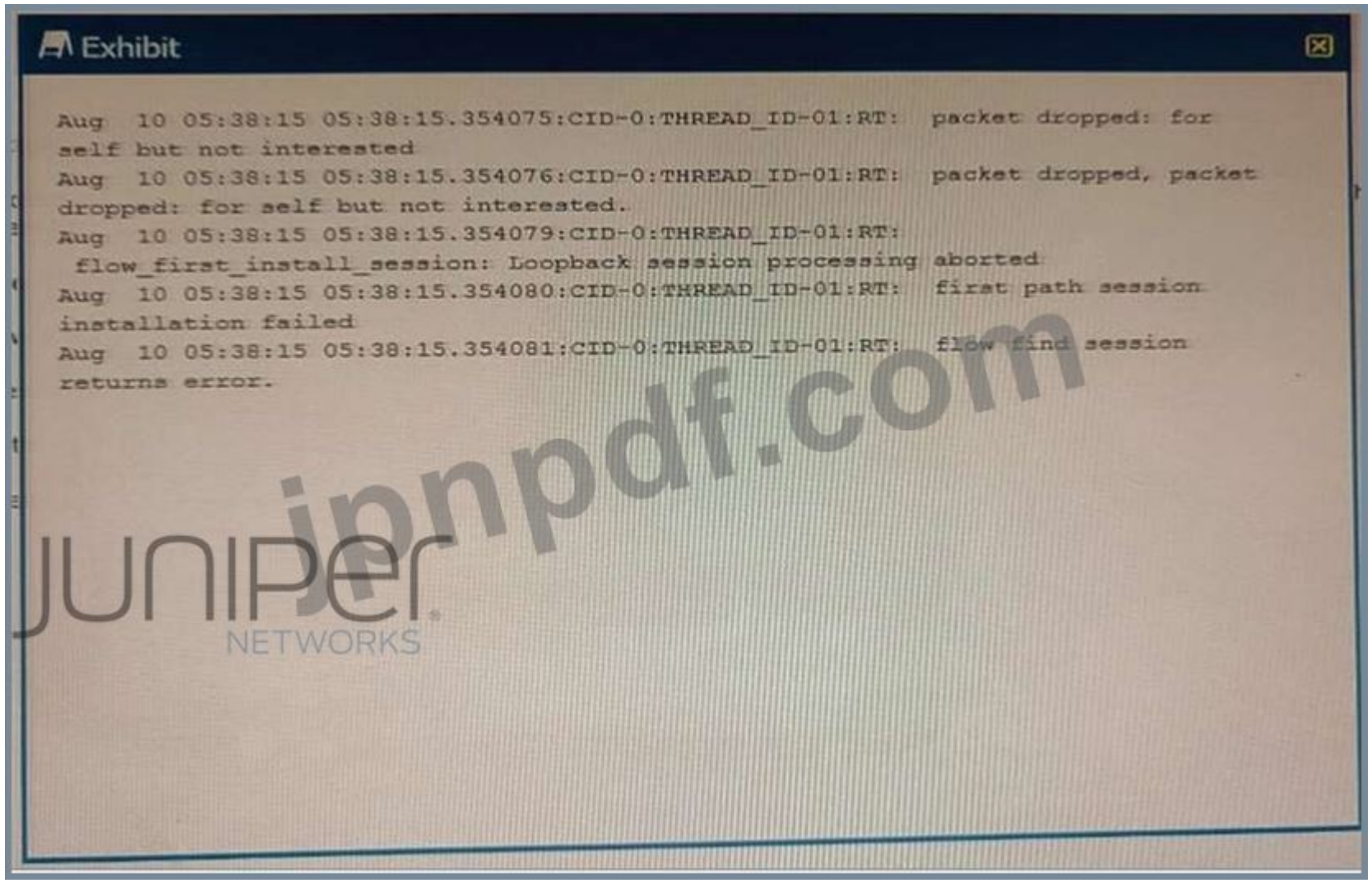
C. パケットは SSH パケットです

D. 送信元アドレスが変換されます。

Answer: C,D (メーッセージを残す**)**

最新問題**: 16**

示す



SRX シリーズ デバイスとルーターの間に IBGP ピアリングを確立するように求められますが、セッションは確立されていません。SRX デバイスのセキュリティ フロー トレースでは、図に示すようにパケット ドロップが観察されます。
SRX デバイスの問題を解決するための正しいアクションは何ですか?

A. BGP トラフィックを許可するようにセキュリティ ポリシーを変更します。
B. インターフェイスの許可されたホスト受信トラフィックに BGP を追加します。
C. BGP トラフィックを受け入れるファイアウォール フィルターを作成します。
D. BGP トラフィックの宛先 NAT を構成します。
Answer: C (メーッセージを残す)

最新問題: 17

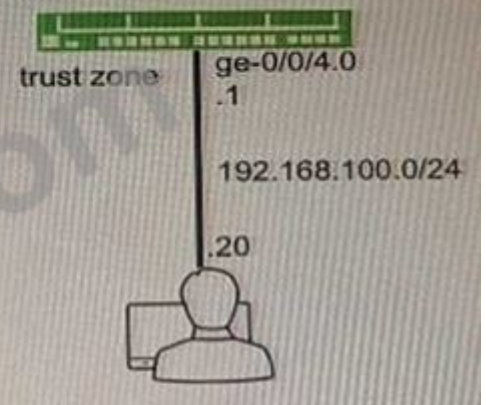
展示されているサードパーティ フィードが適切に動作するために必要な追加の構成アクションを 2 つ選択してください。(2つお選びください。)
A. セキュリティ ポリシーで動的アドレス エントリを適用する必要があります。
B. IP フィルター カテゴリと ipfilter_office365 値を使用して動的アドレス エントリを作成する必要があります。
C. C&C カテゴリと cc_offic365 値を使用して動的アドレス エントリを作成する必要があります。
D. セキュリティ インテリジェンス ポリシーで動的アドレス エントリを適用する必要があります。
Answer: (解答を表示する**)**

最新問題**: 18**
Juniper ATP Appliance コレクター上に SSH ハニーポットをセットアップしようとしています。コレクターは、2 つの物理インターフェイスと 2 つの物理 CPU コアを備えたハードウェア上で実行されます。ハニーポット機能が動作していません。
このシナリオではどの記述が真実ですか?
A. コレクターには少なくとも 4 つの物理インターフェイスが必要です
B. コレクターには少なくとも 6 つの物理コアが必要です
C. コレクターには少なくとも 4 つの物理コアが必要です
D. コレクターには少なくとも 3 つの物理インターフェイスが必要です
Answer: D (メーッセージを残す**)**

最新問題**: 19**
SRX シリーズ ファイアウォール上にあるネットワークのデフォルト ゲートウェイ 192.168.100.1 に ping を実行できません。
展示を参照して、SRX シリーズ デバイスの構成を修正する 2 つのコマンドはどれですか? (2つお選びください。)

```
[edit]
user@SRX# show interfaces ge-0/0/4
unit 0 {
    family inet {
        address 192.168.100.1/32;
    }
}

[edit security zones]
user@SRX# show security-zone trust
host-inbound-traffic {
    system-services {
        netconf;
    }
}
interfaces {
    ge-0/0/4.0 {
        host-inbound-traffic {
            system-services {
                ssh;
            }
        }
    }
}
```



A.
```
[edit security zones security-zone trust]
user@SRX# set interfaces ge-0/0/4.0 host-inbound-traffic system-services ping
```
B.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping
```
C.
```
[edit security zones security-zone trust]
user@SRX# set host-inbound-traffic system-services ping except
```
D.
```
[edit interfaces ge-0/0/4]
user@SRX# replace pattern 32 with 24
```
Answer: (解答を表示する)

最新問題: **20**
最近買収した会社のネットワークと企業ネットワークを結合するように求められます。
どちらのネットワークも同じプライベート IPv4 アドレス空間 (172.25.126.0/24) を使用します。SRX シリーズ デバイスは、各ネットワークのゲートウェイとして機能します。
現在のアドレス割り当てを変更せずに 2 つのネットワークを結合できるソリューションはどれですか?
A. 永続的 NAT
B. NAT46
C. ソース NAT
D. ダブルNAT
Answer: D (メーッセージを残す)
https://kb.juniper.net/InfoCenter/index?page=content&id=KB21286

最新問題: **21**
示す

```
[edit security policies from-zone trust to-zone untrust policy Adaptive-Threat-
Profiling]
user@SRX-1# show
match {
    source-address any;
    destination-address any;
    application any;
    dynamic-application [ junos:web:proxy junos:web:anonymizer junos:TOR ];
}
then {
    reject {
        application-services {
            security-intelligence {
                add-default-action-ip-to-feed {
                    Proxy_Nodes;
...
```

展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)
A. Proxy_Nodes フィードを、別の SRX シリーズ デバイス上の別のセキュリティ ポリシーの送信元アドレスと宛先アドレスの一致基準として使用できます。

B. SRX-1 デバイスは Proxy_wodes フィードを作成するため、それを別のセキュリティ ポリシーで使用できません。
C. Proxy_Node3 フィードは、別の SRX シリーズ デバイス上の別のセキュリティ ポリシーの宛先アドレス一致基準としてのみ使用できます。
D. SRX-1 デバイスは、別のセキュリティ ポリシーで Proxy__Nodes フィードを使用できます。
Answer: (解答を表示する**)**

最新問題**: 22**
セキュリティ ポリシーのトラブルシューティング中に、カウント アクションを追加しました。
このアクションの結果はどこで確認できますか?
A. show securitypolicyhit-count コマンドの出力。
B. show securitypolicydetail コマンドの出力。
C. showsecurityflowstatisticsコマンドの出力。
D. show firewall log コマンドの出力。
Answer: D (メーッセージを残す**)**

最新問題**: 23**
示す

```
[edit]
user@branch1# show interfaces
ge-0/0/2 {
    unit 0 {
        family inet {
            dhcp;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.0.0.2/30;
        }
    }
}
[edit security zones]
user@branch1# show security-zone untrust
interfaces {
    ge-0/0/2.0 {
        host-inbound-traffic {
            system-services {
                ike;
                dhcp;
            }
        }
    }
}
gateway gateway-1 {
    ike-policy ike-policy-1;
    address 203.0.113.5;
    local-identity hostname "branch1@srx.juniper.net";
    external-interface ge-0/0/2;
}
[edit security ike]
user@corporate# show
policy ike-policy-branch1 {
    mode main;
    proposal-set standard;
    pre-shared-key ascii-text "$9$6st6CpOhSeX7V1R7VwYZG1AB"; ## SECRET-DATA
}
gateway gateway-branch1 {
    ike-policy ike-policy-branch1;
    dynamic hostname "branch1@srx.juniper.net";
    external-interface ge-0/0/1;
```


JUNIPER NETWORKS

本社と支店 1 の SRX シリーズ デバイス間に IPsec トンネルを構成しようとしています。展示に示されている構成をコミットしましたが、IPsec トンネルが確立されていません。
このシナリオでは、何がこの問題を解決しますか。
A. Branch1 デバイス上のローカル ID を inet advpn に変更します。
B. Branch1 デバイスの st0.0 インターフェイス設定にマルチポイントを追加します。
C. Branch1 および企業デバイスの IKE モードをアグレッシブに変更します。
D. IKE プロポーザル セットを、branch1 と企業デバイスで互換性のあるものに変更します。
Answer: (解答を表示する**)**

最新問題**: 24**
DMZ 内の Web サーバーに対して静的 NAT を構成しました。内部ユーザーと外部ユーザーの両方が、Web サーバーの IP アドレスを使用して Web サーバーにアクセスできます。ただし、Web サーバーの DNS 名を使用して Web サーバーにアクセスできるのは内部ユーザーのみです。外部ユーザーが Web サーバーの DNS 名を使用して Web サーバーにアクセスしようとすると、エラー メッセージが受信されます。
どのアクションがこの問題を解決するでしょうか?
A. Webフィルタリングを無効にする
B. DNS ドクタリングを使用する
C. セキュリティポリシーを変更する
D. 静的 NAT の代わりに宛先 NAT を使用します。
Answer: (解答を表示する**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-dns-algs.html

最新問題**: 25**
Web サーバーと DNS サーバーが同じ内部 DMZ サブネット内に存在しています。サーバーのパブリック静的 NAT アドレスは、SRX シリーズ デバイスのインターネット接続インターフェイスと同じサブネット内にあります。DNS ドクタリングを実装して、リモート ユーザーが Web サーバーにアクセスできるようにします。このシナリオで正しいのは次の 2 つのステートメントのうちどれですか? (2つお選びください。)
A. DNS CNAME レコードが変換されます。
B. DNS ドクタリング ALG はデフォルトで有効になっています。
C. DNS ドクタリング ALG はデフォルトでは有効になっていません。
D. プロキシ ARP 機能を設定する必要があります。
Answer: B,D (メーッセージを残す**)**

最新問題**: 26**
展示を見ると、ADVPN のスポーク メンバーが正しく機能していません。
この問題を解決する 2 つのコマンドはどれですか? (2つお選びください。)

```
[edit security ike gateway advpn-gateway]
user@srx# show
ike-policy advpn-policy;
address 192.168.3.1;
local-identity distinguished-name;
remote-identity distinguished-name container O=Juniper;
external-interface ge-0/0/3.0;
version v2-only;
[edit interfaces]
user@srx# show st0
unit 0 {
    family inet {
        address 10.100.100.1/24;
    }
}
```

A.
```
[edit security ike gateway advpn-gateway]
user@srx# set advpn partner disable
```

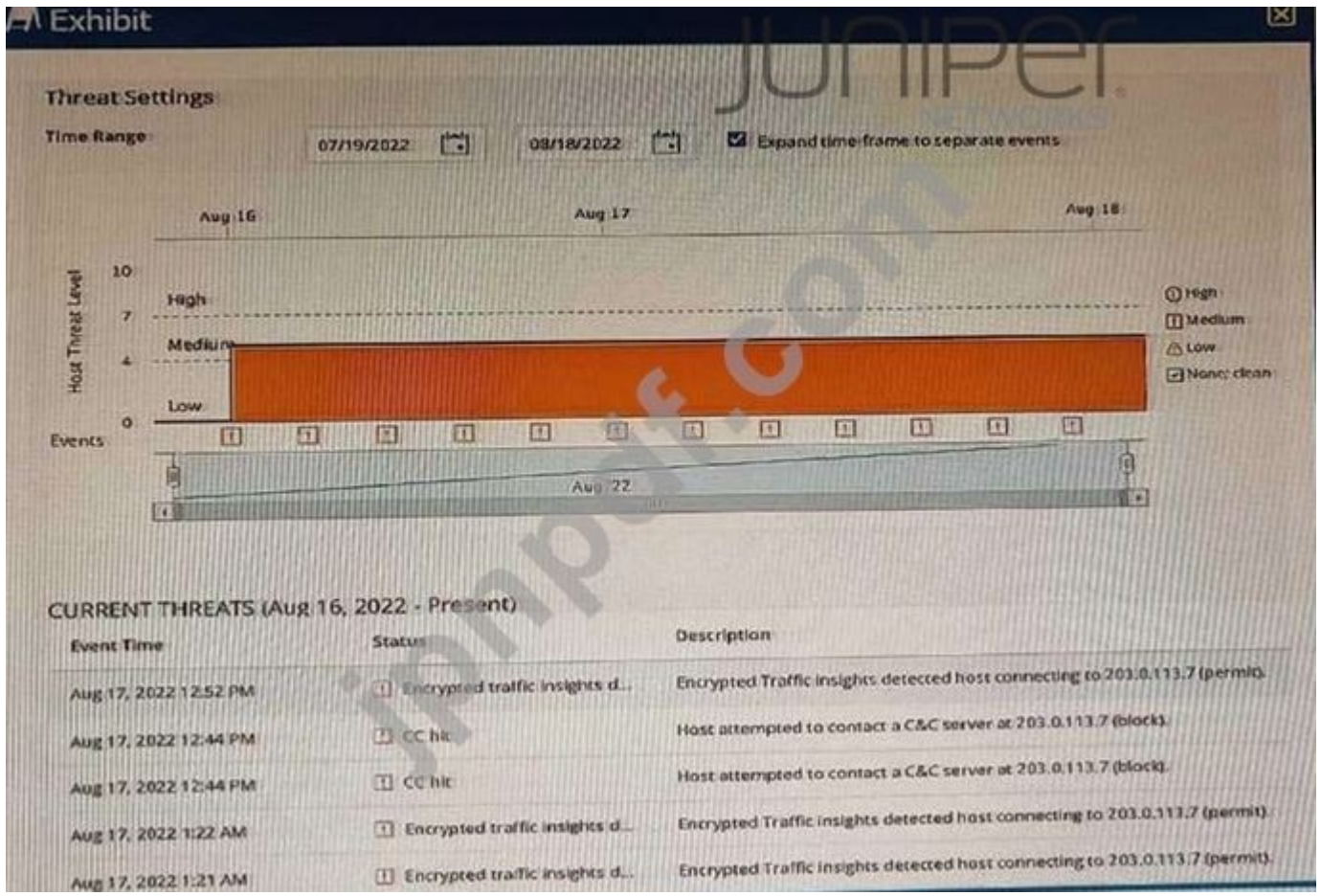
B.
```
[edit security ike gateway advpn-gateway]
user@srx# set advpn suggester disable
```

C.
```
[edit interfaces]
user@srx# set st0.0 multipoint
```

D.
```
[edit security ike gateway advpn-gateway]
user@srx# set local-identity inet advpn
```

Answer: D (メーッセージを残す)

最新問題: **27**
ATP クラウドを使用していて、同じ調査から得られた多数の ETI および C&C ヒットを持つホストがあることに気付き、一部のイベントが自動的に緩和されていないことに気付きます。
展示物を参照して、この動作の理由は何ですか?



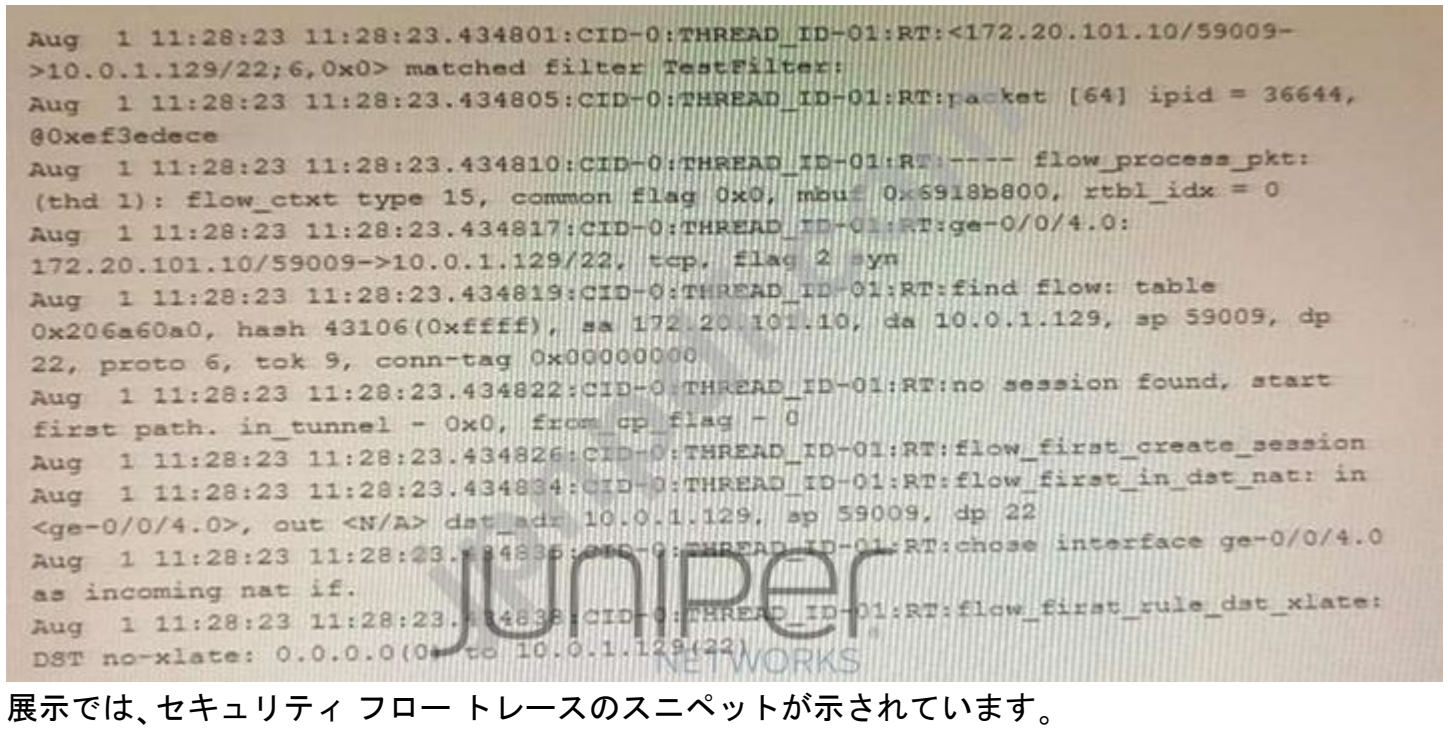
A. 感染ホストのスコアは、脅威レベル 5 未満にグローバルに設定されています。
B. 感染ホストのスコアは、脅威レベル 5 を超えてグローバルに設定されています。
C. C&C イベントは誤検知です。
D. ETI イベントは誤検知です。
Answer: D (メーッセージを残す)

最新問題**: 28**
ネットワーク内のセキュリティ デバイスを備えた仮想化ソリューションを展開している。各 SRX シリーズ デバイスは少なくとも 100 の仮想化インスタンスをサポートする必要があり、各仮想化インスタンスには独自の個別の管理ドメインが必要です。
このシナリオでは、どのソリューションを選択しますか?
A. テナントシステム
B. 仮想ルーターインスタンス
C. 論理システム
D. VRF インスタンス
Answer: C (メーッセージを残す)

最新問題**: 29**
IP アドレス 203.0.113.5 が、Juniper SecInte1 からサードパーティのセキュリティ フィード DS hield に追加されているかどうかを確認するよう求められます。
Juniper ATP Cloud からの SecInte1 フィードを使用する SRX シリーズ デバイスがあります。
どのコマンドがこの情報を返しますか?

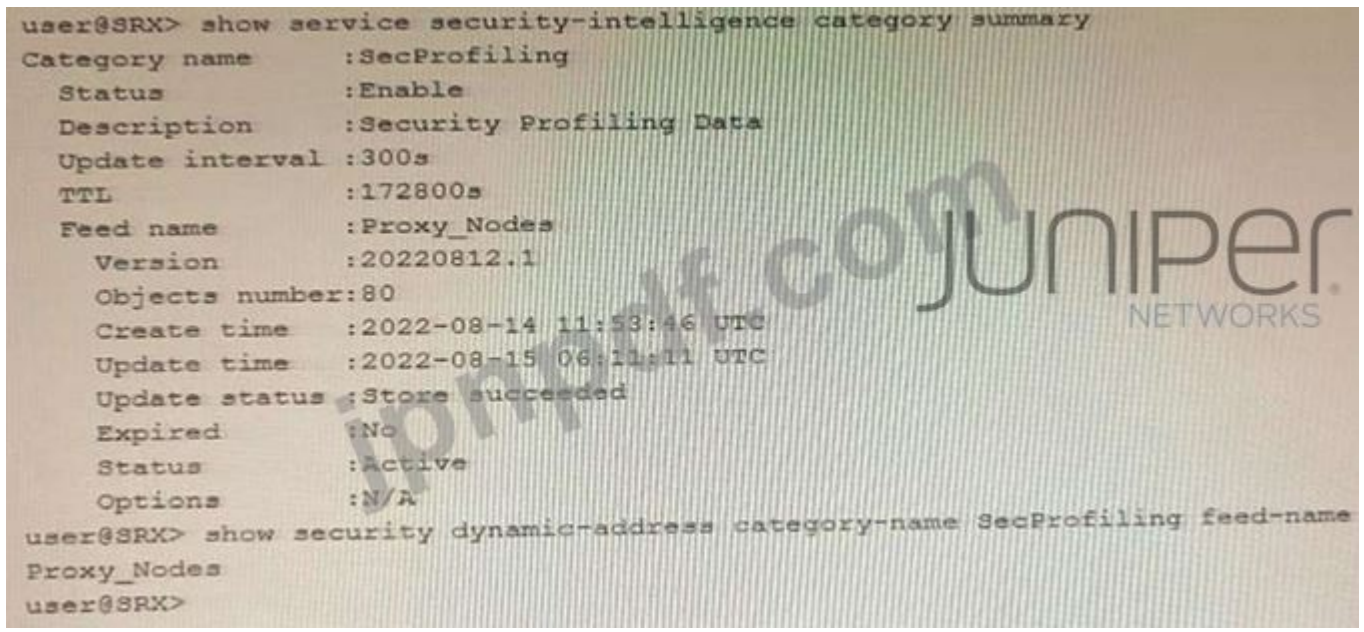
A. セキュリティ ダイナミック アドレス カテゴリ名 IP フィルタを表示します。203.0.113.5 に一致します。
B. 動的セキュリティを表示 -- アドレス カテゴリ -- 名前 感染 -- ホスト | 203.0.113.5 に一致
C. セキュリティを動的に表示 -- アドレス カテゴリ -- 名前 CC | 203.0.113.5 に一致
D. セキュリティ動的アドレス カテゴリ名 JWAS | を表示します。203.0.113.5 に一致
Answer: D (メーッセージを残す**)**

最新問題**: 30**
示す



展示では、セキュリティ フロー トレースのスニペットが示されています。
このシナリオでは、どの 2 つの記述が正しいでしょうか? (2つお選びください。)
A. 宛先NATが発生します。
B. このパケットはインターフェイス ge-0/0/4.0 に到着しました。
C. テーブル内に既存のセッションが見つかりました。
D. キャプチャは、送信元アドレス 172.20.101.10 から 10.0.1.129 宛てのパケットです。
Answer: C,D (メーッセージを残す**)**

最新問題**: 31**
示す



最近、適応型脅威プロファイリングを構成しましたが、図に示すように、ジュニパー ATP クラウド ポータルの監視セクションに 20 個の IP アドレス エントリがローカルの SRX シリーズ デバイス上のエントリ数と一致しないことに気づきました。
SRX デバイスでこの問題を解決するための正しいアクションは何ですか?

A. SRX デバイスの DNS キャッシュをフラッシュします。
B. SRX デバイスのセキュリティ ポリシーで DAE を構成する必要があります。
C. Proxy__Nodes フィードの手動ダウンロードを強制します。
D. ATP クラウドのフィードを更新します。
Answer: A (メーッセージを残す)

最新問題: **32**
通過トラフィックをキャプチャできる構成可能な SRX シリーズ デバイス機能はどれですか?

A. アーカイブ
B. パケットキャプチャ
C. syslog
D. トレースオプション
Answer: D (メーッセージを残す)

最新問題: **33**
展示」ボタンをクリックします。

```
user@host# show security idp-policy my-policy rulebase-ips
rule 1 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  no-action;
            }
      }
}
rule 2 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  ignore-connection;
            }
      }
}
rule 3 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  drop-packet;
            }
      }
}
rule 4 {
      match {
            attacks {
                  custom-attacks my-signature;
            }
      }
      then {
            action {
                  close-client-and-server;
            }
      }
}
```

最近、展示に示されている IPS ポリシーをコミットしました。予想される動作を評価すると、IPS ポリシー内のすべてのルールに一致するセッションがあることがわかります。
このシナリオでは、どのようなアクションが取られるでしょうか?
A. パケットをドロップします
B. アクションなし
C. クライアントとサーバーを閉じる
D. 接続を無視する
Answer: (解答を表示する**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-idp-policy-rules- and-rulebases.html

最新問題**: 34**
このシナリオでは、どの 2 種類のソース NAT 変換がサポートされますか? (2つお選びください。)
A. ポート アドレス変換を使用した 1 つの IPv4 サブネットから 1 つの IPv6 サブネットへの変換
B. ポート アドレス変換の有無にかかわらず、IPv4 ホストから IPv6 ホストへの変換
C. ポート アドレス変換を行わない、ある IPv6 サブネットから別の IPv6 サブネットへの変換
D. ポート アドレス変換を使用した、ある IPv6 サブネットから別の IPv6 サブネットへの変換
Answer: B,D (メーッセージを残す**)**

最新問題**: 35**
Juniper ATP Cloud ではどの 2 つのモードがサポートされていますか? (2つお選びください。)
A. レイヤー3モード
B. 透過モード
C. プライベートモード
D. グローバルモード
Answer: A,B (メーッセージを残す**)**

最新問題**: 36**
SSL プロキシによるセッション内容の復号化を必要とせずに、SSL 暗号化セッション内の潜在的な脅威を特定したいと考えています。この目的を達成できるセキュリティ機能はどれですか?
A. DNSセキュリティ
B. 感染したホストのフィード
C. セキュアな Web プロキシ
D. 暗号化されたトラフィックの分析情報
Answer: A (メーッセージを残す**)**

最新問題**: 37**
フィルタベースの転送を実装して、172.25.0.0/24 ネットワークからのトラフィックを ISP-1 経由で送信しながら、他のすべてのトラフィックを接続経由で ISP-2 に送信します。
ge-0/0/1 インターフェイスは、172.25.0.0/24 ネットワークを含む 2 つのネットワークに接続します。

展示に示されている構成が実装されました。172.25.0.0/24 ネットワークからのトラフィックは予想どおり 172.20.0.2 に転送されますが、他のネットワーク (172.25.1.0/24) からのトラフィックは上流の 172.21.0.2 ネイバーに転送されません。
このシナリオでは、どのアクションがこの問題を解決しますか?

```
[edit]
user@srx# show interfaces ge-0/0/1
unit 0 {
    family inet {
        filter {
            input my-filter;
        }
        address 172.25.0.1/24;
        address 172.25.1.1/24;
    }
}
[edit]
user@srx# show routing-instances
ISP-1 {
    instance-type forwarding;
    routing-options {
        static {
            route 0.0.0.0/0 next-hop 172.20.0.2;
        }
    }
}
[edit]
user@srx# show routing-options
static {
    route 0.0.0.0/0 next-hop 172.21.0.2;
}
interface-routes {
    rib-group inet my-rib-group;
}
rib-groups {
    my-rib-group {
        import-rib [ inet.0 ISP-1.inet.0 ];
    }
```

A. ISP-1 ルーティング インスタンス階層の下にネイバー 172.21.0.2 へのスタティック デフォルト ルートを作成する必要があります。
B. 172.25.1.0/24 ネットワークからのトラフィックを受け入れるには、ファイアウォール フィルターに別の用語を追加する必要があります。
C. 172.25.1.1/24 IP アドレスが ge-0/0/1 インターフェイスのプライマリ アドレスであることを指定する必要があります。
D. フィルタベースの転送を使用する場合は、lo0 インターフェイスにファイアウォール フィルタを適用する必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 38**
送信元アドレスに基づいて選択的なステートレス パケットベースの転送を使用したいと考えています。このシナリオでは、トラフィックが SRX シリーズ デバイス フロー デーモンをバイパスできるようにするコマンドはどれですか?

A. ファイアウォール ファミリ inet フィルター bypass_flowd term t1 を設定し、次にルーティング インスタンス ステートレスを設定します。
B. ファイアウォール ファミリの inet フィルターを paa3_flowd term t1 で設定し、スキップ -- サービスが受け入れる
C. ファイアウォール ファミリの inet フィルターを bypas3_flowd term t1 に設定し、次に仮想チャネル ステートレスを設定します。
D. ファイアウォール ファミリ inet フィルター bypass__f lowd term t1 を設定し、packet--mode
Answer: B (メーッセージを残す)

最新問題**: 39**
Juniper ATP アプライアンスのサポート チケットを JTAC にオープンしました。JTAC は、リバース SSH 接続を使用してデバイスへのアクセスをセットアップするように要求します。この要求を満たすために構成する必要がある 3 つの設定はどれですか? （3つお選びください。）
A. JTAC リモート アクセスを有効にする
B. 一時的な root アカウントを作成します。
C. JATP サポート アカウントを有効にします。
D. 一時的な管理者アカウントを作成します。
E. リモートサポートを有効にします。
Answer: C,D,E (メーッセージを残す)
https://kb.juniper.net/InfoCenter/index?page=content&id=TN326&cat=&actp=LIST&showDraft=false

最新問題**: 40**
IPsec で使用される安全なキー管理プロトコルとは何ですか?
A. TCP
B. 超能力
C. ああ
D. イケ
Answer: D (メーッセージを残す)

最新問題**: 41**
CoS ベースの IPsec VPN でサポートされているピア デバイスの 3 つのタイプはどれですか? （3つお選びください。）
A. SRX シリーズデバイスの分岐
B. サードパーティ製デバイス
C. cSRX
D. ハイエンド SRX シリーズ デバイス
E. vSRX
Answer: (解答を表示する)
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-based-ipsec-vpns.html

最新問題**: 42**
エンジニアリング部門からの IP トラフィックのすべてのセキュリティ機能をバイパスするように SRX シリーズ デバイスを構成するように求められます。
このタスクを実行できるファイアウォール フィルターはどれですか?

A.

```
user@srx# show firewall filter eng-filter
term 1 {
      from {
            source-prefix-list {
                  eng-subnet;
            }
      }
      then packet-mode;
}
term 2 {
      then accept;
}
```

B.

```
user@srx# show firewall filter eng-filter
term 1 {
      from {
            source-prefix-list {
                  eng-subnet;
            }
      }
      then accept;
}
term 2 {
      then accept;
}
```

C.

```
user@srx# show firewall filter eng-filter
term 1 {
      from {
            source-prefix-list {
                  eng-subnet;
            }
            destination-prefix-list {
                  hr-subnet;
            }
      }
      then accept;
}
term 2 {
      then packet-mode;
}
```

D.

```
user@srx# show firewall filter eng-filter
term 1 {
      from {
            source-prefix-list {
                  hr-subnet;
            }
            destination-prefix-list {
                  eng-subnet;
            }
      }
      then packet-mode;
}
term 2 {
      then accept;
}
```

Answer: (解答を表示する)

最新問題: **43**

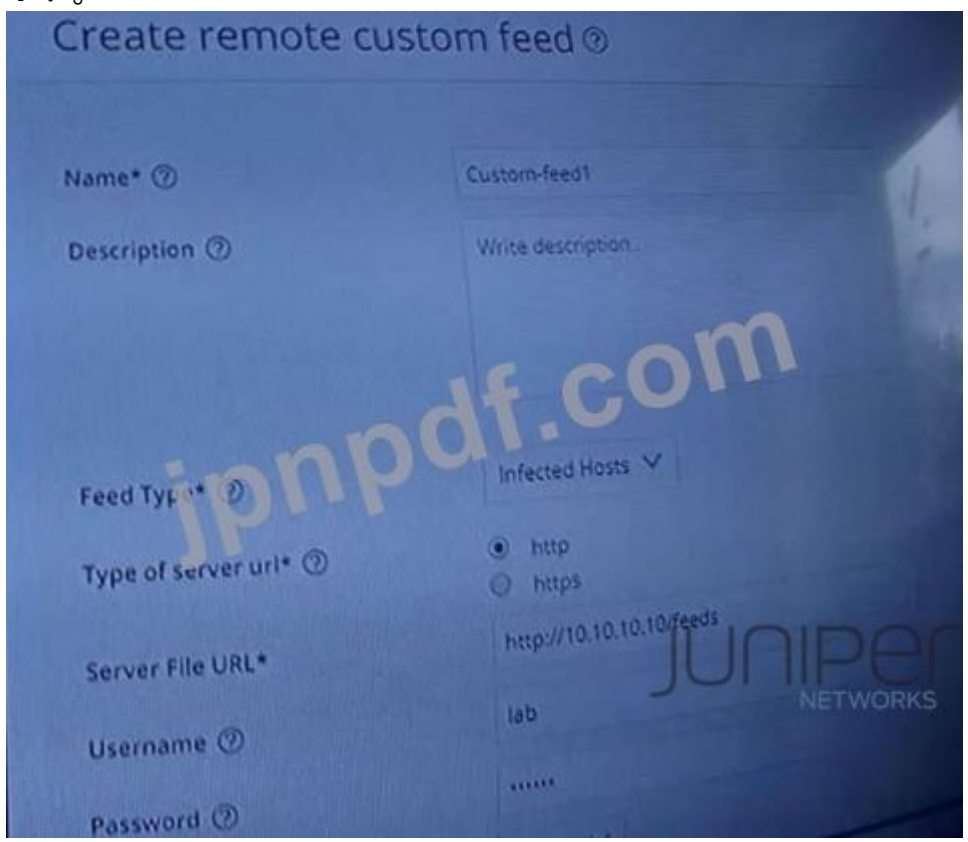
ソース NAT 実装では、複数の IPv4 アドレスを含むアドレス プールが使用されています。外部アプリケーションと複数のセッションを確立すると、認証を複数回要求されるとユーザーが報告しています。外部ホストは、内部ネットワーク ホストとのセッションを確立できてはなりません。この問題は解決しますか？

A. 永続的 NAT を有効にする

B. 宛先 NAT を有効にします。

C. PAT を無効にします。
D. アドレスの永続性を有効にします。
Answer: A (メーッセージを残す**)**

最新問題**: 44**
示す。

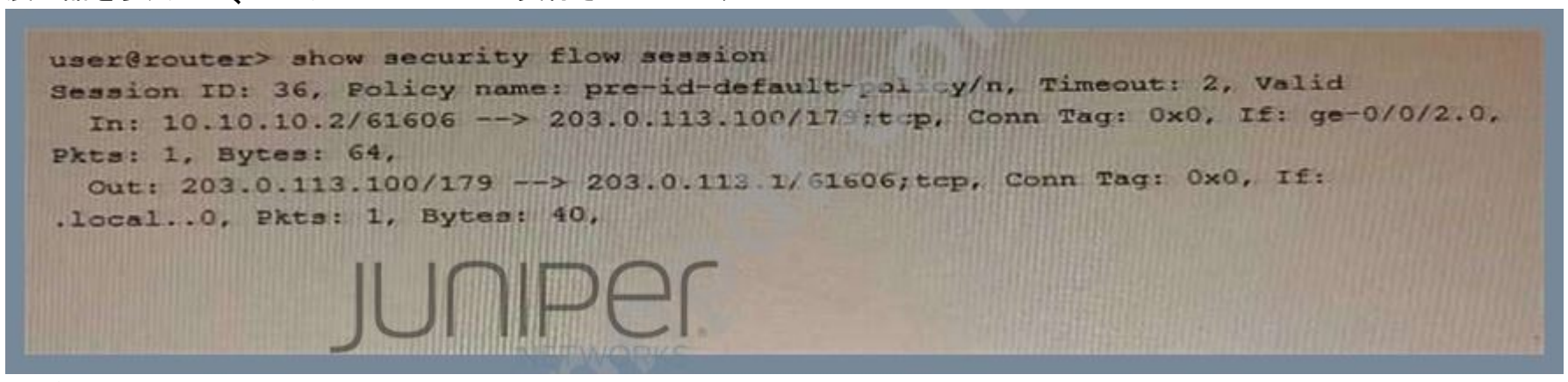


展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)
A. ジュニパーネットワークスは、このカスタム フィードによって生成された誤検知を調査しません。
B. カスタムの感染ホスト フィードは、Sky ATP 感染ホストのフィードを上書きしません。
C. カスタムの感染ホスト フィードは、Sky ATP 感染ホストのフィードを上書きします。
D. ジュニパーネットワークスは、このカスタム フィードによって生成された誤検知を調査します。
Answer: (解答を表示する**)**
https://www.juniper.net/documentation/en_US/junos-space18.1/policy-enforcer/topics/task/configuration/junos-space-policyenforcer-custom-feeds-infected-host-configure.html

最新問題**: 45**
トランスペアレント モードに関係するすべてのインターフェイスは、どのプロトコル ファミリで構成されていますか?
A. mpls
B. イーサネット - スイッチング
C. ブリッジ
D. inet
Answer: A (メーッセージを残す**)**

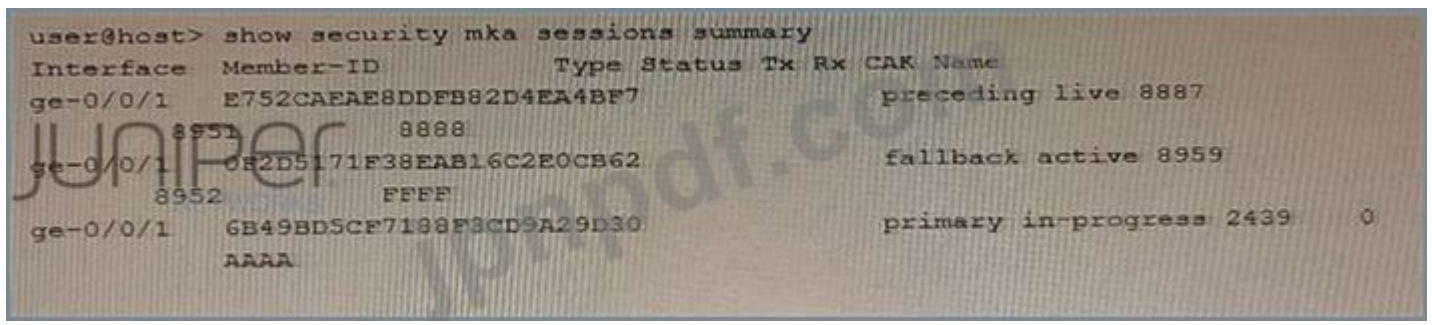
最新問題: **46**
Monitor Traffic Interface コマンドは、SRX シリーズ デバイスに送受信されるパケットをキャプチャするために使用されます。
このシナリオでは、機能に関連する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
A. この機能は通過トラフィックをキャプチャしません。
B. この機能は、SRX シリーズ デバイスとの間の ICMP トラフィックをキャプチャします。
C. この機能はハイエンド SRX シリーズ デバイスでのみサポートされています。
D. この機能は、ブランチ デバイスとハイエンド SRX シリーズ デバイスの両方でサポートされています。
Answer: (解答を表示する**)**
https://forums.juniper.net/t5/Ethernet-Switching/monitor-traffic-interface/td-p/462528

最新問題: **47**
展示品を参照して、どのタイプの NAT が実行されていますか?



A. 静的 NAT
B. 宛先NAT
C. ソース NAT
D. 永続的 NAT
Answer: (解答を表示する**)**

最新問題: **48**
示す



展示物を参照して、FFFP」という名前の CAK の CAK ステータスについて正しい 2 つの記述はどれですか?
(2つお選びください。)

A. MACsec セッションの暗号化および復号化には CAK は使用されません。

B. このキーを使用して SAK が正常に生成されました。

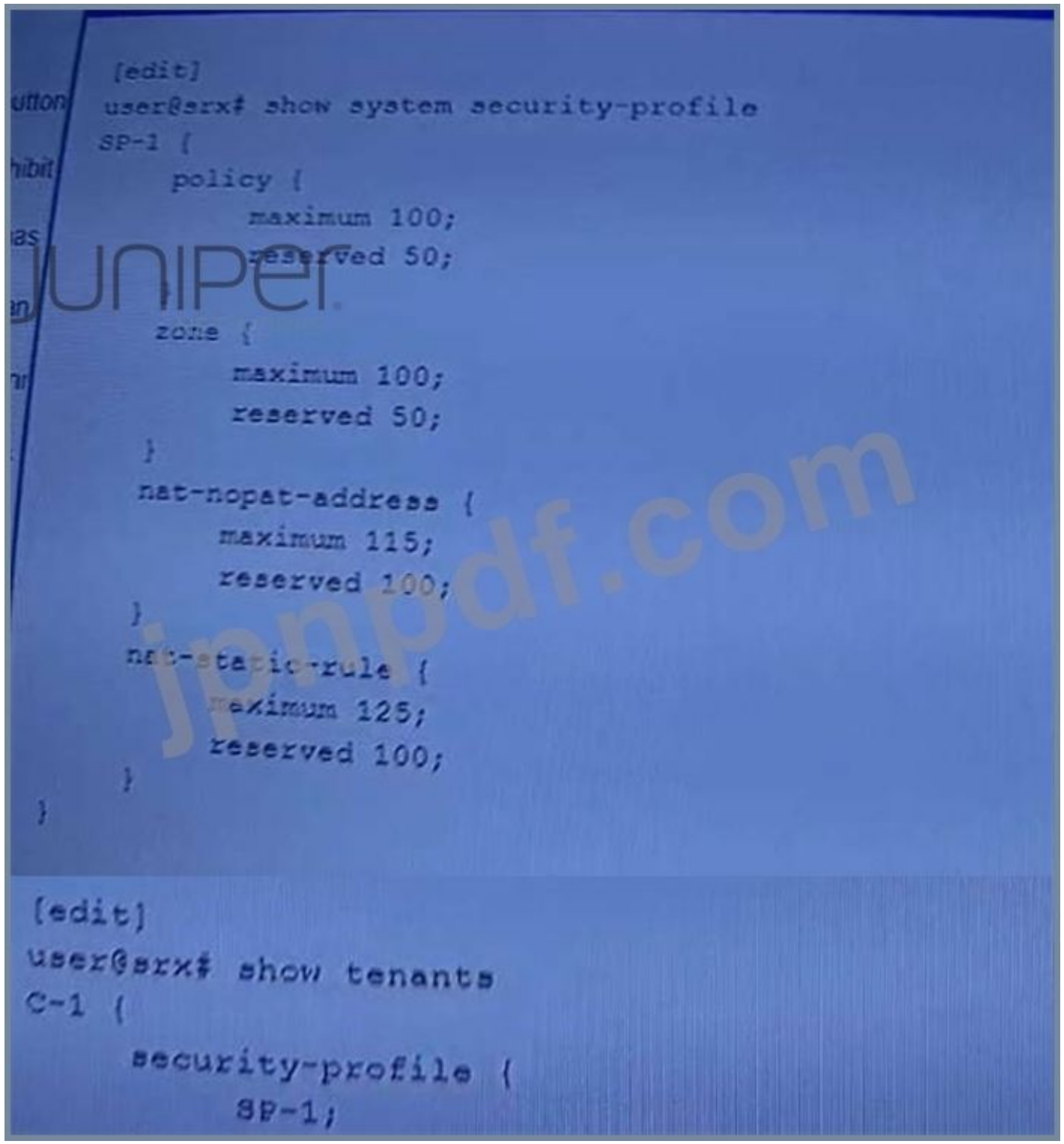
C. このキーを使用して SAK は生成されません。

D. CAK は MACsec セッションの暗号化と復号化に使用されます。

Answer: (解答を表示する**)**

最新問題: **49**

示す。



展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)

A. c-1 TSYS にはセキュリティ フロー リソースが予約されています。

B. c-1 TSYS は、システムの最大値までセキュリティ フロー リソースを使用できます。

C. c-1 TSYS はセキュリティ フロー リソースを使用できません。

D. c-1 TSYS にはセキュリティ フロー リソースの予約がありません。

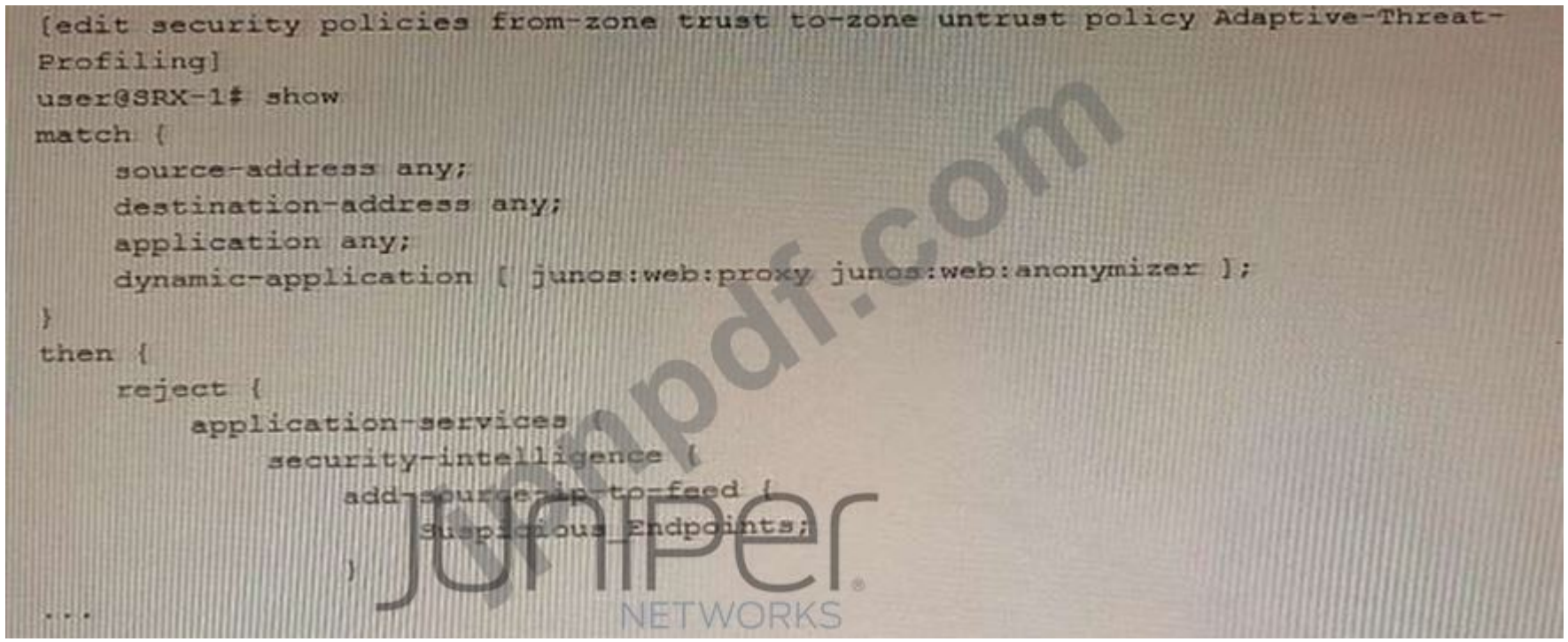
Answer: C,D (メーッセージを残す)

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-profile-logical-system.html

最新問題**: 50**

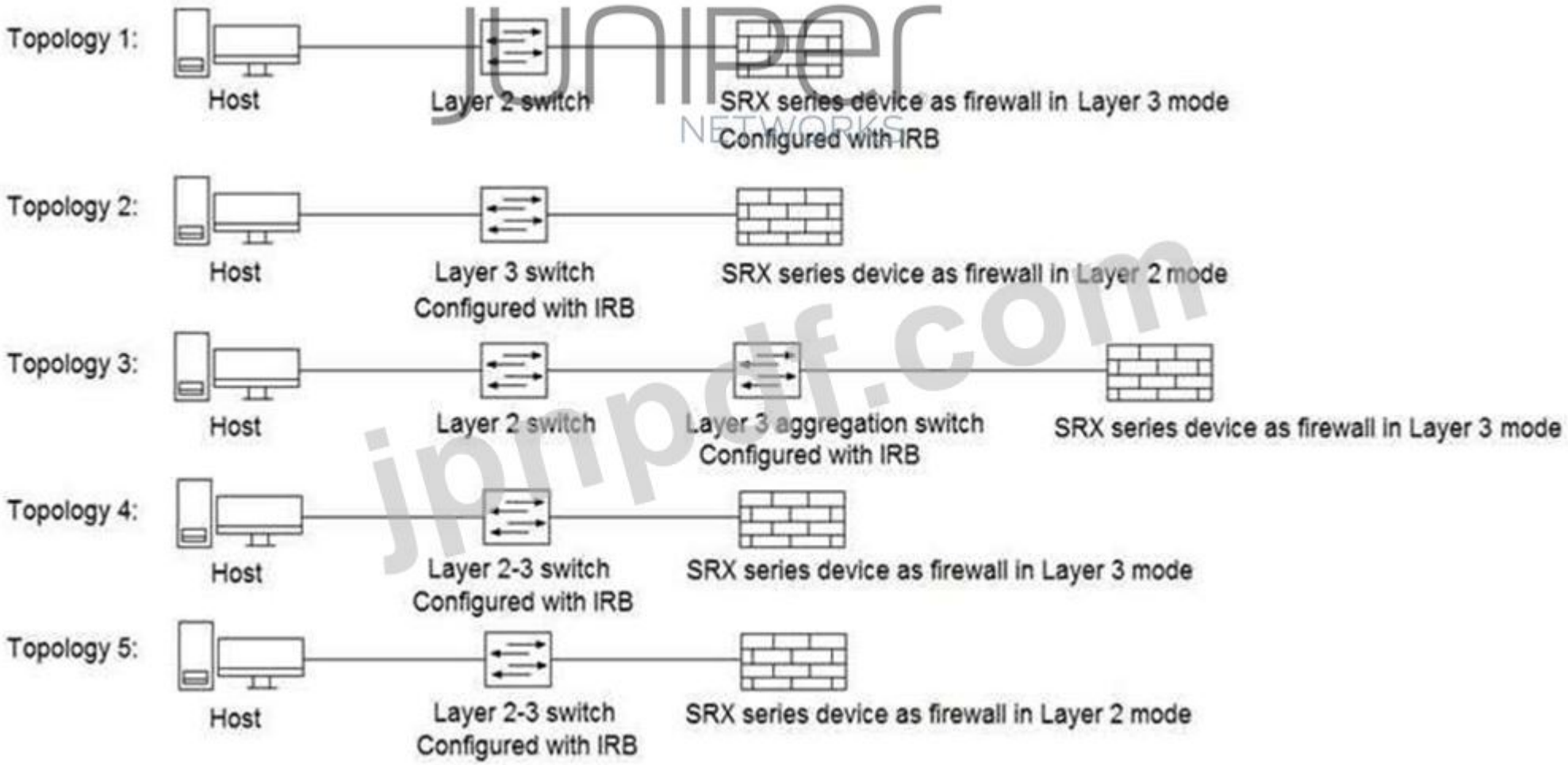
Juniper ATP アプライアンスの 2 つの有効なモードは何ですか? (2つお選びください。)
A. オールインワン
B. フローコレクター
C. イベントコレクター
D. コア
Answer: (解答を表示する**)**

最新問題**: 51**
示す



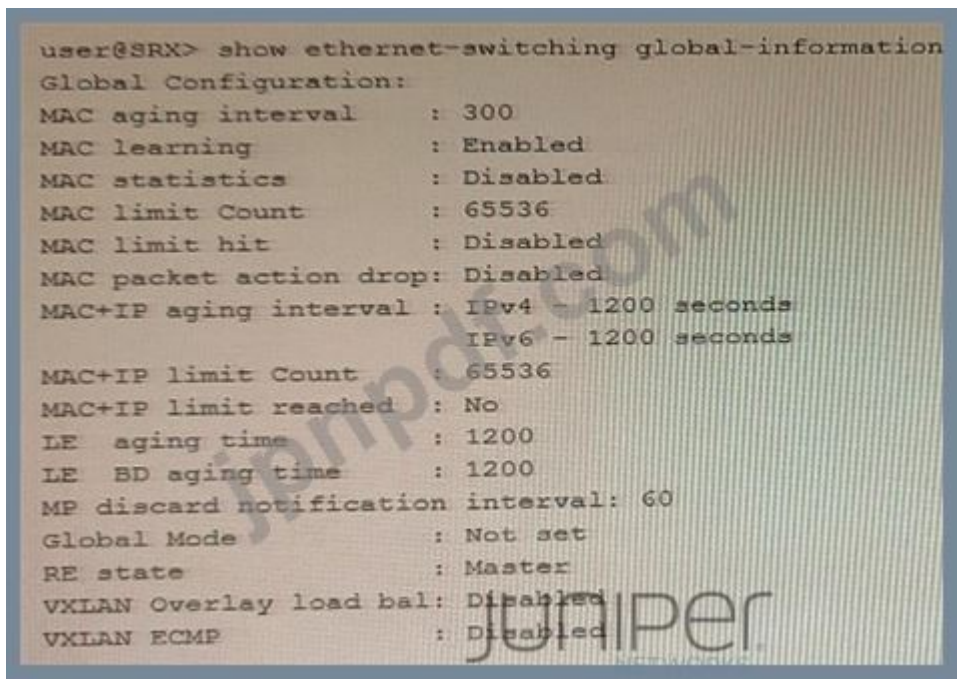
展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)
A. Juniper ATP Cloud は、セキュリティ ポリシーをコミットした後、3uopi'cioua_Endpoints フィードを自動的に作成します。
B. 3uspicious_Endpoint3 フィードは SRX-1 デバイスでのみ使用できます。
C. 3uspiciou3_Endpoint3 フィードは、SRX-1 と同じレルムの一部である任意の SRX シリーズ デバイスで使用できます。
D. Juniper ATP Cloud インターフェイスで疑わしい_Endpoint3 フィードを手動で作成する必要があります。
Answer: B,C (メーッセージを残す**)**

最新問題**: 52**
展示を参照すると、Policy Enforcer によってサポートされている 3 つのトポロジはどれですか? (3つお選びください。)



A. トポロジー 3
B. トポロジ 5
C. トポロジ 2
D. トポロジ 4
E. トポロジ 1
Answer: A,D,E (メーッセージを残す)
https://www.juniper.net/documentation/en_US/junos-space17.2/policy-enforcer/topics/concept/policy-enforcer-deployment-supported-topologies.html

最新問題: **53**
示す



同じブロードキャスト ドメイン内にある直接接続された複数のホストのパケットをスイッチングするように SRX シリーズ デバイスを設定しました。ただし、同じブロードキャスト ドメイン内の 2 つのホスト間のトラフィックがどのセキュリティ ポリシーにも一致しません。展示を参照すると、次のことを行う必要があります。この問題を解決します？

A. グローバルモードをスイッチングモードに変更する必要があります。

B. グローバル モードをセキュリティ ブリッジ モードに変更する必要があります

C. グローバルモードをセキュリティ切り替えモードに変更する必要があります。

D. グローバル モードをトランスペアレント ブリッジ モードに変更する必要があります。

Answer: B (メーッセージを残す**)**

最新問題**: 54**

SRX シリーズ デバイスで高可用性を実現するためにシャーシ クラスターを構成し、この HA クラスターを Juniper ATP クラウドに登録しました。

このシナリオで正しい 2 つの記述はどれですか? (2つお選びください。)

A. Juniper ATP Cloud にデバイスを登録した後、HA クラスターをセットアップする必要があります。

B. 両方のクラスター ノードで同じライセンス キーを使用する必要があります。

C. デバイスを登録する場合、登録する必要があるノードは 1 つだけです。

D. 両方のクラスター ノードで異なるライセンス キーを使用する必要があります。

Answer: A,B (メーッセージを残す**)**

最新問題**: 55**

HTTP トラフィックに I DP ポリシーを適用したいと考えています。

このシナリオでは、SRX シリーズ デバイスでどの 2 つのアクションを実行する必要がありますか? (2つお選びください)

A. 事前定義された攻撃グループ HTTP-All で攻撃タイプを選択します。

B. アプリケーション junos-http で一致します。

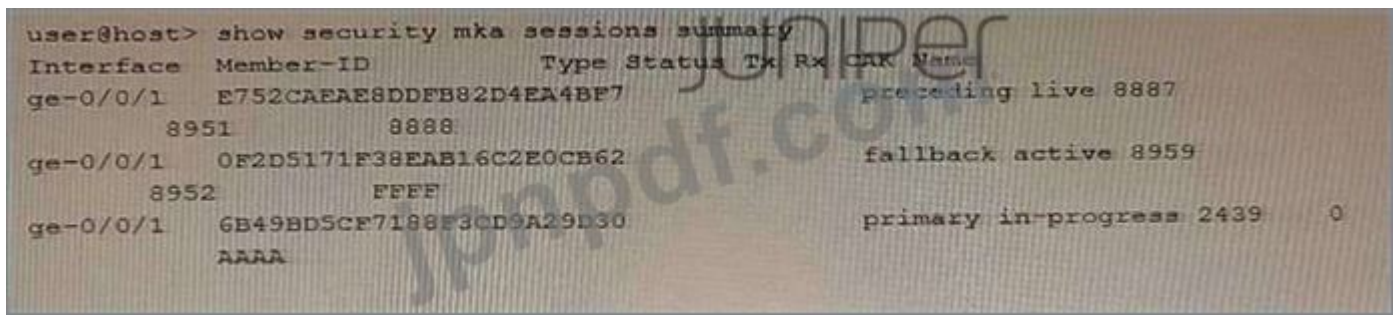
C. Untrust ゾーンの画面オプションを無効にします。

D. アクションなしを指定します。

Answer: (解答を表示する**)**

最新問題**: 56**
SRX5800 の構成オプションを使用して、論理システムを使用せずに、新しく作成された 2 つの仮想ルーター間のトラフィックをルーティングしたいと考えています。
仮想ルーター間の転送方法として、どちらをお勧めしますか? (2つお選びください。)
A. next-table コマンドを使用して、各仮想ルーターにスタティック ルートを作成します。
B. RIB グループを使用して、マスター ルーティング インスタンスからの内部ルーティング プロトコル ルートを共有します。
C. next-table オプションを使用して、静的ルートを使用して仮想ルーター間でトラフィックを転送します。
RIB グループを使用してリターン ルートを有効にします。
D. 各仮想ルータに 1 つある Boo 物理インターフェイス間を直接ケーブルで接続し、next-hop コマンドで静的ルートを使用します。
Answer: A,D (メーッセージを残す**)**

最新問題**: 57**
展示物を参照して、という名前の CAK の CAK ステータスについて正しい 2 つの記述はどれですか。
FFFP」? (2つお選びください。)



A. MACsec セッションの暗号化および復号化に CAK は使用されません。
B. CAK は MACsec セッションの暗号化と復号化に使用されます。
C. このキーを使用して SAK が正常に生成されました。
D. このキーを使用して SAK は生成されません。
Answer: B,D (メーッセージを残す**)**

最新問題**: 58**
マルウェアを分析および検出するために、Juniper ATP Cloud はどの 2 つの機能を実行しますか? (2つお選びください。)
A. ウイルス対策スキャン: 単一ベンダーのソリューションを使用して、ファイルに潜在的な脅威が含まれているかどうかを確認します。
B. 静的解析: ファイルを実際の環境で実行するとどうなるかを確認します。
C. キャッシュ検索: ファイルがすでに認識されており、悪意があることがわかっているかどうかを確認します。
D. 動的解析: 実際の環境でファイルを実行するとどうなるかを確認します。
Answer: (解答を表示する**)**

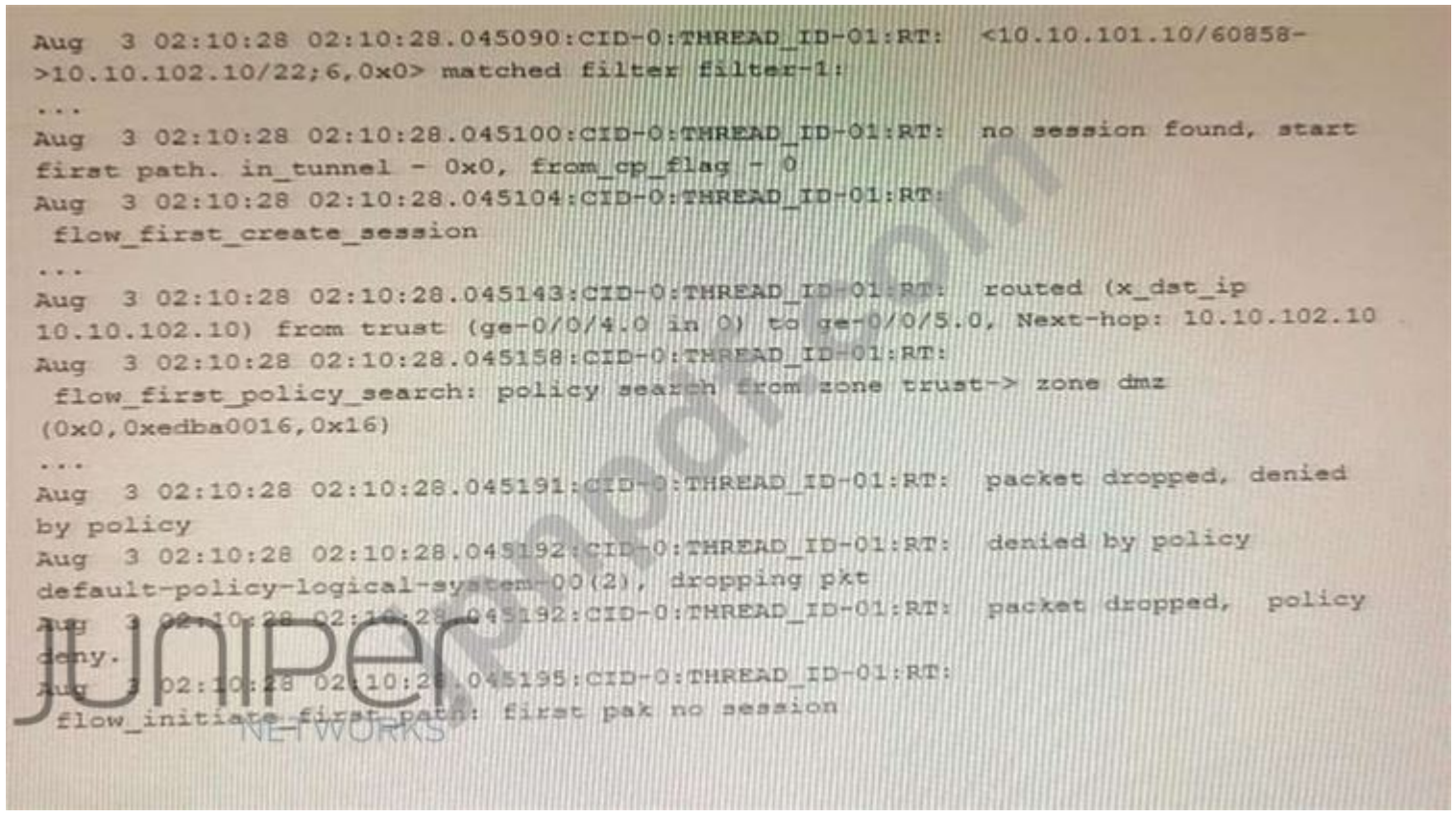
最新問題**: 59**
SRX シリーズ ファイアウォールでの DNS ドクタリングに使用される 2 つの機能はどれですか? (2つお選びください。)
A. ソース NAT

B. DNS ALG を有効にする必要があります。
C. 静的 NAT
D. DNS ALG を無効にする必要があります。
Answer: (解答を表示する**)**

最新問題**: 60**
組織には、ユーザー アクセスを制御するために複数の Active Directory ドメインがあります。セキュリティ ポリシーがユーザーのアクセス権に基づいてトラフィックを通過させていることを確認する必要があります。SRX シリーズ デバイスがこのタスクを達成するのに役立つものは何ですか?
A. ジムズ
B. ジュノススペース
C. JSA
D. JATP アプライアンス
Answer: A (メーッセージを残す**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-configure-jims.html

最新問題**: 61**
Juniper ATP Cloud にシングル サインオン (SSO) を提供するように求められます。この目標を達成するには、どの 2 つの手順を実行しますか?
(2つお選びください。)
A. Juniper ATP Cloud をアイデンティティ プロバイダー (IdP) として構成します。
B. Microsoft Azure をアイデンティティ プロバイダー (IdP) として構成します。
C. Juniper ATP Cloud をサービス プロバイダー (SP) として構成します。
D. Microsoft Azure をサービス プロバイダー (SP) として構成します。
Answer: B,D (メーッセージを残す**)**

最新問題**: 62**
示す



展示物に示されている出力について正しい 2 つの記述はどれですか? (2つお選びください。)

A. パケットはホストの受信トラフィックとして処理されます。

B. パケットはデフォルトのセキュリティ ポリシーに一致します。

C. パケットは設定されたセキュリティ ポリシーに一致します。

D. パケットは最初のパスのパケット フローで処理されます。

Answer: A,B (メーッセージを残す)

最新問題: **63**

SRX シリーズ デバイスを Juniper ATP Appliance に登録したいと考えています。デバイス間のパスにファイアウォール デバイスが存在します。このシナリオでは、ファイアウォール デバイスでどのポートを開く必要がありますか?

A. 8080

B. 443

C. 80

D. 22

Answer: (解答を表示する)

最新問題: **64**

「展示」ボタンをクリックします。

```
user@srx> show security mka statistics
Interface name: fxp1
Received packets:                          3
Transmitted packets:                       3
Version mismatch packets:                  0
CAK mismatch packets:                      6
ICV mismatch packets:                      0
Duplicate message identifier packets:      0
Duplicate message number packets:          0
Duplicate address packets:                 0
Invalid destination address packets:       0
Formatting error packets:                  0
Old Replayed message number packets        0
```

SRX345 の構成中に、デバイス間の MACsec 接続を確認すると、それが機能していないことに気づきました。
展示を参照して、問題を特定するためにどのアクションを使用しますか?

A. デバイス間のフォーマット設定が正しいこと、およびソフトウェアが使用中の MACsec のバージョンをサポートしていることを確認します。

B. 接続アソシエーション キーと接続アソシエーション キーの名前が両方のデバイスで一致することを確認します。

C. 伝送路でパケットの複製やフレームチェックシーケンスエラーパケットの修正が行われていないことを確認する

D. 2 つのデバイス間のインターフェイスが稼働しており、エラーが発生していないことを確認します。

Answer: B (メーッセージを残す**)**

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-security-mka-statistics.html

最新問題**: 65**

ADVPN を構成するときに必要な 3 つの役割またはプロトコルはどれですか? （3つお選びください。）

A. OSPF

B. ショートカットパートナー

C. ショートカット提案者

D. IKEv1

E. BGP

Answer: (解答を表示する**)**

https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-auto-discovery-vpns.html

最新問題**: 66**

シグネチャベースの攻撃防止にはどの Junos セキュリティ機能が使用されますか?

A. IPS

B. 半径

C. アプリのQoS

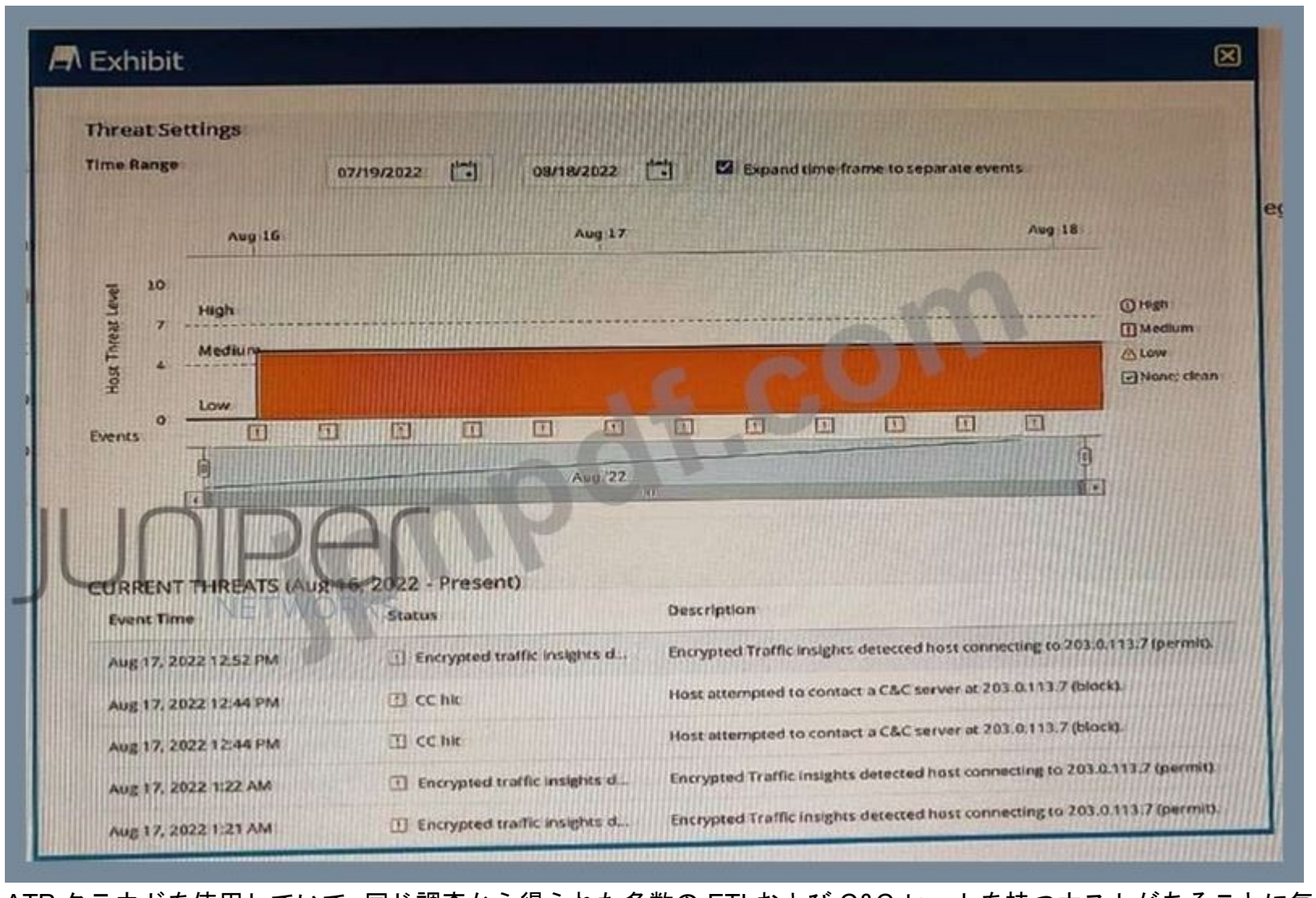
D. PIM

Answer: (解答を表示する**)**

最新問題**: 67**

中間ルーターでの CoS の処理を可能にする、2 台の SRX シリーズ デバイス間に IPsec VPN を構成するように求められます。
この要件を満たすものは何でしょうか?
A. ルートベース VPN
B. OpenVPN
C. リモート アクセス VPN
D. ポリシーベースの VPN
Answer: A (メーッセージを残す**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/secuirty-cos-based-ipsec-vpns.html

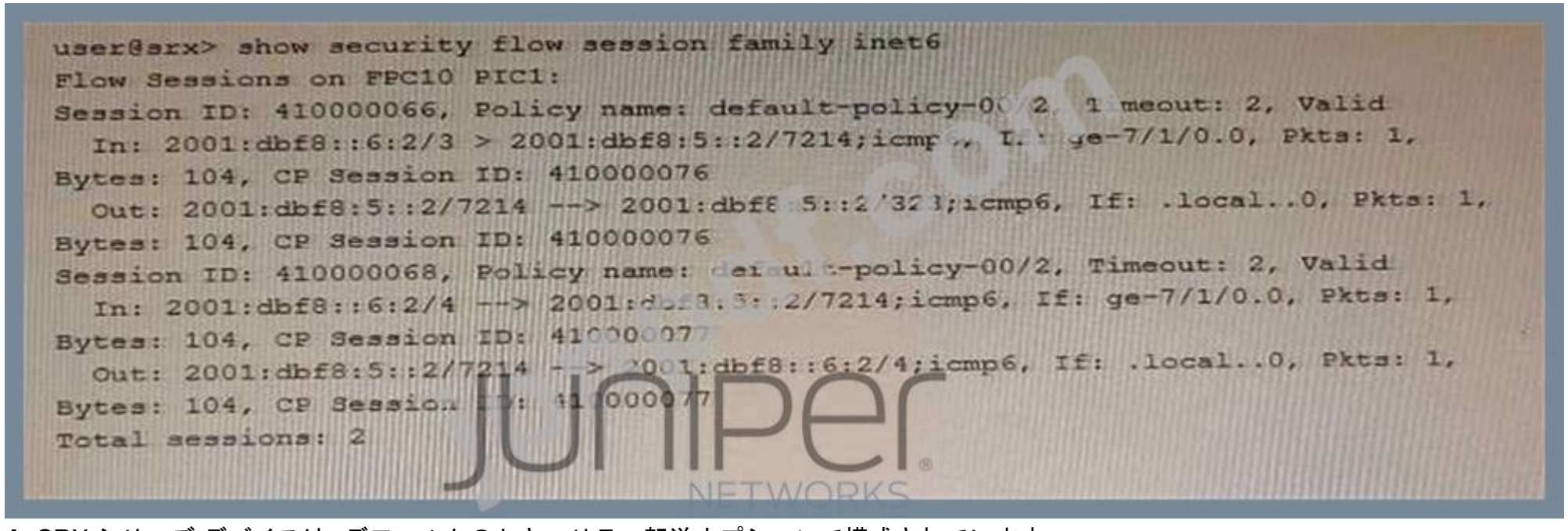
最新問題**: 68**
示す



ATP クラウドを使用していて、同じ調査から得られた多数の ETI および C&C ヒットを持つホストがあることに気付き、一部のイベントが自動的に緩和されていないことに気付きます。
展示物を参照して、この動作の理由は何ですか?
A. ETI イベントは誤検知です。
B. 感染ホストのスコアは、脅威レベル 5 未満にグローバルに設定されています。
C. C&C イベントは誤検知です。
D. 感染ホストのスコアは、脅威レベル 5 を超えてグローバルに設定されています。

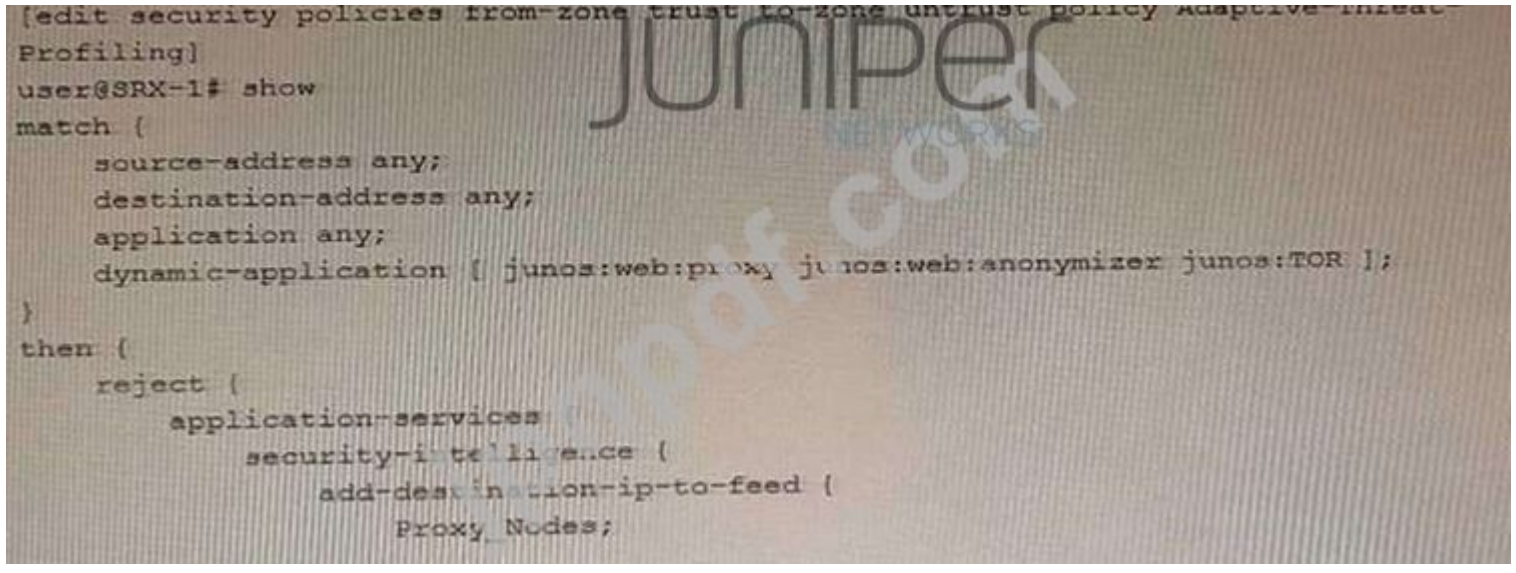
Answer: A (メーッセージを残す)

最新問題: **69**
展示物に示されている出力について正しいのはどれですか?



A. SRX シリーズ デバイスは、デフォルトのセキュリティ転送オプションで構成されています。
B. SRX シリーズ デバイスは、フローベースの IPv6 転送オプションを使用して構成されています。
C. SRX シリーズ デバイスは、パケットベースの IPv6 転送オプションを使用して構成されています。
D. SRX シリーズ デバイスは、IPv6 パケット転送を無効にするように構成されています。
Answer: A (メーッセージを残す)

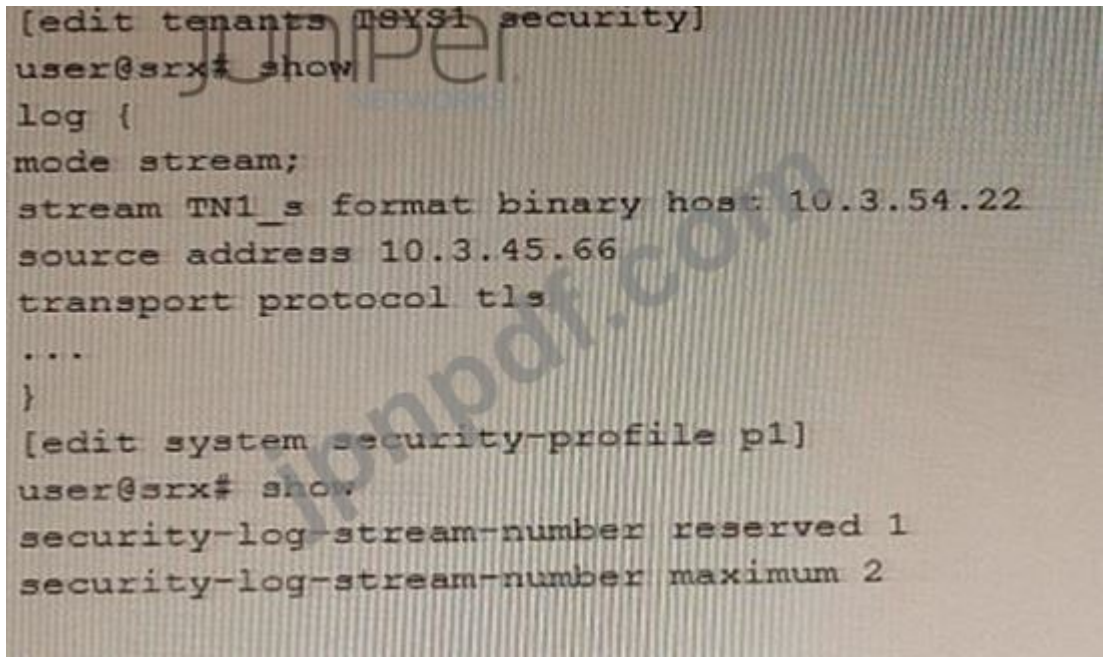
最新問題: **70**
展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)



A. SRX-1 デバイスは Proxy_wodes フィードを作成するため、それを別のセキュリティ ポリシーで使用できません。
B. Proxy_Node3 フィードは、別の SRX シリーズ デバイス上の別のセキュリティ ポリシーの宛先アドレス一致基準としてのみ使用できます。

C. SRX-1 デバイスは、別のセキュリティ ポリシーで Proxy__Nodes フィードを使用できます。
D. Proxy_Nodes フィードを、別の SRX シリーズ デバイス上の別のセキュリティ ポリシーの送信元アドレスと宛先アドレスの一致基準として使用できます。
Answer: (解答を表示する**)**

最新問題**: 71**
示す



管理者は、テナント システムのバイナリ セキュリティ イベントをログに記録するように SRX シリーズ デバイスを構成したいと考えています。
展示物を参照すると、どのステートメントが構成を完了しますか?
A. テナントを pi セキュリティ プロファイルのマスターとして構成します。
B. pi セキュリティ プロファイルのテナントを TSYS1 として構成します。
C. テナントを pi セキュリティ プロファイルの root として構成します。
D. テナントを pi セキュリティ プロファイルのローカルとして構成します
Answer: (解答を表示する**)**

最新問題**: 72**
展示」ボタンをクリックします。

SRX シリーズ デバイスを JATP に登録しようとすると、次のエラーが表示されます。
エラーの原因は何ですか?

A. ファイアウォールが fxp0 の HTTPS をブロックしています。
B. fxp0 IP アドレスはルーティング可能ではありません
C. SRX シリーズのデバイス証明書が JATP 証明書と一致しません
D. SRX シリーズ デバイスには、JATP にアクセスするインターフェイスに割り当てられた IP アドレスがありません。
Answer: (解答を表示する**)**

最新問題**: 73**
展示品に関して、正しい 2 つの記述はどれですか? (2つお選びください。)

A. 3uspiciou3_Endpoint3 フィードは、SRX-1 と同じレルムの一部である任意の SRX シリーズ デバイスで使用できます。
B. Juniper ATP Cloud は、セキュリティ ポリシーをコミットした後、3uopi'cioua_Endpoints フィードを自動的に作成します。
C. 3uspicious_Endpoint3 フィードは、SRX-1 デバイスでのみ使用できます。
D. Juniper ATP Cloud インターフェイスで疑わしい_Endpoint3 フィードを手動で作成する必要があります。
Answer: (解答を表示する**)**

最新問題**: 74**
示す

Exhibit

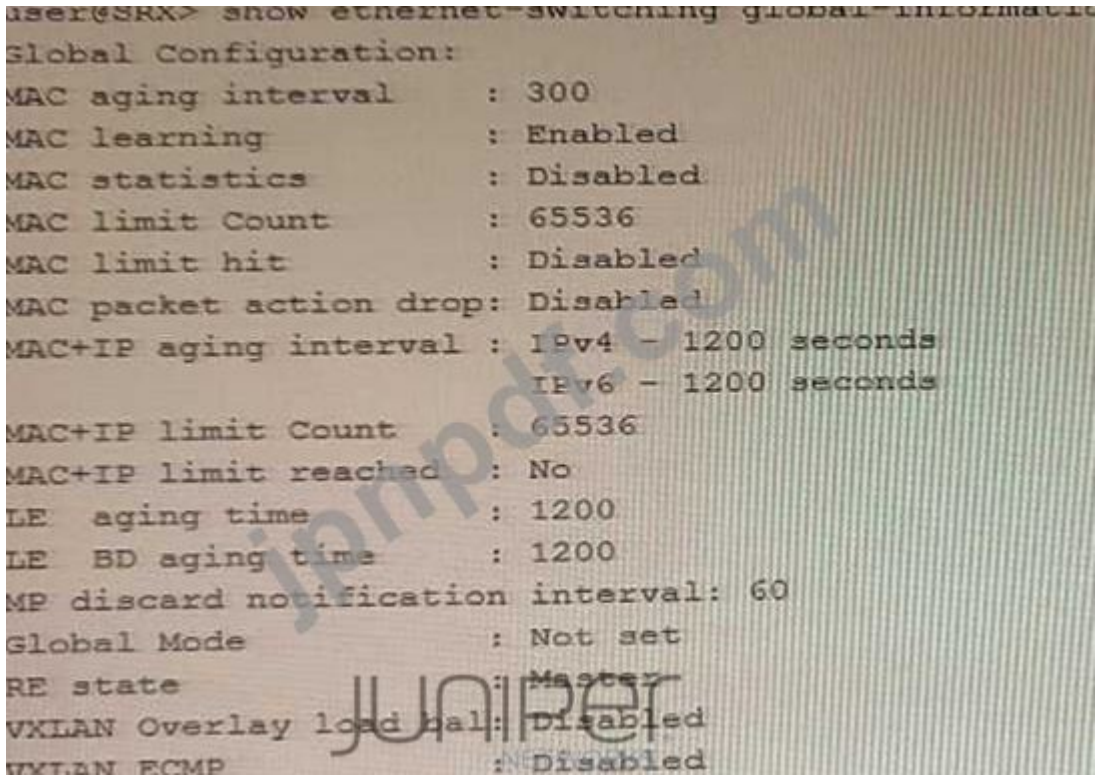
```
user@srx> show log flow-log
Apr 13 17:46:17 17:46:17.316930:CID-0:THREAD_ID-01:RT:<10.10.101.10/65131-
>10.10.102.1/22;6,0x0> matched filter F1:
Apr 13 17:46:17 17:46:17.317009:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from trust (ge-0/0/4.0 in 0) to ge-0/0/5.0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317016:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone trust-> zone dmz
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317019:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(8:trust) -> zone(9:dmz) scope:0
Apr 13 17:46:17 17:46:17.317020:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: permitted by policy
trust-to-dmz(8)
Apr 13 17:46:17 17:46:17.317031:CID-0:THREAD_ID-01:RT: packet passed,
Permitted by policy.
Apr 13 17:46:17 17:46:17.317038:CID-0:THREAD_ID-01:RT: choose interface ge-
0/0/5.0(P2P) as outgoing phy if
Apr 13 17:46:17 17:46:17.317042:CID-0:THREAD_ID-01:RT:is_loop_pak: Found loop
on ifp ge-0/0/5.0, addr: 10.10.102.1, rtt_idx: 0 addr_type:0x3.
Apr 13 17:46:17 17:46:17.317044:CID-0:THREAD_ID-
01:RT:flow_first_loopback_check: Setting interface: ge-0/0/5.0 as loop ifp.
Apr 13 17:46:17 17:46:17.317213:CID-0:THREAD_ID-01:RT:
flow_first_create_session
Apr 13 17:46:17 17:46:17.317215:CID-0:THREAD_ID-01:RT: flow_first_in_dst_nat:
0/0/5.0 as incoming nat if.
call flow_route_lookup(): src_ip 10.10.101.10, x_dst_ip 10.10.102.1, in ifp
ge-0/0/5.0, out ifp N/A sp 65131, dp 22, ip_proto 6, tos 0
Apr 13 17:46:17 17:46:17.317227:CID-0:THREAD_ID-01:RT: routed (x_dst_ip
10.10.102.1) from dmz (ge-0/0/5.0 in 0) to .local..0, Next-hop: 10.10.102.1
Apr 13 17:46:17 17:46:17.317228:CID-0:THREAD_ID-
01:RT:flow_first_policy_search: policy search from zone dmz-> zone junos-host
(0x0,0xfe6b0016,0x16)
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT:Policy lkup: vsys 0
zone(9:dmz) -> zone(2:junos-host) scope:0
Apr 13 17:46:17 17:46:17.317230:CID-0:THREAD_ID-01:RT: 10.10.101.10/65131 ->
10.10.102.1/22 proto 6
Apr 13 17:46:17 17:46:17.317236:CID-0:THREAD_ID-01:RT: packet dropped, denied
by policy
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: denied by policy deny-
ssh(9), dropping pkt
Apr 13 17:46:17 17:46:17.317237:CID-0:THREAD_ID-01:RT: packet dropped, policy
deny.
```

展示物に関して、正しい 3 つの記述はどれですか? (3つお選びください。)

A. パケットの宛先は DMZ ゾーン内のサーバーです。

B. パケットは SSH 接続を確立できます。
C. パケットは Trust ゾーン内で発信されました。
D. パケットの宛先は SRX シリーズ デバイスのインターフェイスです。
E. SSH 接続を確立する前にパケットがドロップされます。
Answer: C,D,E (メーッセージを残す**)**

最新問題**: 75**
同じブロードキャスト ドメイン内にある直接接続された複数のホストのパケットをスイッチするように SRX シリーズ デバイスを設定しました。ただし、同じブロードキャスト ドメイン内の 2 つのホスト間のトラフィックは、どのセキュリティ ポリシーにも一致しません。
展示品を参考に、この問題を解決するにはどうすればよいでしょうか?



A. グローバル モードをセキュリティ ブリッジ モードに変更する必要があります
B. グローバル モードをトランスペアレント ブリッジ モードに変更する必要があります。
C. グローバルモードをセキュリティ切替モードに変更する必要があります。
D. グローバルモードをスイッチングモードに変更する必要があります。
Answer: A (メーッセージを残す**)**

最新問題**: 76**
展示」ボタンをクリックします。

```
user@srx> show security flow session
Session ID: 11232, Policy name: Allow-ipv6-Telnet/11, Timeout: 1788, Valid
  In: 2001:db8::1/57707 --> 2001:db8::8/23;tcp, Conn Tag: 0x0, If: vlan.101,
Pkts: 9, Bytes: 799,
  Out: 10.8.8.8/23 --> 10.7.7.5/21868;tcp, Conn Tag: 0x0, If: ge-0/0/2.0,
Pkts: 8, Bytes: 589,
Total sessions: 1
```

展示されている NAT のタイプはどれですか?

A. DS-Lite

B. NAT64

C. NAT46

D. 永続的 NAT

Answer: (解答を表示する**)**

最新問題: **77**

IPsec VPN 構成では、2 つの CoS 転送クラスを使用して音声トラフィックとデータ トラフィックを分離します。このシナリオでは、IPsec ピア間にいくつの IKE セキュリティ アソシエーションが必要ですか?

A. 1

B. 2

C. 3

D. 4

Answer: B (メーッセージを残す**)**

最新問題: **78**

「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. ARP セキュリティは、制御インターフェイス全体でデータを保護します。

B. IPsec は制御インターフェイス全体でデータを保護しています

C. SSH は制御インターフェイス全体でデータを保護しています

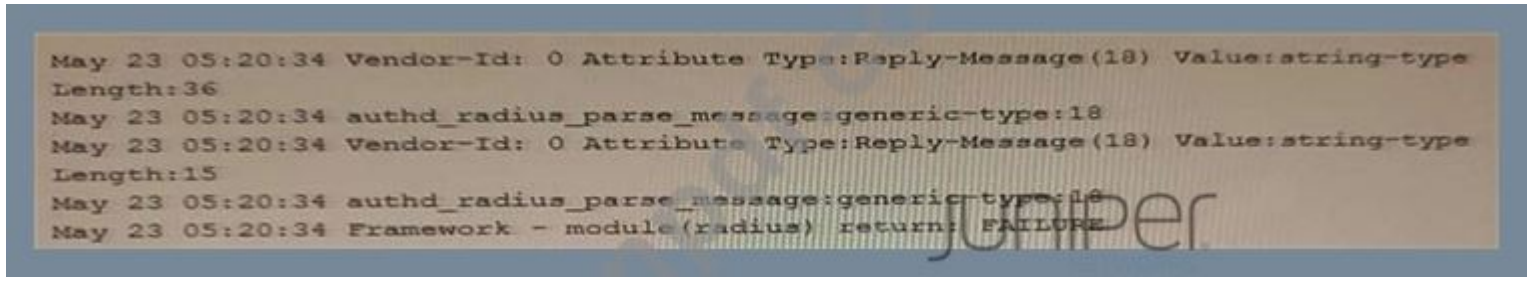
D. MACsec は制御インターフェイス全体でデータを保護しています

Answer: D (メーッセージを残す)

https://www.juniper.net/documentation/en_US/junos/topics/reference/command-summary/show-chassis-cluster-interfaces.html

最新問題**: 79**

示す



radius という名前のトレースオプション ファイルを設定すると、展示に示されている出力が返されます。問題の原因は何ですか?

A. 不正なパスワードが使用されています。

B. 認証順序の設定が間違っています。

C. RADIUS サーバーの IP アドレスに到達できません。

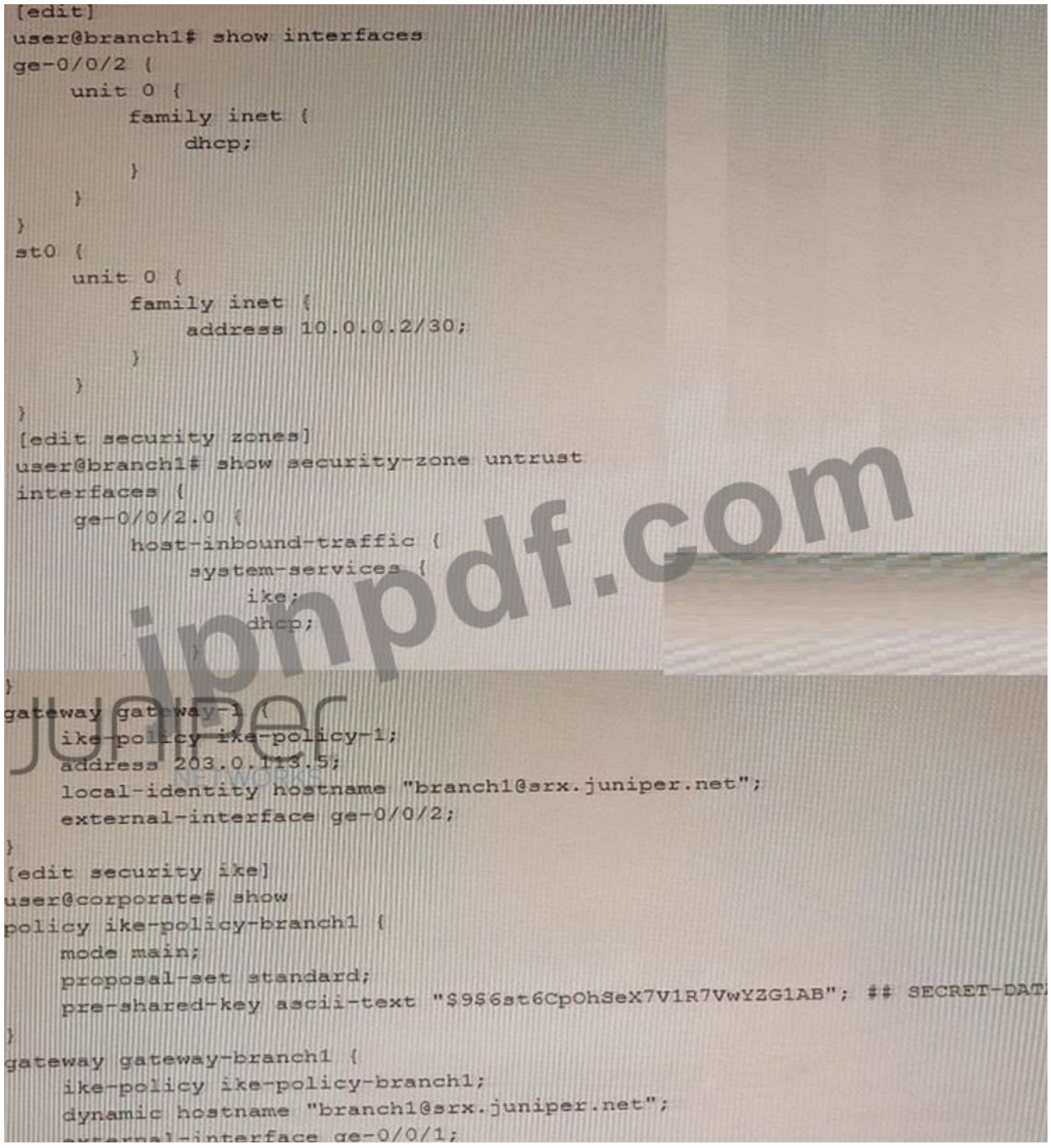
D. RADIUS サーバーにハードウェア障害が発生しました。

Answer: D (メーッセージを残す)

最新問題**: 80**

本社と支店 1 の SRX シリーズ デバイス間に IPsec トンネルを構成しようとしています。展示に示されている構成をコミットしましたが、IPsec トンネルが確立されていません。

このシナリオでは、何がこの問題を解決するでしょうか?



A. Branch1 デバイスの st0.0 インターフェイス設定にマルチポイントを追加します。
B. Branch1 および企業デバイスの IKE モードをアグレッシブに変更します。
C. IKE プロポーザル セットを、branch1 と企業デバイスで互換性のあるものに変更します。
D. Branch1 デバイス上のローカル ID を inet advpn に変更します。
Answer: D (メーッセージを残す)

最新問題**: 81**

組織には、ユーザー アクセスを制御するために複数の Active Directory ドメインがあります。セキュリティ ポリシーがユーザーのアクセス権に基づいてトラフィックを通過させていることを確認する必要があります。
SRX シリーズ デバイスがこのタスクを達成するのに役立つものは何ですか?
A. JATP アプライアンス
B. ジムズ
C. JSA
D. ジュノススペース
Answer: B (メーッセージを残す**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-user-auth-intergrated-user-firewall-overview.html

最新問題**: 82**
リモート オフィスで新しい SRX シリーズ CPE デバイスを構成するように求められます。デバイスは、MPLS および IPsec トラフィックの転送に参加する必要があります。
この実装に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. ホストの受信トラフィックはフロー モジュールによって処理されてはなりません
B. ホストの受信トラフィックはフロー モジュールによって処理される必要があります
C. SRX シリーズ デバイスは、デフォルトのトラフィック処理で MPLS と IPsec の両方を処理できます。
D. パケット モード転送を有効にするようにファイアウォール フィルターを構成する必要があります
Answer: (解答を表示する**)**
https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-packet-based-forwarding.html