PaloAltoNetworks.PCNSE.v2019-06-04.q64

試験コード：	PCNSE
試験名称：	Palo Alto Networks Certified Network Security Engineer Exam
認証ベンダー：	Palo Alto Networks
無料問題の数：	64
バージョン：	v2019-06-04
ページの閲覧量：	750
問題集の閲覧量：	16629

https://www.jpnshiken.com/shiken/PaloAltoNetworks.PCNSE.v2019-06-04.q64.html

質問: **1**
WebサーバーはDMZでホストされ、サーバーはTCPポート443で着信接続をリッスンするように設定されています。Trustゾーンから DMZゾーンへのアクセスを許可するセキュリティポリシールールは、Webブラウジングアクセスを許可するように設定する必要があります。WebサーバーはHTTP（S）を介してコンテンツをホストします。TrustからDMZへのトラフィックは、Forward Proxyルールで復号化されています。
tcp / 443でこのサーバーへの平文のWeb閲覧トラフィックを許可するには、サービスとアプリケーションの組み合わせ、およびセキュリティポリシールールの順序を設定する必要があります。
A. 規則＃1 :アプリケーション :Web閲覧。service :application-default;アクション：規則#2を許可する :application :ssl。service : application-default;アクション：許可
B. 規則1：適用ssl service :application-default;行動：規則#2を許可する :アプリケーション :ウェブ閲覧。service :application-default;アクション：許可
C. 規則＃1 :アプリケーション :Web閲覧。service :service-http;アクション：規則#2を許可する :application :ssl。service : application-default;アクション：許可
D. 規則＃1 :アプリケーション :Web閲覧service :service-https。アクション：規則#2を許可する :application :ssl。service : application-default;アクション：許可
正解: **(**正解を表示します**)**

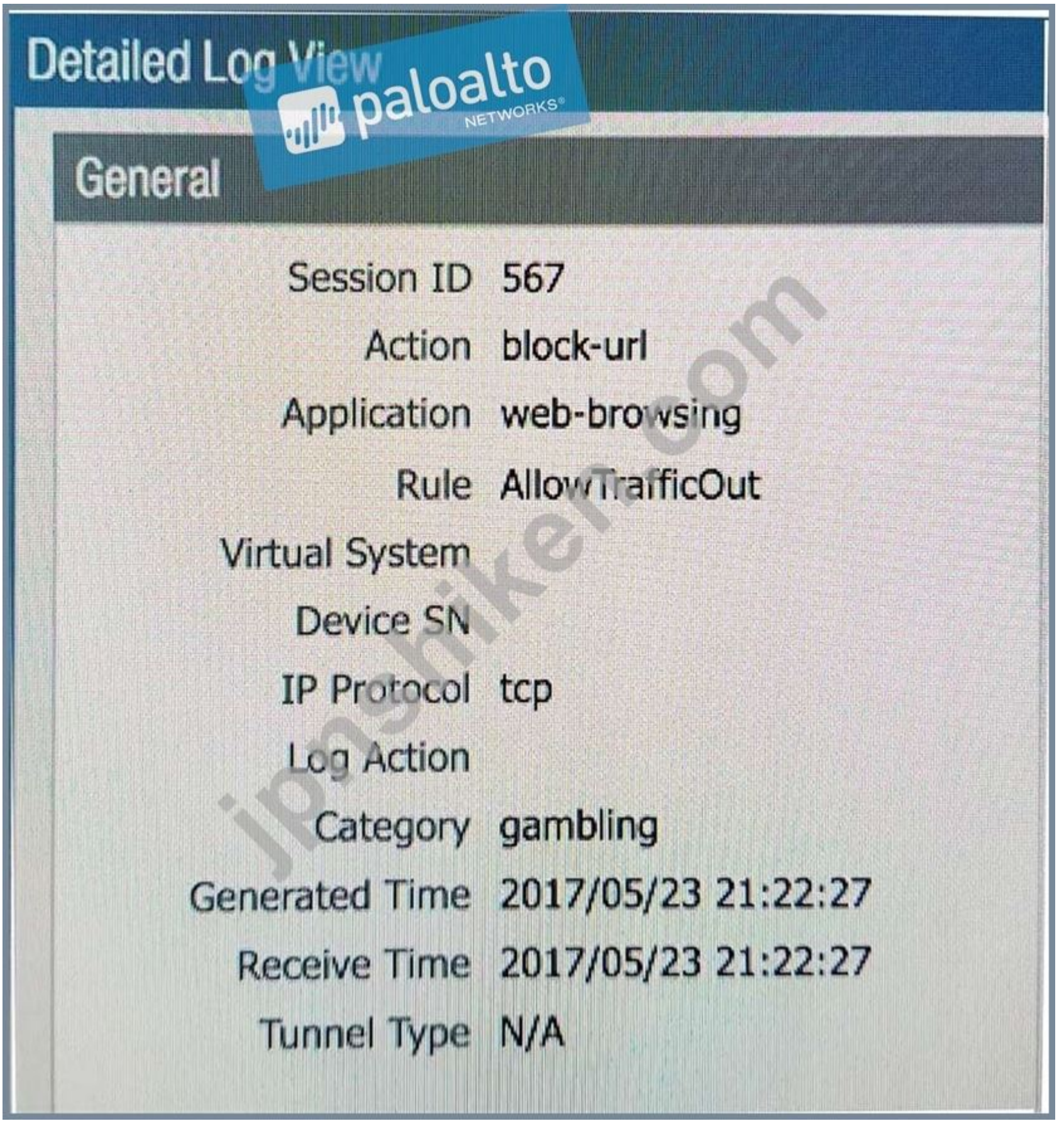
質問: **2**
管理者は、（クラウドではなく）ローカルの社内ラボ環境に100個の仮想ファイアウォールを作成するよう依頼されました。ブートストラップは、このタスクを実行するための最も便利な方法です。
どのオプションが、オンプレミスの仮想環境におけるブートストラップパッケージの展開を説明していますか？
A. USBメモリのconfig-driveを使用してください。
B. ISOの付いたS3バケットを使用します。
C. 仮想ハードディスク（VHD）を作成して接続します。
D. ISO付きの仮想CD-ROMを使用します。
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/virtualization/virtualization/set-up-the-vm-シリーズ-firewall-on-kvm install-the-vm-series-firewall-on-kvm / vmシリーズファイアウォールをデプロイするためのisoファイルの使用

質問: **3**
「復号化なし」アクションを使用して復号化プロファイルを復号化ポリシールールに割り当てると、どの2つの利点がありますか。（2つ選んでください。）
A. 有効期限が切れた証明書を使ってセッションをブロックする
B. クライアント認証でセッションをブロックする
C. サポートされていない暗号スイートとのセッションをブロックする
D. 信頼できない発行者とのセッションをブロックする
E. 認証情報フィッシングをブロックする
正解: **(**正解を表示します**)**
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/define-traf-復号化/復号化プロファイルの作成

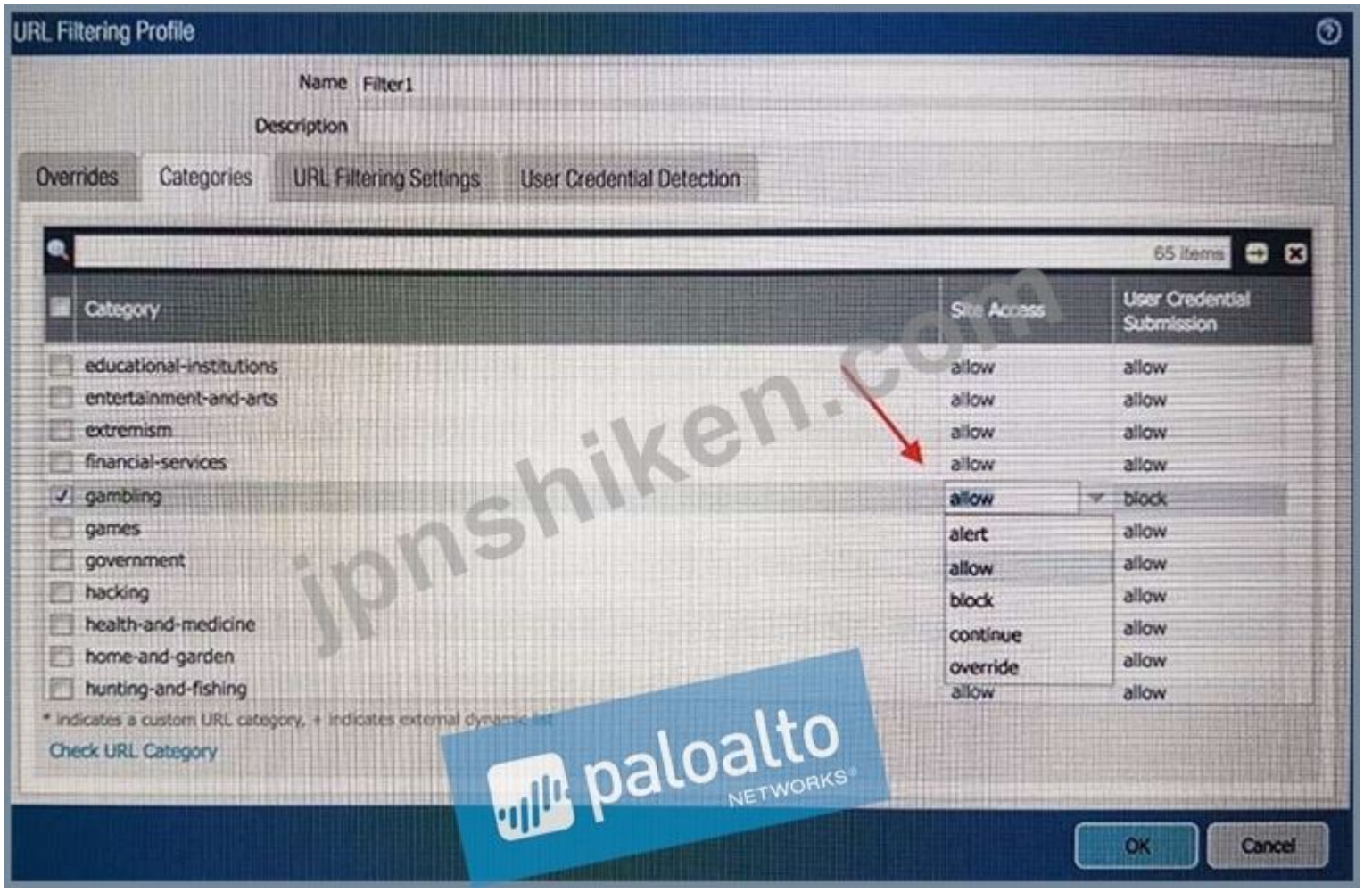
質問: **4**
セキュリティポリシールールは、脆弱性保護プロファイルと「拒否」のアクションで設定されます。
これにより、一致したトラフィックにどのアクションが設定されますか。
A. 設定が不正です。Actionがに設定されていると、Profile Settingsセクションはグレー表示されます。「拒否」
B. 設定が無効です。ファイアウォールはこのセキュリティポリシールールをスキップします。コミット中は警告が表示されます。
C. 脆弱性シグネチャが検出されない限り、設定は一致したセッションを許可します。の「拒否」アクションは、関連する脆弱性保護プロファイルに定義されている重大度ごとに定義されたアクションに優先します。
D. 設定は有効です。ファイアウォールは一致したセッションを拒否します。セキュリティポリシールールのアクションが[拒否]に設定されている場合、設定されているセキュリティプロファイルは無効です。
正解: **(**正解を表示します**)**

質問: **5**
管理者がWebサイトの証明書を所有していない場合、どのSSL復号化モードでPalo AltoネットワークNGFWはユーザーがHTTP $)Webサイトを閲覧したかを検査できますか？
A. SSL受信検査
B. SSL送信検査
C. TLS双方向プロキシ
D. SSL転送プロキシ
正解: **(**正解を表示します**)**

質問: **6**
管理者は、信頼ゾーンのユーザーが特定のWebサイトにアクセスできない理由を特定する必要があります。利用可能な唯一の情報は、次の図に示されています。管理者はどの構成を変更する必要がありますか？
A：


Detailed Log View
paloalto NETWORKS
General
Session ID 567
Action block-url
Application web-browsing
Rule AllowTrafficOut
Virtual System
Device SN
IP Protocol tcp
Log Action
Category gambling
Generated Time 2017/05/23 21:22:27
Receive Time 2017/05/23 21:22:27
Tunnel Type N/A

B :

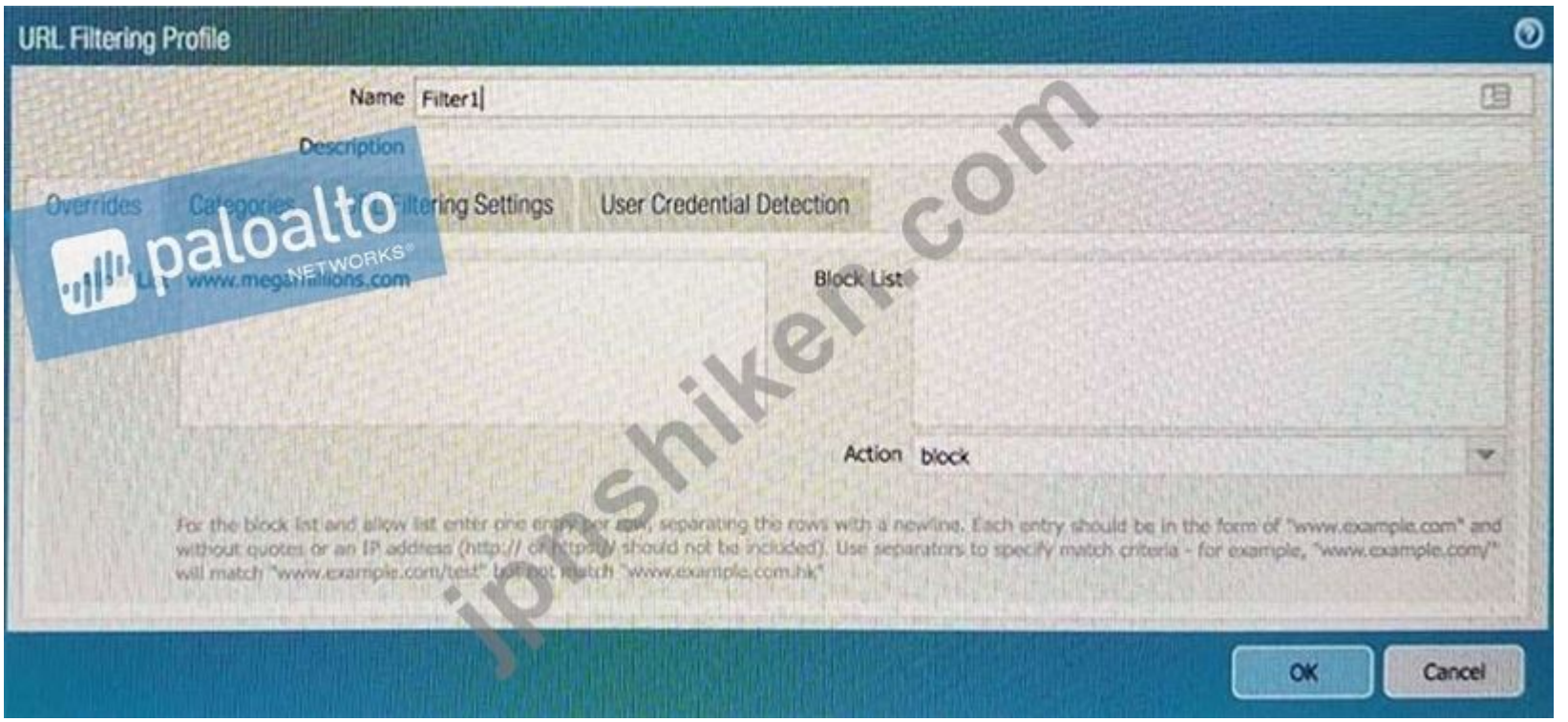

URL Filtering Profile
Name Filter1
Description
Overrides
Categories
URL Filtering Settings
User Credential Detection
65 items
Category
Site Access
User Credential Submission
educational-institutions
entertainment-and-arts
extremism
financial-services
gambling
games
government
hacking
health-and-medicine
home-and-garden
hunting-and-fishing
allow
block
alert
allow
block
continue
override
* indicates a custom URL category, + indicates external dynamic list
Check URL Category
OK
Cancel

子：


Security Policy Rule
General
Application
Service/URL Category
Actions
Name
www.megamillions.com
Rule Type
universal (default)
Description
Tags
OK
Cancel

D：

E :



A. オプションE
B. オプションC
C. オプションA
D. オプションD
E. オプションB
正解: **(**正解を表示します**)**

質問: **7**
高可用性では、HAデータリンクを介してどの情報が転送されますか？
A. セッション情報
B. ハートビート

C. HA状態情報
D. ユーザーID情報
正解: **A (**コメントを発表する**)**
説明/参照：
参照先：https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/high-availability/ha-concepts / ha-links-and-backup-links

質問: **8**
Panoramaでネストされたデバイスグループの2つの利点は何ですか？ （2つ選んでください。）
A. すべての機器に対して機能と設置場所の両方を設定する必要があります
B. すべての機器グループが共有グループの設定を引き継ぎます
C. 既存のセキュリティポリシーの規則とオブジェクトの再利用
D. ローカルファイアウォール設定を上書きします
正解: **(**正解を表示します**)**

質問: **9**
PanoramaのTemplatesオブジェクト内で定義されている3つの設定はどれですか。 （3つ選んでください。）
A. セキュリティ
B. アプリケーションの上書き
C. インタフェース
D. 仮想ルーター
E. 設定
正解: **(**正解を表示します**)**

質問: **10**
展示を参照してください。

```
################################
admin@Lab33-111-PA-3060(active)>show routing fib

id        destination       nexthop       flags   interface       mtu
--------------------------------------------------------------------
47        0.0.0.0/0         10.46.40.1    ug      ethernet1/3     1500
46        10.46.40.0/23     0.0.0.0       u       ethernet1/3     1500
45        10.46.41.111/32   0.0.0.0       uh      ethernet1/3     1500
70        10.46.41.113/32   10.46.40.1    ug      ethernet1/3     1500
51        192.168.111.0/24  0.0.0.0       u       ethernet1/6     1500
50        192.168.111.2/32  0.0.0.0       uh      ethernet1/6     1500

--------------------------------------------------------------------
################################

admin@Lab33-111-PA-3060(active)>show virtual-wire all

total virtual-wire shown:
flags:   m-multicast firewalling
         p= link state pass-through
         s- vlan sub-interface
         i- ip+vlan sub-interface
         t-tenant sub-interface

name          interface1      interface2      flags           allowed-tags
-----------------------------------------------------------------------------
VW-1          ethernet1/7     ethernet1/5     p

####################################
```

トラフィックの入力インターフェイスがイーサネット1/7からの送信である場合、これは出力インターフェイスになります。192.168.111.3と目的地10.46.41.113に？

A. イーサネット1/5
B. イーサネット1/3
C. イーサネット1/6
D. イーサネット1/7
正解: **(**正解を表示します**)**

質問: **11**
どのようにして候補または実行中の設定をPanoramaの外部のホストにコピーできますか？

A. 実行コンフィギュレーションを確定します。
B. 構成スナップショットを保存します。
C. 候補設定を保存します。
D. 名前付き設定スナップショットをエクスポートします。
正解: **D** (コメントを発表する)
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/71/panorama/panorama_adminguide/管理パノラマ/バックアップパノラマとファイアウォールの設定

質問: **12**
Palo Alto Networks NGFWを通過するユーザーのトラフィックは、http ://www.company.comに到達することがあります。それ以外の場合はセッションがタイムアウトします。NGFWは、http://www.company.comにアクセスしたときにユーザーのトラフィックが一致するというPBF規則を使用して構成されています。
ネクストホップがダウンした場合、どうやってファイアウォールを設定してPBFルールを自動的に無効にすることができますか？
A. 問題のPBFルールにフェールオーバーのアクションを含むモニタープロファイルを作成して追加します。
B. 仮想ルーターのデフォルトルートでネクストホップゲートウェイのパス監視を設定します。
C. 問題のPBFルールで、Wait RecoverのアクションでMonitor Profileを作成して追加します。
D. ファイアウォールの外部インターフェース用のリンク監視プロファイルを有効にして設定します。
正解: (正解を表示します)

質問: **13**
どのセキュリティポリシールールで、管理者はFacebookチャットをブロックすることができますが、一般にFacebookは許可されますか。
A. アプリケーションfacebookを許可する前にアプリケーションfacebook-chatを拒否します
B. アプリケーションフェイスブックの拒否
C. アプリケーションフェイスブックを前面に表示する
D. アプリケーションfacebook-chatを拒否する前にアプリケーションfacebookを許可する
正解: (正解を表示します)
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Configuration-Articles/Failed-to-Block-Facebook-Chat-一貫して/ ta-p / 115673

質問: **14**
管理者がNGFWの仮想ルーターでOSPFを有効にしました。OSPFは仮想ルーターに新しいルートを追加していません。
管理者がこの問題を解決するには2つの方法がありますか。 2つ選んでください。）
A. BGPアップデートとして転送する再配布プロファイルを追加します。
B. システムログを表示します。
C. ルーティング段階でトラフィックpcapを実行します。
D. 仮想ルーターのランタイム統計を表示します。
正解: (正解を表示します)

質問: **15**
管理者がPalo Alto Networks NGFWにログインし、WebUIにPoliciesタブがないことを報告します。[ポリシー]タブが表示されない原因は、どのプロファイルですか？
A. 認証
B. 管理者ロール
C. WebUI
D. 権限
正解: **(**正解を表示します**)**

質問: **16**
管理者がPanoramaと複数のPalo Alto Networks NGFWを使用しています。すべてのデバイスを最新のPAN-OS®ソフトウェアにアップグレードした後、管理者はファイアウォールからPanoramaへのログ転送を有効にします。
ファイアウォールからの既存のログは、Panoramaには表示されません。
どのアクションによってファイアウォールが既存のログをPanoramaに送信できるようになりますか？
A. ログデータベースをファイアウォールからエクスポートし、手動でPanoramaにインポートする必要があります。
B. インポートオプションを使用してログをPanoramaにプルします。
C. CLIコマンドは既存のログをPanoramaに転送します。
D. ACCを使用して既存のログを統合します。
正解: **(**正解を表示します**)**

質問: **17**
管理者がApplication Override Policyを使用した場合、どのイベントが発生しますか？
A. 脅威IDの処理時間が短縮されました。
B. Palo Alto Networks NGFWはレイヤ4でApp-ID処理を停止します。
C. セキュリティルールによってトラフィックに割り当てられたアプリケーション名がトラフィックログに書き込まれます。
D. App-IDの処理時間が長くなります。
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Learning-Articles/Tips-amp-Tricks-How-to-Create-an- Application-Override / ta-p / 65513

質問: **18**

ユーザーが誤って企業の認証情報をフィッシングWebサイトに送信するのを防ぐためにどの機能を設定する必要がありますか？
A. URLフィルタリングプロファイル
B. ゾーン保護プロファイル
C. スパイウェア対策プロファイル
D. 脆弱性対策プロファイル
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/threat-prevention/prevent-クレデンシャルフィッシング

質問: **19**
管理者のPalo Alto Networks NGFW宛てのVPNトラフィックが、傍受者によって悪意を持って傍受され、再送信されています。
VPNトンネルを作成するとき、この悪意のある動作を防ぐためにどの保護プロファイルを有効にできますか？
A. ゾーン保護
B. Webアプリケーション
C. リプレイ
D. DoS保護
正解: **(**正解を表示します**)**

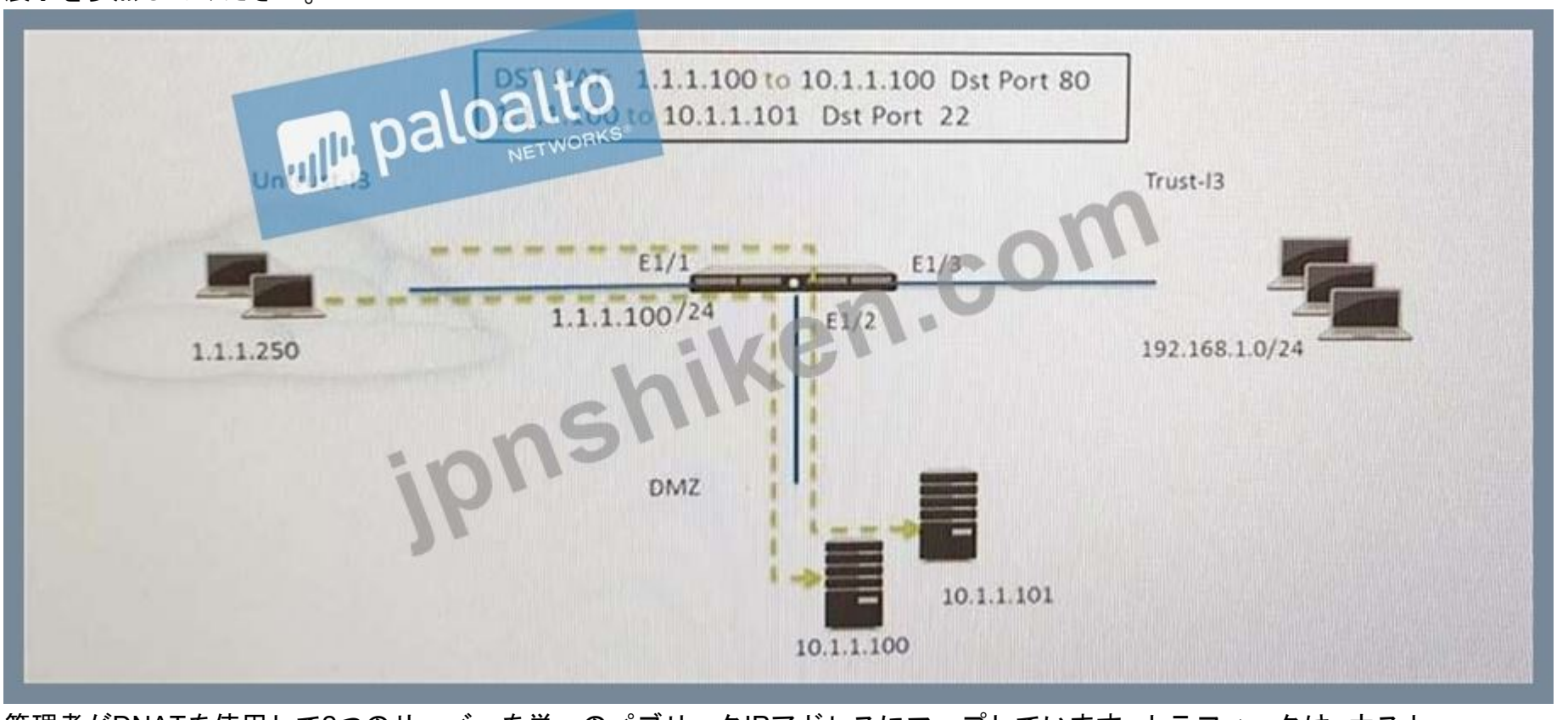
質問: **20**
管理者は、内部システム上のオペレーティングシステムの欠陥を悪用しようとする外部ホストに対する保護を提供するために、Palo Alto Networks NGFWを設定するよう求められました。
どのセキュリティプロファイルタイプがこの攻撃を防ぎますか？
A. 脆弱性対策
B. スパイウェア対策
C. URLフィルタリング
D. ウイルス対策
正解: **(**正解を表示します**)**
説明/参照：
参照先 :https://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/objects/objects/objects/security-profiles-脆弱性保護

質問: **21**
管理者は、Palo Alto Networks NGFWを最新バージョンのPAN-OS®ソフトウェアにアップグレードする必要があります。ファイアウォールは、イーサネットインターフェイスを介してインターネットに接続できますが、管理インターフェイスからはインターネットに接続できません。セキュリティポリシーには、デフォルトのセキュリティルールと、任意のゾーンから任意のゾーンへのすべてのWeb閲覧トラフィックを許可するルールがあります。
PAN-OS®ソフトウェアをアップグレードできるように、管理者は何を設定する必要がありますか？
A. スケジューラ
B. CRL

C. サービス経路
D. セキュリティポリシールール
正解: **(**正解を表示します**)**

質問: **22**
管理者は、重要度の低いアプリケーションよりもビジネスクリティカルなアプリケーションを優先するようにトラフィックを最適化する必要があります。
サービス品質を提供するために、QoSはどの機能とネイティブに統合されていますか。
A. ポート検査
B. 証明書の失効
C. コンテンツID
D. アプリID
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/quality-of-service/qos- concepts /アプリケーションおよびユーザー向けqos#idaed4e749-80b4-4641- a37c-c741aba562e9

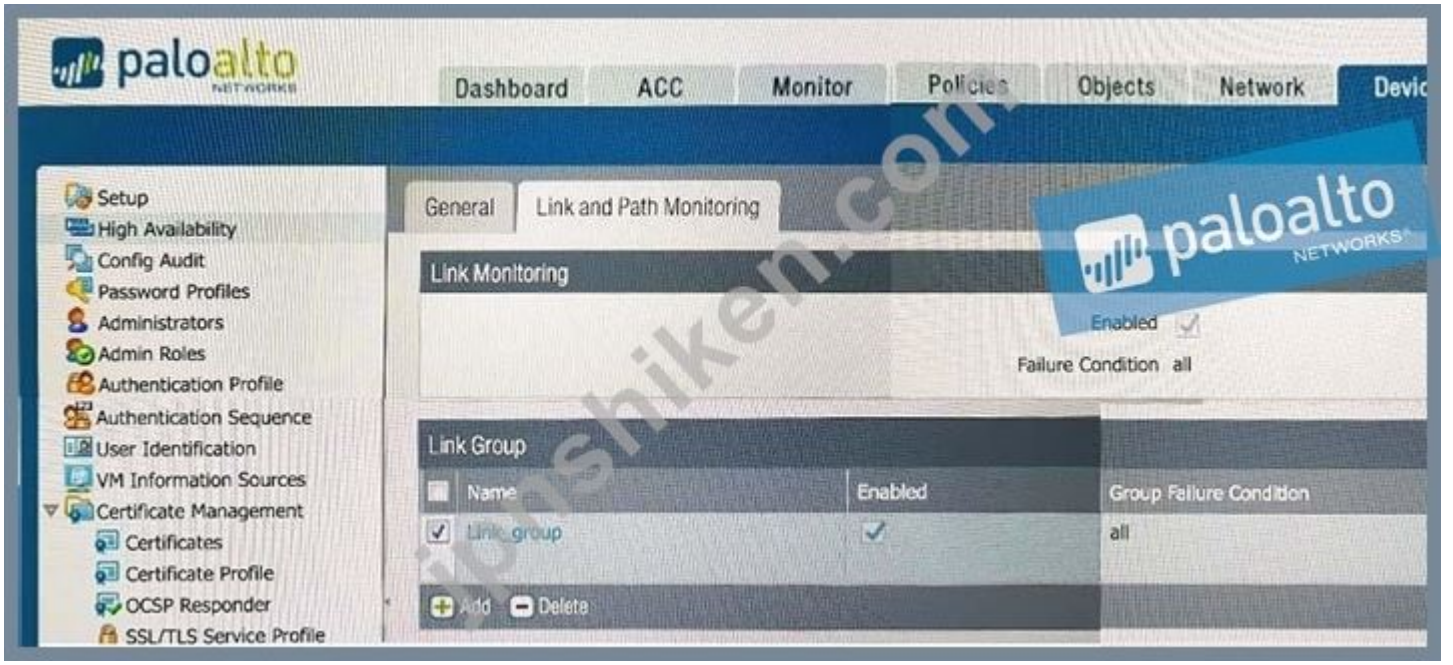
質問: **23**
展示を参照してください。



管理者がDNATを使用して2つのサーバーを単一のパブリックIPアドレスにマップしています。トラフィックは、ホストA（10.1.1.100）がHTTPトラフィックを受信し、ホストB（10.1.1.101）がSSHトラフィックを受信するアプリケーションに基づいて特定のサーバに誘導されます。（2つ選んでください。）
A. Untrust（Any）からUntrust（10.1.1.1）へ、ssh -Allow

B. Untrust（Any）からUntrust（10.1.1.1）へ、Webブラウジング - 許可する
C. DMZ（10.1.1.1）に信頼できない（Any）、ssh - 許可
D. DMZ（10.1.1.1）に信頼できない（Any）、Webブラウジング - 許可する
E. DMZ（10.1.1.100.10.1.1.101）に信頼できない（Any）、ssh、Webブラウジング - 許可する
正解: (正解を表示します)

質問: **24**
ファイアウォールにリンクモニタリング設定がある場合、フェールオーバーの原因は何ですか？



A. ethernet1 / 6がダウン
B. ethernet1 / 3またはEthernet1 / 6が停止しています
C. ethernet1 / 3がダウン
D. ethernet1 / 3とethernet1 / 6がダウンしています
正解: (正解を表示します)

質問: **25**
管理者がレイヤ7シグニチャを含むカスタムアプリケーションを作成します。最新のアプリケーションと脅威の動的アップデートが同じNGFWにダウンロードされます。このアップデートには、カスタムアプリケーションと同じトラフィックシグニチャに一致するアプリケーションが含まれています。
NGFWを通過するトラフィックを識別するために使用するアプリケーションはどれですか。
A. システムログにアプリケーションエラーが表示され、どちらの署名も使用されていません。
B. ダウンロードしたアプリケーション
C. カスタムアプリケーション
D. カスタムおよびダウンロードされたアプリケーションの署名ファイルがマージされ、両方が使用されます
正解: (正解を表示します)

質問: **26**

A Palo Alto Networks NGFWは分析のためにWildFireにファイルを提出しました。分析のために5分間のウィンドウを想定してください。ファイアウォールは5分ごとに判定をチェックするように設定されています。
ファイアウォールはどのくらい早く判定を受けますか？
A. 5〜10分
B. 10〜15分
C. 5分
D. 15分以上
正解: **A** (コメントを発表する)

質問: **27**
ローカルファイアウォールで対応する管理者アカウントを定義せずに、管理者がPalo Alto Networks NGFWの管理者を認証するために使用できる3つの認証サービスはどれですか。 3つ選んでください。）
A. LDAP
B. TACACS +
C. PAP
D. RADIUS
E. SAML
F. Kerberos
正解: (正解を表示します)

質問: **28**
ファイアウォールがそれを通過するトラフィックをキャプチャするのを妨げる2つのオプションはどれですか。 2つ選んでください。）
A. ファイアウォールはマルチvsysモードです。
B. トラフィックはオフロードされています。
C. トラフィックはパケットキャプチャフィルタと一致しません。
D. ファイアウォールのDP CPUが50%を超えています。
正解: (正解を表示します)
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/monitoring/take-packet- captures / disable-hardware-offload

質問: **29**
管理者がPalo Alto Networks NGFW上の仮想ルーターでBGPを有効にしましたが、新しいルーターが仮想ルーターに追加されていないようです。
管理者がこの問題のトラブルシューティングに役立つ2つのオプションはどれですか。 2つ選んでください。）
A. ランタイム統計を表示し、BGP設定に関する問題を探します。
B. システムログを表示し、BGPに関するエラーメッセージを探します。
C. NGFWでトラフィックpcapを実行してBGPの問題を確認します。
D. ルーティングの問題を特定するには、[ACC]タブを表示します。

正解: **A,D** (コメントを発表する)

質問: **30**
エンタープライズPKIを使用している管理者は、Panoramaと管理対象ファイアウォールおよびLog Collectorとの間の相互認証を保証するために独自の信頼チェーンを確立する必要があります。
管理者はどのように信頼チェーンを確立しますか？
A. カスタム証明書を使う
B. LDAPまたはRADIUS統合を有効にします
C. 多要素認証を設定する
D. 強力なパスワード認証を設定します
正解: (正解を表示します)
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/ panorama-overview / plan-your-panorama-deployment

質問: **31**
管理者が、任意のポートのSSLセッションを復号化するSSL復号化ポリシールールを作成しました。
セッションが復号化されていることを確認するために管理者はどのログエントリを使用できますか？
A. トラフィックログの詳細情報
B. 復号化ログ
C. データフィルタリングログ
D. 脅威のログエントリの詳細
正解: (正解を表示します)
説明/参照：
参照：https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Implement-and-Test-SSL-復号化/ ta-p / 59719

質問: **32**
ある顧客が、自分のカスタムPostgreSQLデータベース接続の1つに対して不明トップとして識別されているアプリケーションを持っています。カスタムデータベースアプリケーションを正しく分類するために使用できる設定オプションは2つありますか。 2つ選んでください。）
A. アプリケーションオーバーライドポリシー
B. カスタムアプリケーション
C. カスタムアプリケーションを識別するためのセキュリティポリシー

D. カスタムサービスオブジェクト
正解: **(**正解を表示します**)**

質問: **33**
トラフィックログのセッションがアプリケーションを 珠完了」として報告しています。 不完全」とはどういう意味ですか？
A. 3方向のTCPハンドシェイクが確認されましたが、アプリケーションを識別できませんでした。
B. データは受信されましたが、App-IDが適用される前に拒否ポリシーが適用されたために即座に破棄されました。
C. 3方向TCPハンドシェイクは完了しませんでした。
D. トラフィックはUDPを通過しているため、アプリケーションを識別できませんでした。
正解: **A (**コメントを発表する**)**

質問: **34**
過去30日間に検出された脅威など、一定の期間のトラフィックの傾向を見ることができるツールを管理者に提供するツールはどれですか。
A. セッションブラウザ
B. アプリケーションコマンドセンター
C. TCPダンプ
D. パケットキャプチャ
正解: **B (**コメントを発表する**)**
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Management-Articles/Tips-amp-Tricks-How-to-Use-the- Application-Command-Center-ACC / ta-p / 67342

質問: **35**
基本的なWildFireサービスの一部として、3つのファイルタイプを分析のためにWildFireに転送できますか。
（3つ選んでください。）
A. .dll
B. .exe
C. .src
D. .apk
E. .pdf
F. .jar
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/wildfire/wf_admin/wildfire-overview/ wildfire-file-type-support

質問: **36**
VMシリーズのファイアウォールでどの機能を設定できますか？
A. 複数の仮想システム
B. 集約インターフェース

C. GlobalProtect
D. 機械学習
正解: **(**正解を表示します**)**

質問: **37**
どの3つのファイアウォール状態が有効ですか？ （3つ選んでください。）
A. アクティブ
B. 機能的
C. 保留中
D. パッシブ
E. 中断中
正解: **A,D,E (**コメントを発表する**)**
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/high-availability/ha- firewall-states

質問: **38**
「Domain Credential Filter」メソッドを使用してファイアウォールがクレデンシャルフィッシング防止に設定されている場合、どのログインがクレデンシャルの盗難として検出されますか？
A. ログインユーザーのIPアドレスへのマッピング。
B. 有効な会社のユーザー名と一致するユーザー名の最初の4文字。
C. 同じユーザーの会社のユーザー名とパスワードを使用します。
D. 有効な会社のユーザー名を変更します。
正解: **(**正解を表示します**)**
説明/参照：
参照先：https://www.paloaltonetworks.com/documentation/80/pan-os/newfeaturesguide/content- inspection-features / credential-phishing-protection

質問: **39**
DNSサーバーに対するサービス拒否攻撃のため、クライアントはリソースの枯渇を心配しています。
どのオプションが個々のサーバーを保護しますか？
A. 分類されたDoS保護プロファイルを適用します。
B. DNSシンクホールリングを使用してスパイウェア対策プロファイルを適用します。
C. application-defaultと共にDNS App-IDを使用します。
D. Zone Protection Profileでパケットバッファ保護を有効にします。
正解: **(**正解を表示します**)**

質問: **40**
管理者は、Citrix XenApp 7 xを介してユーザーにネットワークリソースへのアクセス権を与えます。Citrixを使用してネットワークに接続しリソースにアクセスする複数のユーザーをマッピングするのは、どのユーザーIDマッピングソリューションですか？
A. ターミナルサービス業者

B. syslog監視
C. クライアントプロービング
D. GlobalProtect
正解: **D** (コメントを発表する)

質問: **41**
パケットフロープロセス中、アプリケーション識別で実行されるプロセスは2つありますか。 2つ選んでください。）
A. コンテンツ検査からアプリケーションが変更されました
B. パターンベースのアプリケーション識別
C. セッションアプリケーションが識別されました。
D. アプリケーションオーバーライドポリシーの一致
正解: (正解を表示します)

質問: **42**
管理プレーン上のCPU使用率を減らすのはどの3つのステップですか。 3つ選んでください。）
A. 定義済みレポートを無効にします。
B. セキュリティポリシーのセッション開始時のログ記録を無効にします。
C. SSLアプリケーションのアプリケーションオーバーライド
D. ファイアウォールによって復号化されるトラフィックを減らします。
E. 管理インターフェースのSNMPを無効にします。
正解: (正解を表示します)

質問: **43**
管理者はトラフィックログでunknown-tcpとして識別されるいくつかのインバウンドセッションを見ます。管理者は、これらのセッションが会社の独自の会計アプリケーションにアクセスする外部ユーザーのフォームであると判断します。管理者はこのトラフィックをアカウンティングアプリケーションとして確実に識別し、このトラフィックの脅威をスキャンしたいと考えています。
どの選択肢がこの結果を達成するでしょうか？
A. カスタムのApp-IDを作成して、[順序付き条件]チェックボックスを使用します。
B. カスタムApp-IDを作成し、詳細設定タブでスキャンを有効にします。
C. Application Overrideポリシーを作成します。
D. アプリケーションのApplication Overrideポリシーとカスタム脅威シグネチャを作成します。
正解: (正解を表示します)

質問: **44**
PAN-OS®ソフトウェアにすべての非ネイティブMFAプラットフォームを統合するために管理者はどの方法を使用しますか？
A. PingID
B. オクタ
C. RADIUS
D. DUO

正解: **C** (コメントを発表する)

質問: **45**
グローバル本社には、User-IDエージェントが1つだけの大規模ネットワークがあり、User-IDエージェントサーバーの近くにボトルネックが生じます。
この場合、PAN-OS®ソフトウェアのどのソリューションが役立ちますか？
A. アプリケーションの上書き
B. 仮想ワイヤモード
C. コンテンツ検査
D. ユーザーマッピングの再配布
正解: (正解を表示します)
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/user-id/deploy-user-id-in-大規模ネットワーク

質問: **46**
図の時間内にトラフィックの入力インターフェイスが192.168.111.3から宛先10.46.41.113に送信されるethernet1 / 6の場合、出力インターフェイスは何になりますか。

```
Thu Jun  8 12:49:55  PDT  2017
#######################
admin@Lab33-111-PA-3060(active)# show  vsys  vsys1  rulebase  pbf  rules  test-pbf
test-pbf   {
  action   {
    forward  {
       egress-interface  enthernet1/5;
    }
  }
  from  {
    zone  L3-Trust;
  }
  enforce-symmetric-return  {
     enabled  no;
     }
   source  192.168. 11. 3;
   destination  10.46.41.113;
   source-user  any;
   application   any;
   service  any;
   schedule  schedule-pbf ;
}
#######################
admin@Lab33-111-PA-3060(active) #  show vsys  vsys1  schedule  schedule-pbf
schedule-pbf   {
   schedule-type  {
      recurring  {
         daily  16:00-21:00;
      }
   }
}
#######################
admin@Lab33-111-PA-3060(active)>  show  routing fib

id          destination                    nexthop                flags       interface
mtu
--------------------------------------------------------------------------------------------

47          0 .0 .0. 0/0                   10. 46. 40. 1          ug          enthernet1/3
1500
67          10. 10. 20. 0/24               0. 0. 0. 0             u            enthernet1/7
1500
66          10. 10. 20. 111/32             0. 0. 0. 0             uh          enthernet1/7
1500
46          10. 46. 40. 0/23               0. 0. 0. 0             u            enthernet1/3
1500
49          10. 46. 44. 0/23               0. 0. 0. 0             u            enthernet1/5
1500
45          10. 46. 41. 111/32             0. 0. 0. 0             uh          enthernet1/3
1500
70          10. 46. 41. 113/32             10. 46. 40. 1          ug          enthernet1/3
1500
48          10. 46. 41. 111/32             0. 0. 0. 0             uh          enthernet1/5
1500
51          192. 168. 111. 0/24            0. 0. 0. 0             u            enthernet1/6
1500
50          192. 168. 111. 2/32            0. 0. 0. 0             uh          enthernet1/6
1500
--------------------------------------------------------------------------------------------
```

A. イーサネット1/5
B. イーサネット1/7
C. イーサネット1/6
D. イーサネット1/3
正解: **(**正解を表示します**)**

質問: **47**
グローバル本社には、User-IDエージェントが1つだけの大規模ネットワークがあり、User-IDエージェントサーバーの近くにボトルネックが生じます。この場合、PAN-OS®ソフトウェアのどのソリューションが役立ちますか？
A. 仮想ワイヤモード
B. アプリケーションの上書き
C. ユーザーマッピングの再配布
D. コンテンツ検査
正解: **(**正解を表示します**)**

質問: **48**
管理者はどのようにPalo Alto Networks NGFWの管理インターフェース上のトラフィックを監視/捕獲するのでしょうか？
A. debug dataplane packet-diag set capture stage firewall fileコマンドを使用します。
B. 4段階のトラフィックキャプチャ（TX、RX、DROP、ファイアウォール）をすべて有効にします。
C. debug dataplane packet-diag setキャプチャステージ管理ファイルコマンドを使用します。
D. tcpdumpコマンドを使用してください。
正解: **(**正解を表示します**)**
説明/参照：
参照：https://live.paloaltonetworks.com/t5/Learning-Articles/How-to-Run-a-Packet-Capture/tap / 62390

質問: **49**
どのPalo Alto Networks VMシリーズファイアウォールが有効ですか？
A. VM-25
B. VM-800
C. VM-50
D. VM-400
正解: **(**正解を表示します**)**
説明/参照：

参照 :https ://www.paloaltonetworks.com/products/secure-the-network/virtualized-next-generation- firewall / vm-series

質問: **50**
速度/デュプレックスネゴシエーションの不一致は、Palo Alto Networks管理ポートとそれが接続するスイッチポートの間にあります。
管理者はどのように1Gbpsにインターフェースを設定しますか？
A. deviceconfigインターフェイスの速度 - デュプレックス1 Gbps - 全二重に設定
B. deviceconfigシステムの速度 - 二重化1Gbps - 二重化を設定します。
C. deviceconfigシステムの速度 - 二重化1Gbps - 全二重に設定
D. set deviceconfigインターフェイス速度 - デュプレックス1 Gbps - 半二重
正解: **(**正解を表示します**)**
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Configuration-Articles/How-to-Change-the-Speed-and-二重管理ポート/ ta-p / 59034

質問: **51**
管理者は、DMZとコアネットワーク間にNGFWを実装する必要があります。2つの環境間のEIGRPルーティングが必要です。このビジネス要件をサポートするのはどのインタフェースタイプですか？
A. レイヤ3インターフェイス、ただし接続仮想ルータでEIGRPを設定
B. コアとDMZの間でEIGRPルーティングを維持するためのVirtual Wireインタフェース
C. IPsecトンネルでEIGRPルーティングを終了するためのトンネルインターフェイス（SVPNおよびEIGRPプロトコルをサポートするためのGlobalProtectライセンス付き）
D. レイヤ3または集約イーサネットインターフェイス、ただしサブインターフェイス上でのみEIGRPを設定
正解: **(**正解を表示します**)**

質問: **52**
管理者はどのCLIコマンドを使用して、稼働時間、PANOS®バージョン、シリアル番号など、ファイアウォールに関する詳細を表示できますか？
A. デバッグシステムの詳細
B. セッション情報を表示
C. システム情報を表示
D. システムの詳細を表示
正解: **C (**コメントを発表する**)**
説明/参照：
参照 :https://live.paloaltonetworks.com/t5/Learning-Articles/Quick-Reference-Guide-Helpful- Commands / ta-p / 56511

質問: **53**
MFA認証をサポートするにはどのキャプティブポータルモードを設定する必要がありますか？
A. NTLM
B. リダイレクト
C. シングルサインオン

D. 透明
正解: **B** (コメントを発表する)
説明/参照：
参照 :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/authentication/configure-多要素認証

質問: **54**
パケットフロープロセスでコンテンツ検査はいつ実行されますか。
A. アプリケーションが識別された後
B. セッションルックアップ前
C. パケット転送処理前
D. SSLプロキシがパケットを再暗号化した後
正解: **A** (コメントを発表する)
説明/参照：
参照：
https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

質問: **55**
管理者には、復号化されたトラフィックをPalo Alto Networks NGFWからサードパーティのディープレベルパケットインスペクションアプライアンスにエクスポートするという要件があります。
要件を満たすために必要なインターフェイスの種類とライセンス機能はどれですか。
A. Threat Analysisライセンスを使用した復号化ミラーインタフェース
B. 復号化ポートエクスポートライセンスを持つVirtual Wireインタフェース
C. 復号化ポートミラーライセンスのあるタップインターフェース
D. 関連付けられている復号化ポートミラーライセンスを持つ復号化ミラーインターフェイス
正解: **D** (コメントを発表する)
説明/参照：
参照先 :https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/decryption/decryption- concepts /復号化ミラーリング

質問: **56**
展示を参照してください。DMZ内のWebサーバーは、DNATを介してパブリックアドレスにマップされています。

どのセキュリティポリシールールでトラフィックがWebサーバーに流れることを許可しますか。

A. Untrust（any）からUntrust（10.1.1.100）、Web参照 - 許可する

B. DMZ（10. 1. 1. 100）への信頼性がない（any）、ウェブ閲覧 - 許可

C. Untrust（any）からUntrust（1. 1. 1. 100）、Webブラウズ - 許可

D. DMZ（1. 1. 1. 100）への信頼性がない（すべて）、Web参照 - 許可

正解: **C** (コメントを発表する)

質問: **57**

特定の宛先IPアドレスに到達可能かどうかは、どの仮想ルータ機能が判断しますか。

A. ハートビート監視

B. フェイルオーバ

C. パス監視

D. Ping-Path

正解: **C** (コメントを発表する)

説明/参照：

参照先：https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/policy/policy-based- forwarding / pbf / path-monitoring-for-pbf

質問: **58**

次の図に表示されている証明書情報は、どの種類の証明書ですか？

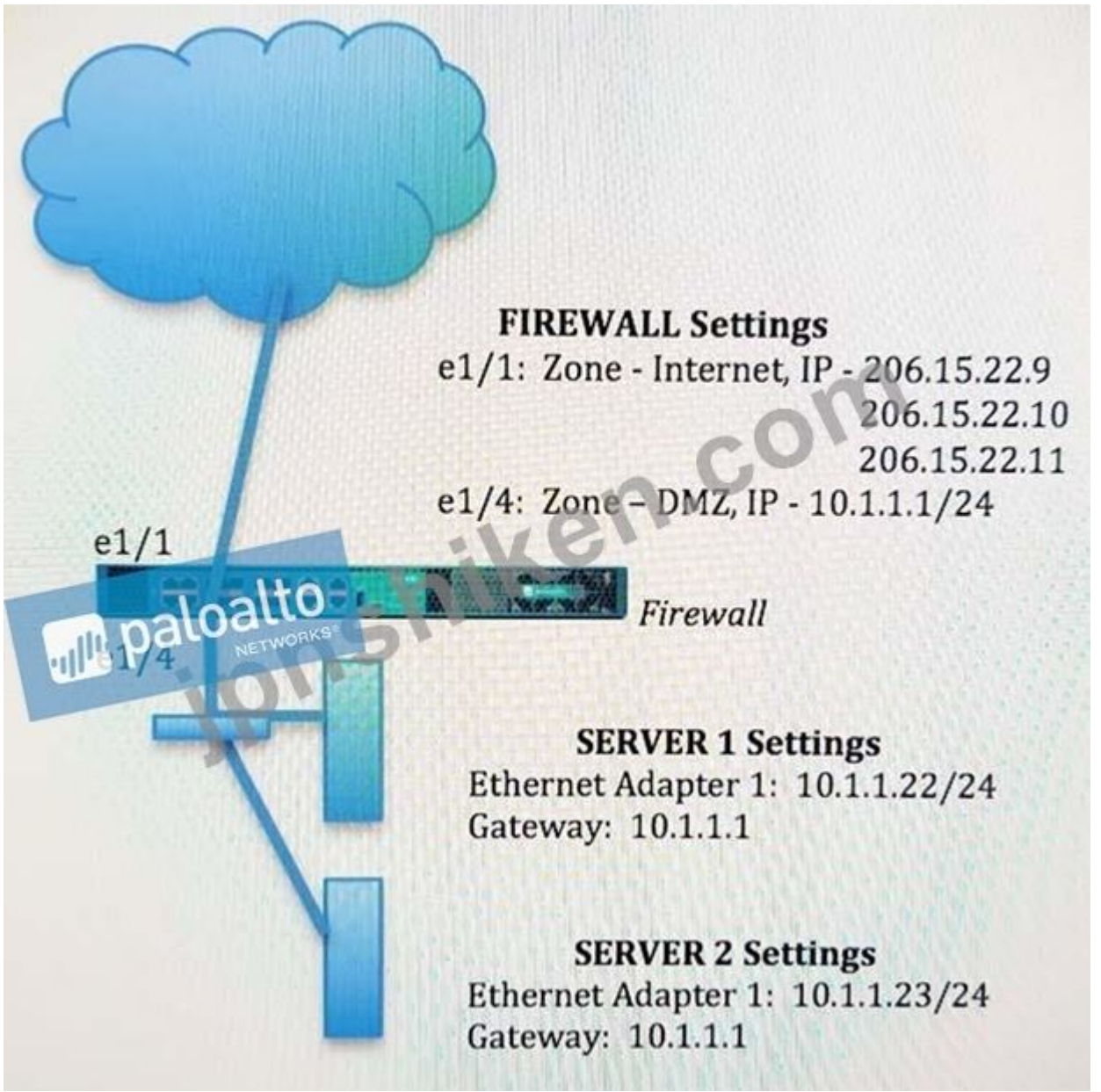
A. 公開CAの署名付き証明書
B. フォワードトラスト証明書
C. 自己署名ルートCA証明書
D. Webサーバ証明書
正解: **(**正解を表示します**)**

質問: **59**
ファイアウォールは、一般的なアプリケーションを不明なTCPとして識別します。
アプリケーションを識別するために利用可能な2つのオプションはどれですか？ （2つ選んでください。）
A. カスタムアプリケーションを作成します。
B. カスタムアプリケーションを識別するためのカスタムアプリケーションサーバー用のカスタムオブジェクトを作成します。
C. Palo Alto NetworksにApple-IDリクエストを送信してください。
D. カスタムアプリケーションを識別するためのセキュリティポリシーを作成します。
正解: **(**正解を表示します**)**
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/app-id/use-application-ポリシー内のオブジェクト/カスタムアプリケーションの作成

質問: **60**
Panorama管理者が 先祖で定義されたオブジェクトが優先される」という設定を選択した場合、どの処理順序が有効になりますか？
A. 子孫オブジェクトは他の子孫オブジェクトよりも優先されます。
B. 子孫オブジェクトは先祖オブジェクトよりも優先されます。
C. 祖先オブジェクトは子孫オブジェクトよりも優先されます。
D. 祖先オブジェクトは他の祖先オブジェクトよりも優先されます。
正解: **(**正解を表示します**)**
説明/参照：
参照 :https ://www.paloaltonetworks.com/documentation/80/pan-os/web-interface-help/device/device-device-setup-management

質問: **61**
WebサーバーはDMZでホストされており、サーバーはTCPポート8080でのみ着信接続を待機するように構成されています。Trustゾーンから DMZゾーンへのアクセスを許可するセキュリティポリシールールを設定する必要があります。サーバ。
tcp / 8080でこのサーバーへのクリアテキストのWeb閲覧トラフィックのみを許可するように設定する必要があるアプリケーションとサービス。
A. アプリケーション :Web閲覧。サービス：（宛先TCPポート8080のカスタム）
B. application :ssl;サービス：任意
C. アプリケーション :Web閲覧。service :service-https
D. アプリケーション :Web閲覧service :application-default
正解: **(**正解を表示します**)**

質問: **62**
管理者は、インターネットから開始された接続をDMZ内の複数のWebサーバーに受信させたいと考えています。
206.15.22.9ポート80 / TCP宛てのトラフィックは、10.1.1.22のサーバに転送する必要があります。イメージに示されている情報に基づいて、どのNATルールでWebブラウジングトラフィックが正しく転送されますか。

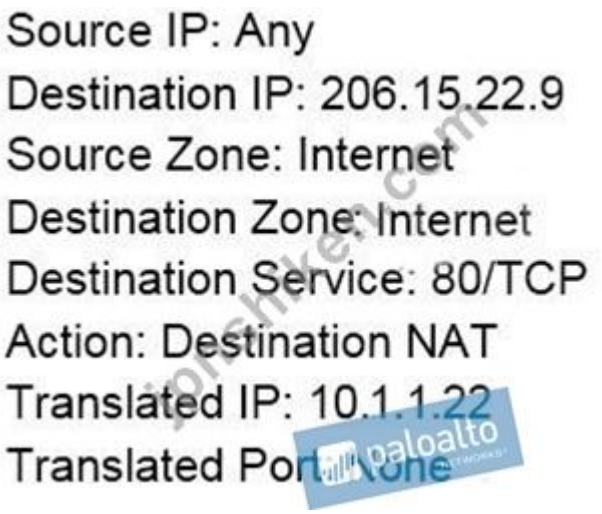


A :

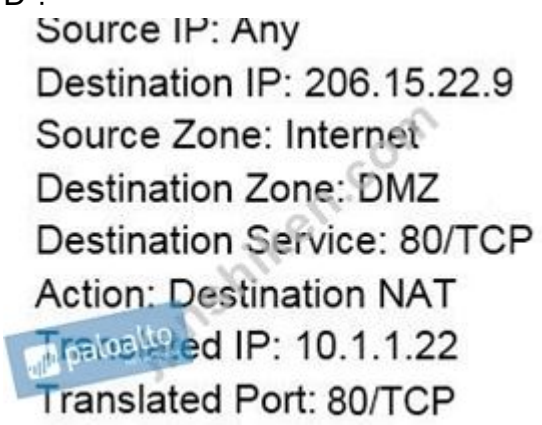
Source IP: Any
Destination IP: 206.15.22.9
Source Zone: Internet
Destination Zone: DMZ
Destination Service: 80/TCP
Action: Destination NAT
Translated IP: 10.2.2.23
Translated Port: 53/UDP

B :

子：



D：



A. オプションC
B. オプションB
C. オプションA
D. オプションD
正解: **A** (コメントを発表する)

質問: **63**
ターミナルサーバーを介して接続されているユーザーのIPアドレスをユーザー名にマッピングするには、どのユーザーID方法を構成する必要がありますか。

A. ポートマッピング
B. サーバ監視
C. クライアントプローブ
D. XFFヘッダ
正解: **(**正解を表示します**)**
説明/参照：
参照：https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os/user-id/configure-user- terminal-server-usersのマッピング

質問: **64**
管理者がすべての管理サービスにデフォルトのポートを使用するためにファイアウォールを離れました。データプレーンによって実行される3つの機能はどれですか。 3つ選んでください。）
A. WildFireのアップデート
B. NTP
C. ファイルブロック
D. NAT
E. ウイルス対策
正解: **(**正解を表示します**)**