NAT(6)

1 NAT overload の性質について正しい説明はどれですか？

A.内部IPアドレスに1対多の関係を適用します

B.内部IPアドレスに1対1の関係を適用します

C.内部IPアドレスに多対多の関係を適用する

D.ギガビットインターフェイスでのみ構成できます

2 展示を参照してください。エンジニアがNAT変換を構成し、構成が正しいことを確認しました。NATが実行された後の送信元IPはどのIPアドレスですか？

```
R1#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp  172.23.104.3:43268  10.4.4.4:43268   172.23.103.10:23   172.23.103.10:23
tcp  172.23.104.4:45507  10.4.4.5:45507   172.23.103.10:80   172.23.103.10:80
```

A. 10.4.4.4

B. 10.4.4.5

C. 172.23.103.10

D. 172.23.104.4

3 NAT構成のどのキーワードが、複数の内部ホストに1つの外部IPアドレスを使用できるようにしますか？

A. source

B. static

C. pool

D. overload

4 NATデバイスのパブリックIPアドレスはどのタイプのアドレスですか？

A. outside global

B. outside local

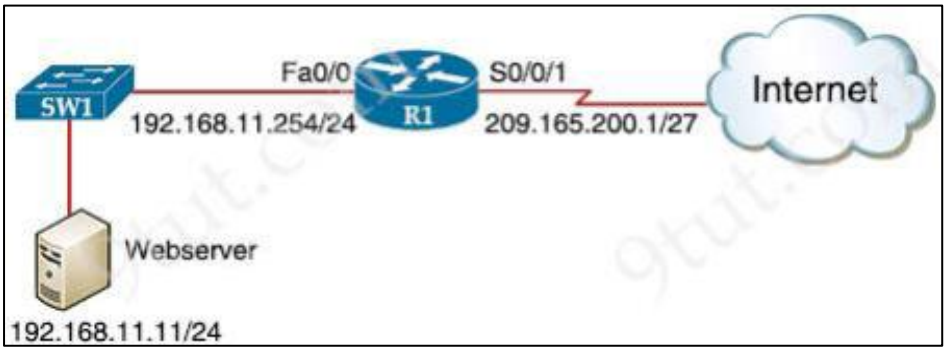
C. inside global

D. inside local

E. outside public

F. inside public

5 展示を参照してください。ルータR1はスタティックNATで設定されています。ルーターとWebサーバーのアドレス指定は正しく構成されていますが、Webサーバーとインターネット上のユーザーの間に接続がありません。この接続性の欠如の考えられる理由は何ですか？




```
R1(config)# ip nat inside source static 192.168.11.254 209.165.200.1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip nat inside
R1(config-if)#interface Serial0/0/1
R1(config-if)#ip nat outside
```

A.ルーターのNAT構成に誤った内部ローカルアドレスがあります
B.内部グローバルアドレスが正しくない
C.インターフェイスS0/0/1のNAT設定が正しくありません。
D.インターフェイスFa0/0は、コマンドip nat outsideで設定する必要があります。

6 エンジニアは、10.10.0.0/24 の送信元サブネットを192.168.3.1、192.168.3.2、192.168.3.3の3つのアドレスのいずれかに変換するようにNATを構成しています。どの構成を使用する必要がありますか？

Option A:	**Option B:**	**Option C:**
enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 route-map permit 10.10.0.0 255.255.255.0 ip nat outside destination list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside	enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 access-list 1 permit 10.10.0.0 0.0.0.255 ip nat outside destination list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside	enable configure terminal ip nat pool mypool 192.168.3.1 192.168.3.3 prefix-length 30 access-list 1 permit 10.10.0.0 0.0.0.255 ip nat inside source list 1 pool mypool interface g1/1 ip nat inside interface g1/2 ip nat outside

A.オプションA
B.オプションB
C.オプションC

NTP (3)

1 デバイスをNTPサーバーとして構成するには、どのコマンドを入力する必要がありますか？

A. ntp server

B. ntp peer

C. ntp authenticate

D. ntp master

2 show ntp statusコマンドの出力から判断できる情報はどれですか。 （2つ選択してください）

A.NTPピアが静的に構成されているかどうか

B.クロックが同期されているピアのIPアドレス

C.構成されたNTPサーバー

D.クロックが同期されているかどうか

E.ピアのNTPバージョン番号

3 単一のネットワークデバイスでクライアントモードの信頼できるサーバーにNTPを構成するには、どの2つのタスクを実行する必要がありますか？ （2つ選択してください）

A.NTP認証を有効にする

B.タイムゾーンを確認します

C.NTPブロードキャストを無効にする

D.NTPサーバーのIPアドレスを指定します

E.NTPサーバーの秘密鍵を設定します

Syslog (3)

1 ルータでlogging trap debugコマンドを設定するとどうなりますか？

A.これにより、ルーターは重大度レベルの低いメッセージをsyslogサーバーに送信します。

B.ルーターは、重大度レベルが警告、エラー、重大、および緊急のすべてのメッセージをsyslogサーバーに送信します。

C.ルーターがすべてのメッセージをsyslogサーバーに送信するようにします

D.ルーターがsyslogサーバーへのすべてのメッセージの送信を停止する原因になります

2 通知レベルのメッセージングがsyslogサーバーに送信された場合、どのイベントが発生しましたか？

A.ネットワークデバイスが再起動しました

B.ARP検査が失敗しました

C.ルーティングインスタンスがフラップしました

D.デバッグ操作が実行されています

3 ルーターが通知レベルのメッセージをsyslogサーバーに送信した場合、どのようなイベントが発生しましたか？

A.TCP接続が切断されました

B.ICMP接続が構築されました

C.インターフェイスラインのステータスが変更されました

D.証明書の有効期限が切れています

HSRP (7)

1 優先度の高いHSRPルータがリロード後にHSRPプライマリルータになることを保証するには、どのコマンドを入力する必要がありますか。

A. standby 10 preempt
B. standby 10 version 1
C. standby 10 priority 150
D. standby 10 version 2

2 HSRPグループ内のルータの優先度を確認するには、どのコマンドを入力する必要がありますか。

A. show hsrp
B. show sessions
C. show interfaces
D. show standby

3 どのMACアドレスがVRRP仮想アドレスとして認識されますか？

A. 0000.5E00.010a
B. 0005.3711.0975
C. 0000.0C07.AC99
D. 0007.C070.AB01

4 HSRPの予測可能な動作はどれですか。 （2つ選択してください）

A. 2つのルーターは、LAN上のデバイスのデフォルトゲートウェイとして使用される仮想IPアドレスを共有します
B. 2つのルーターは、一方のルーターをアクティブルーターとして、もう一方のルーターをスタンバイルーターとしてネゴシエートします。
C. 各ルーターには異なるIPアドレスがあり、両方のルーターがLANのデフォルトゲートウェイとして機能し、トラフィックはルーター間で負荷分散されます。
D. 2つのルーターは構成を同期して、一貫したパケット転送を提供します。
E. ルーティングされた2つのルーターは同じIPアドレスを共有し、デフォルトゲートウェイトラフィックはそれらの間で負荷分散されます。

5 HSRPはどのようにファーストホップ冗長性を提供しますか？

A. IPルーティングテーブルの同じ宛先への複数のルートに同じメトリック値を割り当てることにより、トラフィックの負荷を分散します

B.同じVLANで設定されたすべてのインターフェイスからトラフィックをフラッディングすることにより、パスに沿ってレイヤ2トラフィックのロードバランシングを行います。

C.異なるルーテッドリンクとデータパスを介して複数のパケットを同じ宛先に転送します

D.LAN上のホストのデフォルトゲートウェイとして機能するルーターのグループへの共有仮想MACと仮想IPアドレスを使用します

6 ファーストホップ冗長プロトコルの主な目的は何ですか？

A.直接接続されたネイバーが設定情報を共有できるようにします

B.これにより、ルーターはブリッジの優先順位を使用して、単一の宛先への複数のループのないパスを作成できます。

C.同じリンクメトリックを持つOSPFネイバー間のレイヤ3ロードバランシングを許可することにより、ルーティングエラーを削減します

D.ネットワークのデフォルトゲートウェイとして、複数のルーターがそれ自体を表すことを許可することにより、ルーティングの失敗を減らします

7 HSRPグループ内のアクティブルータに障害が発生した場合、どのルータがその役割を引き受け、パケットを転送しますか。

A. listening

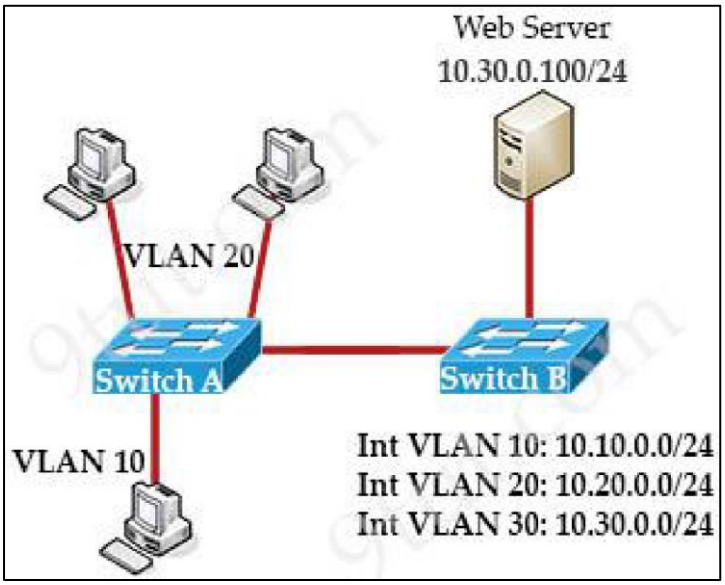
B. backup

C. forwarding

D. standby

ACL (7)

1 展示を参照してください。ネットワークエンジニアは、WebサーバーへのHTTPを介したVLAN20上のすべてのコンピューターのアクセスをブロックする必要があります。他のすべてのコンピューターは、Webサーバーにアクセスできる必要があります。スイッチAに適用するとき、どの構成がこのタスクを実行しますか？



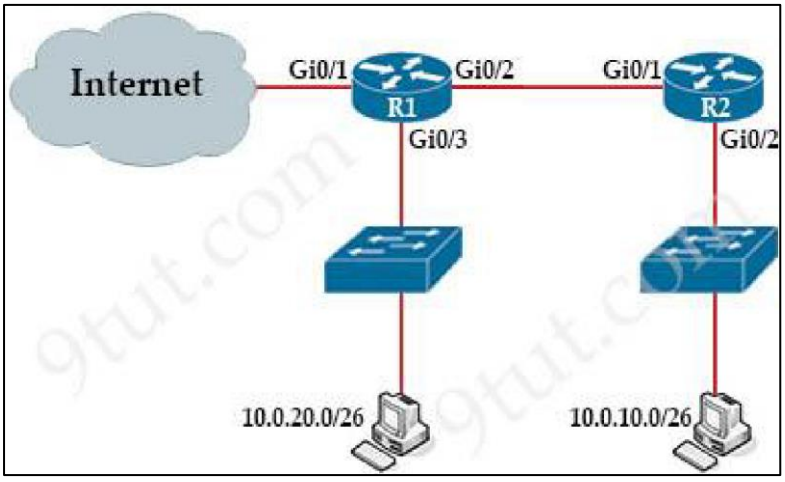
A.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 100
ip access-group wwwblock in
```

B.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
permit ip any any
int vlan 20
ip access-group wwwblock in
```

C.
```
config t
ip access-list extended wwwblock
permit ip any any
deny tcp any host 10.30.0.100 eq 80
int vlan 30
ip access-group wwwblock in
```

D.
```
config t
ip access-list extended wwwblock
deny tcp any host 10.30.0.100 eq 80
int vlan 20
ip access-group wwwblock in
```

2 展示を参照してください。 拡張ACLが設定され、ルータR2に適用されました。 構成が意図したとおりに機能しませんでした。 他のすべてのトラフィックを許可しながら、TCPポート25および80のアウトバウンドトラフィックを10.0.10.0/26サブネットから10.0.20.0/26に停止する2つの変更はどれですか。 （2つ選択してください）



```
R2#config t
R2(config)#access-list 101 deny tcp 10.0.20.0 0.0.0.63 10.0.10.0 0.0.0.63 eq smtp
R2(config)#access-list 101 deny tcp 10.0.20.0 0.0.0.63 10.0.10.0 0.0.0.63 eq www
R2(config)#int gi0/2
R2(config-if)#ip access-group 101 in
```

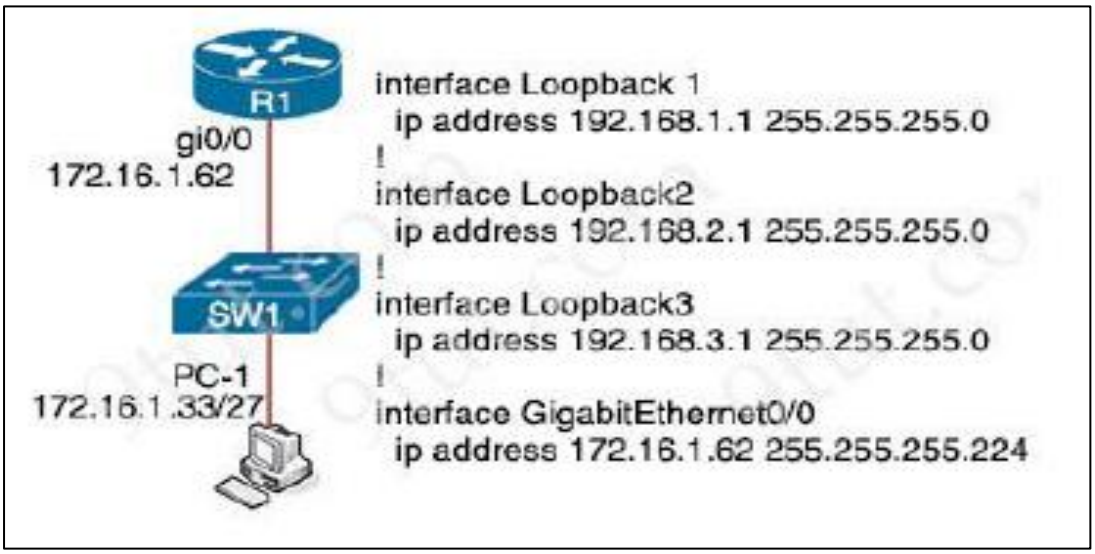
A.許可されたトラフィックのACL101の先頭に「permit ip any any」ステートメントを追加します
B.許可されたトラフィックのACL101の最後に「permit ip any any」ステートメントを追加します
C.送信元IPと宛先IPはACL101で交換する必要があります
D.ACLはR1でインバウンドのGi0 / 2インターフェイスを設定する必要がありますE.ACLはR2でアウトバウンドのGi0 / 1インターフェイスに移動する必要があります

3

ネットワーク上の過剰なトラフィックを調べている間、IPv4 ACLがインターフェイスに適用されていても、インターフェイス上のすべての着信パケットが許可されているように見えるということが知られています。この動作の原因となる2つの設定ミスはどれですか？ （2つ選択してください）

A.パケットが許可ステートメントと一致しません
B.一致する許可ステートメントがアクセスリストで高すぎます
C.一致する許可ステートメントが広範に定義されている
D.ACLが空です
E.一致する拒否ステートメントがアクセスリストで高すぎます

4 展示を参照してください。 R1のどの構成がPC-1から任意のR1インターフェイスへのSSHアクセスを拒否し、他のすべてのトラフィックを許可しますか？



A. access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any
interface GigabitEthernet0/0
ip access-group 100 in

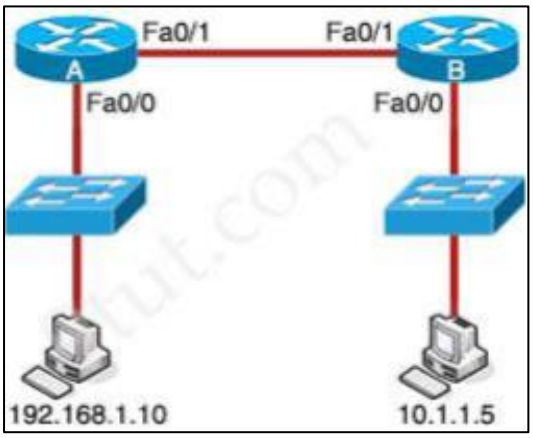
B. access-list 100 deny tcp host 172.16.1.33 any eq 22
access-list 100 permit ip any any

C. line vty 0 15
access-class 100 in
access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any

interface GigabitEthernet0/0
ip access-group 100 in

D. access-list 100 deny tcp host 172.16.1.33 any eq 23
access-list 100 permit ip any any
line vty 0 15
access-class 100 in

5 展示を参照してください。管理者は、192.168.1.0サブネット上のデバイスが10.1.1.5のサーバーにアクセスできないようにするために、次のACLを構成します。

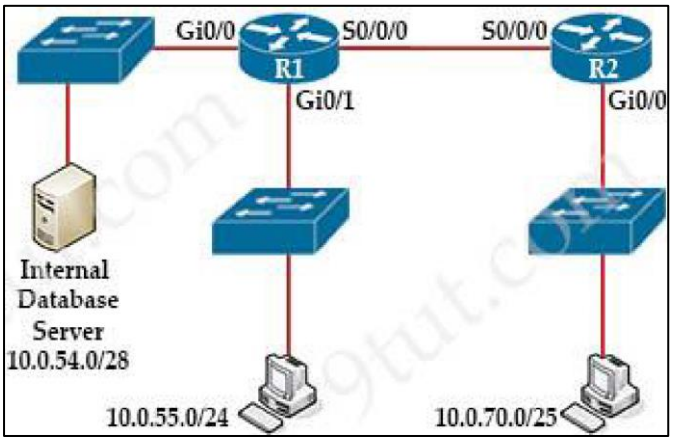



```
access-list 100 deny ip 192.168.1.0 0.0.0.255 host 10.1.1.5
access-list 100 permit ip any any
```

ネットワークリソースを最も効率的に使用するために、管理者はこのACLをどこに配置する必要がありますか？

A.ルータAでのインバウンドFa0/0
B.ルーターBでのアウトバウンドFa0/0
C.ルーターAFa0/1でのアウトバウンド
D.ルーターBのインバウンドFa0/1

6 展示を参照してください。 10.0.70.0/25ネットワークデバイスのみが内部データベースサーバーにアクセスできるように、R1で標準アクセスリストを作成して適用するために使用される2つの構成はどれですか。 （2つ選択してください）



A. R1（config）#interface GigabitEthernet 0/0
R1（config-if）#ip access-group 5 out
B. R1（config）#access-list 5 permit 10.0.54.0 0.0.1.255
C. R1（config）#interface Serial 0/0/0
R1（config-if）#ip access-group 5 in
D. R1（config）#access-list 5 permit 10.0.70.0 0.0.0.127
E. R1（config）#access-list 5 permit any

7 展示を参照してください。

```
interface GigabitEthernet0/1
ip address 192.168.1.2 255.255.255.0
ip access-group 2699 in
!
access-list 2699 deny icmp any 10.10.1.0 0.0.0.255 echo
access-list 2699 deny ip any 10.20.1.0 0.0.0.255
access-list 2699 permit ip any 10.10.1.0 0.0.0.255
access-list 2699 permit tcp any 10.20.1.0 0.0.0.127 eq 22
```

ネットワーク管理者は、ネットワーク内のルーターをリモート管理するためにSSHアクセスを許可する必要があります。運用チームは10.20.1.0/25ネットワーク上にあります。どのコマンドがこのタスクを実行しますか？

A. access-list 2699 permit udp 10.20.1.0 0.0.0.255
B. no access-list 2699 deny tcp any 10.20.1.0 0.0.0.127 eq 22
C. access-list 2699 permit tcp any 10.20.1.0 0.0.0.255 eq 22
D. no access-list 2699 deny ip any 10.20.1.0 0.0.0.255

AAA (6)

1 AAAは、認証、許可、およびアカウンティングの略です。

A.誤り

B.本当

2 aaa new-model コンフィギュレーションコマンドにはどのような影響がありますか？

A.AAA用のRADIUSサーバーに接続するようにデバイスを構成します。

B.デバイスのローカルユーザーを構成します。

C.AAAグループのRADIUSサーバーに関連付けられます。

D.デバイスでAAAサービスを有効にします。

3 AAA認証と認可の主な違いは何ですか？

A.認証はユーザー名とパスワードを検証し、認可は認証エージェントとユーザーデータベース間の通信を処理します

B.認証はシステムにアクセスしようとしているユーザーを識別し、認可はユーザーのパスワードを検証します

C.認証はシステムにアクセスしようとしているユーザーを識別および検証し、認可はユーザーが実行できるタスクを制御します

D.認証はユーザーがアクセスできるシステムプロセスと、ユーザーが開始するアクティビティの承認ログを制御します

4 展示を参照してください。エンジニアがイネーブルモードに入るには、どのパスワードを使用する必要がありますか？

```
Atlanta#config t
Atlanta(config)#aaa new-model
Atlanta(config)#aaa authentication login default local
Atlanta(config)#line vty 0 4
Atlanta(config-line)#login authentication default
Atlanta(config-line)#exit
Atlanta(config)#username ciscoadmin password adminadmin123
Atlanta(config)#username ciscoadmin privilege 15
Atlanta(config)#enable password cisco123
Atlanta(config)#enable secret testing1234
Atlanta(config)#end
```

A. adminadmin123

B. default

C. testing1234

D. cisco123

5 RADIUSとTACACS +の違いは何ですか？

A. RADIUSはダイヤル認証に最適ですが、TACACS +は複数のタイプの認証に使用できます

B. TACACS +はパスワード情報のみを暗号化し、RADIUSはペイロード全体を暗号化します

C. TACACS +は認証と承認を分離し、RADIUSはそれらをマージします

D. RADIUSは、管理者が入力したすべてのコマンドをログに記録しますが、TACACS +は、開始、停止、および中間コマンドのみをログに記録します。

6 AAA操作は、ユーザID、ユーザサービス、およびアクセス制御に関してどのように比較されますか？

A.承認はアクセス制御を提供し、認証はユーザーサービスを追跡します

B.認証はユーザーを識別し、アカウンティングはユーザーサービスを追跡します

C.アカウンティングはユーザーサービスを追跡し、認証はアクセス制御を提供します

D.承認はユーザーを識別し、認証はアクセス制御を提供します

Secu (11)

1 電子メールユーザーは、自社のセキュリティ組織から送信された電子メールのリンクをクリックするように誘惑されました。開いたWebページは、安全であると報告していますが、リンクに悪意のあるコードが含まれている可能性があります。 どのタイプのセキュリティプログラムが実施されていますか？

A.物理的なアクセス制御
B.ソーシャルエンジニアリング攻撃
C.ブルートフォース攻撃
D.ユーザーの意識

2 エンジニアは、スイッチのデフォルトVLANに設定されている未使用のポートを保護するように求められます。リクエストを満たす2つのステップはどれですか？ （2つ選択してください）

A.EtherChannelでポートを構成します
B.ポートを管理上シャットダウンする
C.ポートタイプをアクセスとして設定し、VLAN99に配置します
D.ポートをトランクポートとして設定します
E.Cisco Discovery Protocol を有効にします

3 ルーターでSSHのRSAキーを生成するには、どの構成が必要ですか？

A.SSHのバージョンを構成します
B.VTYアクセスを構成する
C.パスワードを使用してユーザーを作成する
D.DNSドメイン名を割り当てます

4 SSHがCiscoIOSスイッチで正常に動作するために満たす必要がある2つはどれですか。 （2つ選択してください）

A.スイッチはk9（crypto）IOSイメージを実行している必要があります
B. ip domain-name コマンドをスイッチで設定する必要があります
C.スイッチでIPルーティングを有効にする必要があります
D.コンソールパスワードをスイッチで設定する必要があります
E.スイッチでTelnetを無効にする必要があります

5 サイト間VPNを使用する場合、ユーザーデータの転送を担当するプロトコルはどれですか。

A. IKEv2
B. IKEv1
C.IPsec
D. MD5

6 多要素認証の要件を満たすアクションのセットはどれですか？

A.ユーザーがキーフォブをスワイプしてから、メールリンクをクリックします

B.ユーザーはユーザー名とパスワードを入力し、モバイルデバイスの認証アプリで通知をクリックします

C.ユーザーはRSAトークンにPINを入力し、ログイン画面に表示されたRSAキーを入力します

D.ユーザーはユーザー名とパスワードを入力し、2番目の画面で資格情報を再入力します

7 パスワードがルーターまたはスイッチのプレーンテキストとして構成に保存されないようにするコマンドはどれですか。

A. enable secret

B. service password-encryption

C. username Cisco password encrypt

D. enable password

8 展示を参照してください。管理者は、暗号化ハッシュに格納されているパスワードを使用して、ローカル認証用に4つのスイッチを構成します。 4つのスイッチは、管理者がネットワークインフラストラクチャを管理するためのSSHアクセスもサポートする必要があります。これらの要件を満たすように正しく構成されているスイッチはどれですか？

```
SW1(config-line) #line vty 0 15
SW1(config-line) #no login local
SW1(config-line) #password cisco

SW2(config) #username admin1 password abcd1234
SW2(config) #username admin2 password abcd1234
SW2(config-line) #line vty 0 15
SW2(config-line) #login local

SW3(config) #username admin1 secret abcd1234
SW3(config) #username admin2 secret abcd1234
SW3(config-line) #line vty 0 15
SW3(config-line) #login local

SW4(config) #username admin1 secret abcd1234
SW4(config) #username admin2 secret abcd1234
SW4(config-line) #line console 0
SW4(config-line) #login local
```

A. SW1
B. SW2
C. SW3
D. SW4

9 service password-encryption コマンドがルータで入力されました。この構成の効果は何ですか？
A.許可されていないユーザーが実行コンフィギュレーションでクリアテキストパスワードを表示することを制限します
B.ネットワーク管理者がクリアテキストのパスワードを設定できないようにする
C.スイッチ上の不正なPC接続からVLANデータベースを保護します
D.VPNトンネルが確立されたときにパスワード交換を暗号化する

10 パスワードマネージャーが、ハッカーがユーザーのパスワードを盗む可能性を減らす2つの方法はどれですか。（2つ選択してください）
A.元のユーザーには知られていない2番目の認証要素を自動的に提供します
B.内部ファイアウォールを使用して、パスワードリポジトリを不正アクセスから保護します
C.侵害されたデバイスまたはWebサイトでのキーストロークロギングから保護します
D.ウイルス対策およびマルウェア対策機能が組み込まれたローカルワークステーションにパスワードリポジトリを保存します
E.ユーザーがより強力なパスワードを作成するように促します

11 ネットワークに偵察攻撃を仕掛ける2つの目的は何ですか？（2つ選択してください）
A.他のユーザーがシステムにアクセスするのを防ぐため
B.アクセス権限をエスカレートするため
C.ネットワークとデバイスに関する情報を収集するため
D.アクセシビリティをスキャンするため
E.データを取得および変更するため

Secu(8)

1 展示を参照してください。エンジニアが新しいスイッチを起動し、コンソールポートを介してこの構成を適用しました。管理者がローカルユーザー名とパスワードを使用してTelnet経由で特権モードを有効にするために直接認証できるようにするには、どの追加構成を適用する必要がありますか？

```
Switch(config)#hostname R1
R1(config)#interface FastEthernet0/1
R1(config-if)#no switchport
R1(config-if)#ip address 10.100.20.42 255.255.255.0
R1(config-if)#line vty 0 4
R1(config-line)#login
```

A. R1(config)#username admin
R1(config-if)#line vty 0 4
R1(config-line)#password p@ss1234

B. R1(config)#username admin
R1(config-if)#line vty 0 4
R1(config-line)#password p@ss1234
R1(config-line)#transport input telnet

C. R1(config)#username admin secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local
R1(config)#enable secret p@ss1234

D. R1(config)#username admin privilege 15 secret p@ss1234
R1(config-if)#line vty 0 4
R1(config-line)#login local

2 組織は、従業員のスマートフォンの認証アプリを使用して、多要素認証でネットワークを保護します。ユーザーのスマートフォンを紛失したり盗まれたりした場合、アプリケーションはどのように保護されますか？

A.アプリケーションは、設定された間隔の後に再アクティブ化するために管理者パスワードを必要とします。

B.アプリケーションは、2番目の要素を提供する前に、ユーザーが特定の場所にいることを確認します。

C.アプリケーションでは、2番目の要素を提供する前にユーザーがPINを入力する必要があります。

D.アプリケーションは、スマートフォンの再起動時に管理者パスワードを再アクティブ化するように要求することにより、ユーザーにチャレンジします。

3 動的ARP検査によってどのタイプの攻撃を軽減できますか？

A.マルウェア

B. DDoS

C.ワーム

D.中間者

4 プロキシキャッシングによってWebトラフィックのパフォーマンスを向上させるために使用されているテクノロジーはどれですか？

A. Firepower

B. FireSIGHT

C. ASA

D. WSA

5 どのデバイスがトラフィックのステートフルインスペクションを実行しますか？

A.アクセスポイント

B.スイッチ

C.ワイヤレスコントローラー

D.ファイアウォール

6 ITクローゼットの外のオフィススペースにあるときにネットワークポートが悪用されないように保護するための2つの推奨事項は何ですか？（2つ選択してください）

A.未使用のポートをシャットダウンします

B.ポートでPortFast機能を有効にする

C.ポートベースの認証を実装する

D.ポートを固定速度に構成する

E.静的ARPエントリを設定する

7 VLANホッピング攻撃からネットワークを保護する方法は何ですか？

A.ネイティブVLANを未使用のVLANIDに変更します

B.動的ARP検査を有効にする

C.トラフィックがVLANを変更しないようにACLを構成します

D.インターネットに面したVLANにポートセキュリティを実装する

8 クライアントデバイスが状態を修正せずにネットワークに任意に接続するのを防ぐことができるテクノロジーはどれですか？

A.MAC認証バイパス

B.IPソースガード

C.802.1x

D.802.11n

DAI (2)

1 展示を参照してください。 この構成の効果は何ですか？

```
ip arp inspection vlan 2
interface fastethernet 0/1
switchport mode access
switchport access vlan 2
```

A.すべてのARPパケットはスイッチによってドロップされます
B.出力トラフィックは、宛先がDHCPサーバーである場合にのみ渡されます
C.インターフェイスが信頼されていないため、すべての入力トラフィックと出力トラフィックがドロップされます
D.スイッチは、無効なMAC-to-IPアドレスバインディングを持つすべての入力ARPトラフィックを破棄します

2 展示を参照してください。 この構成の効果は何ですか？

```
ip arp inspection vlan 2
interface fastethernet 0/1
switchport mode access
switchport access vlan 2
```

A.スイッチポートインターフェイスの信頼状態が信頼できない状態になります
B.インターフェイスが別のスイッチに接続されるまで、スイッチポートは管理上ダウンしたままです。
C. ARP ACLがないため、動的ARP検査が無効になっている
D.スイッチポートは、着信パケットを信頼または信頼解除するように設定されるまでダウンしたままです。