

KTest

更に上のクオリティ 更に上のサービス



問題集

<http://www.ktest.jp>

1年で無料進級することに提供する

Exam : **642-618**

Title : Deploying Cisco ASA
Firewall Solutions
(FIREWALL v2.0)

Version : DEMO

1. Cisco ASA の上、tcp マップはどの CLI コンフィギュレーションコマンド MPF を使用して、トラフィッククラスに適用することができますか？

- A. 検査する
- B. sysopt 接続する
- C. TCP-オプション
- D. パラメータ
- E. 接続高度なオプションを設定する

Answer: E

2. デフォルトでは、どのトラフィックが明示的に ACL を使用できるようにすることなく、透過モードで動作していなかったの Cisco ASA を通過することができますか？

- A. ARP
- B. BPDU
- C. CDP
- D. OSPF マルチキャスト
- E. DHCP

Answer: A

3. syslog サーバに syslog メッセージを送信するように Cisco ASA を有効にする場合、どのレベルの syslog は、ほとんどのメッセージが生成されますか？

- A. 通知
- B. 情報
- C. 頼む
- D. 緊急事態
- E. エラー
- F. デバッグング

Answer: F

4. 展示を参照してください。

```

ASA-5510# show conn
54764 in use, 54764 most used
TCP outside 172.16.1.118:26093 inside 10.1.1.50:80, idle 0:00:23, bytes 0, flags aB
TCP outside 172.16.5.19:23598 inside 10.1.1.50:80, idle 0:00:13, bytes 0, flags aB
TCP outside 192.168.1.202:32729 inside 10.1.1.50:80, idle 0:00:25, bytes 0, flags aB
TCP outside 192.168.2.20:56481 inside 10.1.1.50:80, idle 0:00:29, bytes 0, flags aB
TCP outside 192.168.3.205:18073 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 172.16.2.63:51503 inside 10.1.1.50:80, idle 0:00:03, bytes 0, flags aB
TCP outside 172.16.18.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
TCP outside 192.168.1.202:20773 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 192.168.4.192:23112 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 172.16.25.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
!<output omitted>

```

Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
 B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
 D - DNS, d - dump, E - outside back connection, F - outside FIN, f - inside FIN,
 G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
 i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
 k - Skinny media, M - SMTP data, m - SIP media, n - GUP
 O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
 q - SQL*Net data, R - outside acknowledged FIN,
 R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
 s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
 V - VPN orphan, W - WAAS,
 X - inspected by service module

接続状態について決定することができますか？

- A. 出力は、内部の 10.1.1.50 Web サーバに正常な活動を見せています。
- B. Web サーバ 10.1.1.50 への多くの HTTP 接続に成功 3 ウェイ TCP ハンドシェイクを完了しました。
- C. 多くの初期接続は、ランダムソースから 10.1.1.50 の Web サーバに対して行われます。
- D. 10.1.1.50 ホストが外側にランダムホストに対して SYN フラッド攻撃をトリガされます。
- E. 10.1.1.50 の Web サーバは、着信 HTTP 接続のすべてを終了しています。

Answer: C

5. 10.1.1.50 のウェブサーバは、着信 HTTP 接続のすべてを終了していますか？

- A. HTTP インスペクション
- B. DNS 検査とスヌーピング
- C. WebACL
- D. 動的なボットネットデータベースがフェッチ（更新）
- E. 静的ブラックリスト
- F. 静的ホワイト

Answer: B

6. 展示を参照してください。

```

class-map http
  match port tcp eq 21
class-map ftp
  match port tcp eq 21
policy-map test
  class http
    inspect http
  class ftp
    inspect ftp

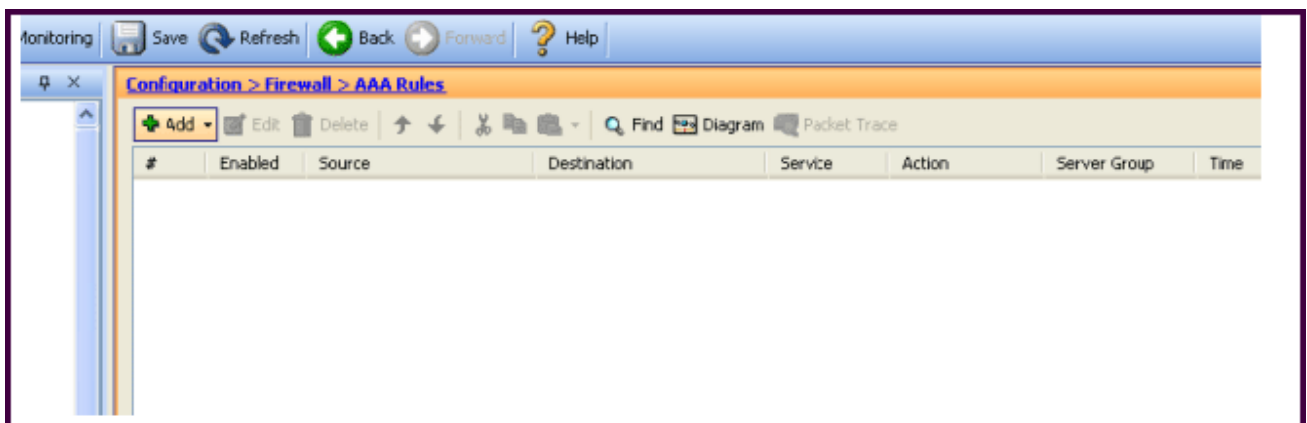
```

test という名前のポリシーマップについて正しい説明はどれですか？

- A. のみ HTTP 検査は、TCP ポート 21 のトラフィックに適用されます。
- B. のみ FTP 検査は、TCP ポート 21 のトラフィックに適用されます。
- C. HTTP と FTP 検査の両方が TCP ポート 21 のトラフィックに適用されます。
- D. いえ検査は、FTP クラスマップで HTTP クラスマップコンフィギュレーションの競合するので、TCP ポート 21 のトラフィックに適用されません。
- E. FTP、HTTP トラフィックが検査に失敗しますので、すべての FTP トラフィックが、拒否されます。

Answer: B

7. 展示を参照してください。



どの Cisco ASA の機能は、この Cisco ASDM 画面を使用して設定することができますか？

- A. Cisco ASA のコマンド許可は、TACACS+を使用する
- B. シスコ ASA にシリアル、SSH、および Telnet 接続を追跡する AAA アカウンティング
- C. AAA を使用した EXEC シェルアクセスの許可する
- D. カットスループロキシ
- E. シスコ ASDM アクセスのための AAA 認証ポリシー

Answer: D

8. 展示を参照してください。

```
failover
failover lan unit primary
failover lan interface MYFAILOVER GigabitEthernet0/2
failover interface ip MYFAILOVER 172.16.5.1 255.255.255.0 standby 172.16.5.10
failover link MYFAILOVER GigabitEthernet0/2
failover key cisco123
failover group 1
primary
preempt
failover group 2
secondary
preempt
```

どちらのコマンドでは、ステートフルフェールオーバーオプションを有効にしますか？

- A. MYFAILOVER リンクフェールオーバー GigabitEthernet0/2
- B. MYFAILOVER フェールオーバーLAN インターフェイス GigabitEthernet0/2
- C. MYFAILOVER フェールオーバーインターフェイスの IP255.255.255.0 スタンバイ 172.16.5.1 172.16.5.10
- D. 先取る
- E. フェールオーバーグループ 1 は、プライマリ
- F. 主フェールオーバー LAN ユニット

Answer: A

9. 環境の種類は、Cisco ASA MPF セット接続高度なオプションは、TCP 状態です→最も有用なのバイパスオプションしますか？

- A. SIP プロキシ
- B. WCCP
- C. BGP の Cisco ASA を通してピアリング
- D. 非対称トラフィックフロー
- E. 透過ファイアウォール

Answer: D

10. 展示を参照してください。

```
class-map type inspect ftp match-all ftp-cmd
  match request-command put
policy-map type inspect ftp ftp-insp
  class ftp-cmd
  reset
access-list ftp-acl extended permit tcp any any eq ftp
class-map ftp-cm
  match access-list ftp-acl
policy-map ftp-pm
  class ftp-cm
  inspect ftp strict ftp-insp
service-policy ftp-pm interface outside
```

どのステートメントは、MPF の設定について本当ですか？

- A. 任意の非 RFC の苦情 FTP トラフィックは、追加の FTP ディープパケット検査を通過します。
- B. FTP トラフィックは、RFC に準拠している必要があり、FTP、および PUT コマンドが使用されている場合は FTP 接続はドロップされます。
- C. ディープ FTP パケット検査は、外部インターフェイス上のすべてのインバウンドおよびアウトバウンドの TCP トラフィックで実行されます。
- D. FTP 午後ポリシーマップ型検査は、タイプでなければなりません。
- E. 設定エラーのために、外部インターフェイスを経由するすべての FTP 接続は許可されません。

Answer: B

11. 展示を参照してください。

```

ASA# show local-host 10.1.1.99
Interfaceinside: 250 active, 250 maximum active, 0 denied
local host: <10.1.1.99>,
TCP connection count/limit = 146608/unlimited
TCP embryonic count = 146606
UDP connection count/limit = 0/unlimited
Xlate(s):
Global 209.165.201.21 Local 10.1.1.99
Conn(s):
TCP out 10.101.32.157:135 in 10.1.1.99:34580 idle 0:01:43 Bytes 0 flags saA
TCP out 10.103.108.191:135 in 10.1.1.99:8688 idle 0:01:43 Bytes 0 flags saA
TCP out 10.100.205.160:135 in 10.1.1.99:7774 idle 0:01:43 Bytes 0 flags saA
TCP out 10.101.182.19:135 in 10.1.1.99:39193 idle 0:01:43 Bytes 0 flags saA
TCP out 10.102.218.45:135 in 10.1.1.99:16462 idle 0:01:43 Bytes 0 flags saA
TCP out 10.100.21.120:135 in 10.1.1.99:30322 idle 0:01:43 Bytes 0 flags saA
TCP out 10.101.25.195:135 in 10.1.1.99:41116 idle 0:01:43 Bytes 0 flags saA
TCP out 10.103.17.219:135 in 10.1.1.99:59163 idle 0:01:43 Bytes 0 flags saA
TCP out 10.102.201.141:135 in 10.1.1.99:2978 idle 0:01:43 Bytes 0 flags saA
! <output omitted>

```

合理的な結論とは何ですか？

- A. TCP 接続の最大数は、10.1.1.99 ホストが確立することができます 146608 番目になりたいんです。
- B. 10.1.1.99 からのすべての接続は、TCP 3 ウェイハンドシェイクを完了しました。
- C. 10.1.1.99 のホストは、ウイルスが原因で、おそらく、発信接続の膨大な数を生成しています。
- D. 内部の 10.1.1.99 上のホストが SYN フラッド攻撃を受けています。
- E. 内側に 10.1.1.99 ホスト操作が正常に見えます。

Answer: C

12. デフォルトでは、どのように Cisco ASA のは、Cisco ASDM ユーザに自分自身を認証しますか？

- A. 管理者は、Cisco ASA の ID 証明書の拇印内蔵工場を調べることによって、Cisco ASA のを検証します。
- B. Cisco ASA が自動的に作成し、管理者に自分自身を認証するために永続的な自己署名 X.509 証明書を使用しています。
- C. シスコ ASA は自動的に管理者に対して自身を認証するために、各再起動時に自己署名 X.509 証明書を作成します。
- D. Cisco ASA の管理者と相互に互いを認証するためのパスワードを使用しています。
- E. シスコ ASA は、ワンタイムパスワードを使用して管理者に対して自身を認証します。

Answer: C

13. 場合、Cisco ASA はパケットの発信インターフェイスは、決定論的な鋤山ルック代わりに MAC アドレスルックアップテーブルのルーティングテーブルを行う透過ファイアウォールモードで動作していたのだろうか？

- A. マルチコンテキストモードでは、設定されている場合
- B. 宛先 MAC アドレスが不明の場合
- C. 目的地は、Cisco ASA から離れホップ以上であれば

- D. NAT が設定されている場合
- E. ダイナミック ARP 検査が設定されている場合

Answer: D

14. どのフラグ `show conn` コマンドの出力に表示すると、表示が初期の SYN パケットで外部（低セキュリティレベルのインターフェイス）からのものでなかった示すために使用されていますか？

```
ASA5520# show conn
29 in use, 63 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22 bytes 1774 flags UIO
<output omitted>
```

- A. B
- B. D
- C. b
- D. A
- E. a
- F. i
- G. I
- H. O

Answer: A

15. Cisco ASA のデフォルトの ACL ロギング動作について正しい説明はどれですか？

- A. ACE を拒否拒否されたパケットごとのための Cisco ASA 遺伝子レートシステムメッセージ 106023 が設定されています。
- B. マッチした各パケットのための Cisco ASA 遺伝子レートシステムメッセージ 106023 は、ACE をしました。
- C. 唯一の最初のパケットのための Cisco ASA システムメッセージ 106100 の汎用率が ACE に一致しなかった。
- D. マッチした各パケットのための Cisco ASA 遺伝子レートシステムメッセージ 106100 は、ACE をしました。
- E. No ACL ロギングは、デフォルトで有効になっています。

Answer: A

16. どの Cisco ASA の機能は、ASA はこれらの 2 つのを行うようにしますか？

1) サーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成する。 2) は、Cisco ASA でのクライアントから ACK バックを受信すると、Cisco ASA は、クライアントを認証し、サーバーへの接続を可能にします。

- A. TCP ノーマライザ
- B. TCP ステートバイパス
- C. TCP インターセプト
- D. 基本的な脅威検出
- E. 高度な脅威検出
- F. ボットネットトラフィックフィルタ

Answer: C

17. Cisco ASA のは、複数の透過的な方法で動作しているので、セキュリティコンテキストを使用している場合、どのオプションがサポートされていませんか？

- A. NAT
- B. 共有インターフェイス
- C. セキュリティコンテキストリソース管理
- D. レイヤ7 検査
- E. failover

Answer: B

18. 展示を参照してください。

Context Name	Class	Interfaces	URL
admin	default	GigabitEthernet0/0 , GigabitEthernet0/1	disk0:/admin.cfg
*CTX	default	GigabitEthernet0/0 , GigabitEthernet0/2	disk0:/CTX.cfg

Total active Security Contexts: 2

セキュリティコンテキスト CTX 隣*は何の指示を示していますか？

- A. CTX コンテキストは、Cisco ASA 上でアクティブなコンテキストです。
- B. CTX コンテキストは、Cisco ASA 上のスタンバイコンテキストです。
- C. CTX コンテキストは、システム構成が含まれています。
- D. CTX コンテキストは、admin ロールを持っています。

Answer: D

19. どの Cisco ASA の機能が IP リバースパスインターフェイス interface_name コマンドを検証することによって実装されていますか？

- A. uRPF
- B. TCP インターセプト
- C. ボットネットトラフィックフィルタ
- D. スキャン脅威検出
- E. IPS (IP 監査)

Answer: A

20. 一つのカスタム動的なアプリケーションでは、クライアントは TCP ポート 4444 を使用して外部のサーバーへの内部に接続し、リターン・クライアントは 5000～第五千五百のポート範囲でトラフィックをネゴシエートその後、サーバーは、指定された範囲内で交渉されたポート上でクライアントに UDP データのストリーミングを開始します。どの Cisco ASA の機能またはコマンドを実行すると、この動的なカスタムアプリケーションをサポートしていますか？

- A. TCP ノーマライザ
- B. TCP インターセプト
- C. IP verify コマンド
- D. established コマンド

- E. tcp マップコマンドし、tcp オプション
- F. 接続高度なオプションのコマンドを設定する

Answer: D