Firewall Overview

1. Which of the following is not a factor in choosing a firewall? ?

A. The applications that your network uses
B. Information in your security policy
C. How much traffic will pass through the firewall
D. Security audit measures in place

Answers

1.

- ☑ **D.** Security measures that are put in place should not dictate the firewall solution you purchase.
- ☒ Answers **A**, **B**, and **C** are factors in choosing a firewall.

Firewall Categories

2. What is an example of a packet-filtering firewall? ?

A. Websense
B. Router ACLs
C. ASA state table
D. Cut-through proxy

3. Which is an advantage of a stateful firewall over a packet-filtering firewall? ?

A. Allows traffic for a connection to return through the firewall
B. Is more difficult to implement filtering of fragments
C. Supports user authentication of connections
D. Is complex to configure filtering policies

4. What kind of firewall terminates users' connections and establishes new connections to the actual destination? ?

A. Application inspection firewall
B. Stateful firewall
C. Packet-filtering firewall
D. Application gateway firewall

5. What information is found in a state table of a stateful filtering firewall? (Choose two.) ?

A. TCP flags
B. Protocol numbers or names
C. MAC addresses
D. FTP commands executed by a user

6. What kind of firewall would be used to allow multiple connections securely through the firewall for a protocol, like RTP? ?

A. Application proxy
B. Packet filter
C. Application inspection
D. Stateful

7. Application inspection firewalls are necessary for which of the following primary reasons? (Choose three.) ?

A. Reduce security weaknesses in applications and protocols

B. Allow additional connections securely through the firewall for an application
C. Allow returning traffic securely through the firewall for existing connections
D. Translate embedded addressing information in the payload of connections

Answers

2.
- ☑ **B.** Router ACLs are an example of a packet-filtering firewall.
- ☒ **A** and **D** are examples of application gateway and proxy firewalls. **C** is an example of a stateful firewall.

3.
- ☑ **A.** An advantage of a stateful firewall over a packet-filtering firewall is that a stateful firewall easily allows traffic for a connection to return through the firewall.
- ☒ **B** and **D** are true of packet-filtering firewalls. **C** is an advantage of a proxy.

4.
- ☑ **D.** An application gateway firewall terminates users' connections and establishes new connections to the actual destination, proxying traffic between the two sets of connections at the application layer.
- ☒ **A** examines application-layer information and enforces policies. **B** allows returning traffic for connections back through the firewall. **C** filters individual packets.

5.
- ☑ **A** and **B.** Stateful firewalls filter information based on packet contents (layer 3/network and layer 4/transport) as well as session information. They maintain sessions by placing connection information in a state table. This information commonly includes IP addresses, protocols, and protocol info (like TCP and UDP port numbers and TCP flags).
- ☒ **C** is layer 2 information. **D** is application-layer information.

6.
- ☑ **C.** Application inspection firewalls examine applications that use multiple connections, like RTP, and allow the additional connections securely through the firewall.
- ☒ **A** is used to proxy application information between users and servers. **B** filters individual packets. **D** allows returning traffic for existing connections securely back through the firewall.

7.
- ☑ **A**, **B**, and **D**. There are three main reasons why application inspection of traffic is necessary: security weaknesses exist in many applications and protocols; some applications and protocols use multiple connections for a session; and some applications and protocols embed addressing information in payloads, which can cause problems with address translation devices.
- ☒ **C** is a stateful firewall feature.

Cisco Firewall Products

8. What firewall feature was added in IOS version 12.4T code that gives routers similar firewall capabilities compared to the ASAs and PIXs? ?

A. CBAC
B. Reflexive ACLs

C. ZBF
D. ACLs

Answers

8.
- ☑ **C.** ZBF was added in IOS version 12.4T code and gives routers similar firewall capabilities compared to the ASAs and PIXs.
- ☒ **A** is the precursor to ZBF and was introduced in version 12.0. **B** is even older than CBAC. **D** has been around since version 7 of the IOS.

Firewall Policy Recommendations

9. What traffic should you typically be denying inbound into your network? (Choose two.) ?
A. SMTP
B. DNS
C. ICMP
D. SNMP

10. You have a router with two interfaces: FA0/0 and FA0/1. FA0/0 has networks 10.0.1.0/24, 10.0.2.0/24, and 192.168.1.0/24 associated with it. FA0/1 has networks 10.0.3.0/24, 192.168.2.0/24, and 192.168.3.0/24 associated with it. Users associated with FA0/1 need to connect to servers to FA0/0. In this situation, what addresses should you drop to prevent spoofing attacks? ?
A. Source addresses from 192.168.2.0/24
B. Destination addresses from 192.168.1.0/24
C. Destination addresses of 192.168.2.0/24
D. Source addresses from 192.168.3.0/24
E. Source addresses from 10.0.1.0/24

Answers

9.
- ☑ **C** and **D.** You should be denying traffic like ICMP, traceroute, BOOTP, DHCP, SNMP, TFTP, and others into your network.
- ☒ **A** and **B** should be allowed if you have these services in your network that external users should access.

10.
- ☑ **E.** You should be filtering source addresses associated with FA0/0, since these are not associated with the FA0/1 interface.
- ☒ **A** and **D** are associated with FA0/1 and therefore are not spoofed. **B** and **C** are destination addresses—spoofing involves source addresses.

ACL Introduction

1. Enter the wildcard mask that matches on 512 addresses: _____. ?

2. Which of the following is true concerning ACLs? ?
A. All statements in an ACL are processed.

B. Less restrictive statements should be placed at the top of an ACL.
C. All ACLs, including empty ACLs, have an implicit deny statement.
D. ACLs cannot filter traffic that the router itself originates.

3. Enter the wildcard mask that will match on 16 addresses: _____.

Answers

1.
- ☑ The wildcard mask that matches on 512 addresses is **0.0.1.255**.

2.
- ☑ **D.** ACLs cannot filter traffic that the router itself originates.
- ☒ If a match is found, ACL entries are no longer processed, making **A** incorrect. More restrictive statements should appear at the top of an ACL, making **B**incorrect. An empty ACL (a nonexistent ACL applied to an interface) has no implicit deny statement, making **C** incorrect.

3.
- ☑ The wildcard mask that matches on 16 addresses is **0.0.0.15**.

ACL Configuration from the CLI

4. Which of the following is true concerning ACLs? (Choose two.)

A. Standard ACLs should be placed as close to the source as possible.
B. Standard ACLs should be placed as close to the destination as possible.
C. Extended ACLs should be placed as close to the source as possible.
D. Extended ACLs should be placed as close to the destination as possible.

5. Create an extended ACL configuration that will prevent the Smurf attack directed at 192.1.1.0/24. Permit all other traffic. Your configuration should have no more than three statements and should be applied inbound on FA0/0. Use an ACL ID of 100.

6. Create an extended ACL, using an ACL ID of 100, that will permit SMTP traffic to the e-mail server at 192.1.1.1 and queries to the DNS server at 192.1.1.2. Do not allow spoofed traffic with the ISP-assigned address space of 192.1.1.0/24 to reach these servers. Make sure you can see the hit counts on all dropped packets.

Answers

4.
- ☑ **B** and **C.** Standard ACLs should be placed as close to the destination as possible, and extended ACLs should be placed as close to the source as possible.
- ☒ **A** is incorrect because it should be the destination. **D** is incorrect because it should be the source.

5.
- ☑ Here is the configuration to block the Smurf attack against network 192.1.1.0/24:
-
- `access-list 100 deny ip any host 192.1.1.0`

- **access-list 100 deny ip any host 192.1.1.255**
- **access-list 100 permit ip any any**
- **interface fa0/0**
- **ip access-group 100 in**

6.
- ☑ Here is the ACL:
-
- **access-list 100 deny 192.1.1.0 0.0.0.255 any**
- **access-list 100 permit tcp any host 192.1.1.1 eq 25**
- **access-list 100 permit udp any host 192.1.1.2 eq 53**
- **access-list 100 deny ip any any**

Additional ACL Features

7. What IOS feature reduces search times and provides predictable latency by compiling ACLs into a hash table? ?

A. Sequenced ACLs
B. ZBF
C. Turbo ACLs
D. TCP Intercept

8. Examine the following code: ?

```
Router# show access-list
Extended IP access list 101
    10 permit ip host 192.168.101.66 any
    20 permit ip host 192.168.101.88 any
```

Insert an ACL statement between the two statements in ACL 101 that will allow 192.168.101.77/32 to access any destination: _____.

Answers

7.
- ☑ **C.** Turbo ACLs reduce search times and provide predictable latency by compiling ACLs into a hash table.
- ☒ **A** allows you to easily edit ACLs from the CLI. **B** implements a stateful firewall. **D** prevents TCP SYN flood attacks.

8.
- ☑ Here is the ACL configuration that will insert the correct entry into ACL 101:
-
- **ip access-list extended 101**
- **15 permit ip host 192.168.101.77 any**

SDM and ACLs

9. In SDM, where do you go to create an ACL? ?

A. Configure | Additional Tasks | ACL Editor | Access Rules
B. Configuration | Firewall And ACLs | ACL Editor | Access Rules
C. Configure | Firewall And ACLs | ACL Editor | Access Rules
D. Configure | ACL Editor | Access Rules

10. In SDM, where would you go to activate an ACL to restrict telnet and SSH access on any of the router's interfaces? ?

A. Configure | Additional Tasks | ACL Editor | Access Rules
B. Configure | Additional Tasks | Router Access | VTY
C. Configure | Interfaces
D. Configure | Additional Tasks | Router Properties | VTY

Answers

9.
- ☑ **A.** To create an ACL in SDM, go to Configure | Additional Tasks | ACL Editor | Access Rules.
- ☒ **B** is incorrect because it is the Configure button. **C** and **D** are incorrect because these are invalid SDM paths.

10.
- ☑ **B.** To restrict access to the VTYs in SDM, go to Configure | Additional Tasks | Router Access | VTY.
- ☒ **A** and **C** allow you to associate ACLs to interfaces. **D** is a nonexistent path in SDM.

ZBF Overview

1. What IOS feature defines applications or connections for ZBF? ?

A. PAM
B. CBAC
C. RACL
D. Zone

2. ZBF policies are applied how? ?

A. On an interface
B. Bidirectionally between zones
C. Unidirectionally between zones
D. With ACLs

Answers

1.
- ☑ **A.** Granular Policy Inspection (GPI), commonly called Port Application Mapping (PAM), is used to define applications or connections for CBAC and ZBF.
- ☒ **B** is ZBF's precursor for a stateful firewall feature in the IOS. **C**, reflexive ACLs, was Cisco's first stateful firewall solution. **D** is used by ZBF to implement policies.

2.
- ☑ **C.** ZBF applies unidirectional policies between two zones.

- ☒ **A** is incorrect because policies are applied between zones. **B** is incorrect because policies are applied unidirectionally. **D** can be used to classify traffic, not to apply policies.

Class Maps

3. Examine the following configuration. Which of the following statements is true of this configuration?

```
Router(config)# class-map type inspect match-all mymap
Router(config-cmap)# match protocol http
Router(config-cmap)# match protocol smtp
```

A. Only HTTP traffic is matched on.
B. Only SMTP traffic is matched on.
C. Both HTTP and SMTP traffic is matched.
D. Neither HTTP nor SMTP traffic is matched.

4. Which of the following is not supported by DPI?

A. HTTP
B. POP3
C. IM
D. FTP

Answers

3.
- ☑ **D.** Because the `match-all` parameter is used, it is impossible for a connection to be both HTTP and SMTP.
- ☒ Therefore answers **A**, **B**, and **C** are incorrect.

4.
- ☑ **D.** FTP is not supported by DPI, or L7 class maps.
- ☒ **A**, **B**, and **C** are supported and therefore are incorrect answers.

Parameter Maps

5. Which of the following is a URL filtering server supported by the IOS?

A. Websmart
B. SmartFilter
C. Smartsense
D. ISR routers

Answers

5.
- ☑ **B.** SmartFilter is a URL filtering server supported by the IOS.
- ☒ **A** and **C** are nonexistent products. **D** implements policies defined on a URL filtering server.

Policy Maps

6. Which of the following is not an action you can implement as a policy for a

class map?

A. Drop
B. Reset
C. Inspect
D. Allow

Answers

6.

- ☑ **D.** Common policy actions you can implement on matching a class map include: drop, pass, reset, and inspect. Allow is not a policy—it should be pass.
- ☒ **A**, **B**, and **C** are supported actions.

Zones and Zone Pairs

7. A _____is assigned to a zone pair to implement unidirectional policies.

A. Class map
B. Parameter map
C. Policy map
D. PAM map

8. What IOS command assigns a policy to a zone pair?

A. `zone-pair security`
B. `service-policy`
C. `policy-map type inspect`
D. `zone security`

9. What IOS command displays the sessions in the state table for ZBF?

A. `show policy-map type inspect zone-pair sessions`
B. `show zone-pair security`
C. `show zone security`
D. `show policy-map type inspect`

Answers

7.

- ☑ **C.** A policy map is assigned to a zone pair to implement unidirectional policies.
- ☒ **A** identifies traffic to assign a policy to. **B** assigns additional criteria to traffic, like limiting the number of connections. **D** matches applications to the ports they use.

8.

- ☑ **B.** The `service-policy` command associates a policy to a zone pair.
- ☒ **A** creates the zone pairs, specifying the zones and the direction of the policy. **C** defines the policies for the class maps. **D** associates a zone to an interface.

9.

- ☑ **A.** The `show policy-map type inspect zone-pair sessions` command displays the router's ZBF state table.
- ☒ **B** displays the source and destination zones and the associated

policy. **C** displays the zones and the interfaces associated with them. **D** displays the policy maps.

SDM and ZBF

10. What are the two firewall options for the Firewall and ACL Wizard in SDM?

A. Basic and Advanced
B. Non-DMZ and DMZ
C. Simple and Advanced
D. Simple and Complex

Answers

10.

- ☑ **A.** The basic firewall wizard sets up ZBF without a DMZ. The advanced firewall wizard sets up ZBF with a DMZ.
- ☒ **B**, **C**, and **D** have one or more incorrect options.