



**642-504**

**Securing Networks with Cisco Routers and Switches**

Q&A

DEMO Version

Copyright (c) 2011 Chinatag LLC. All rights reserved.

## **Important Note Please Read Carefully**

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website.

## **Study Tips**

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

## **Latest Version**

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to [feedback@chinatag.com](mailto:feedback@chinatag.com).

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team  
Chinatag LLC.

**QUESTION 1**

Which two technologies can secure the control plane of the Cisco router? (Choose two.)

- A. BPDU protection
- B. role-based access control
- C. routing protocol authentication
- D. CPPr

**Answer:** CD

**QUESTION 2**

Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that provides a comprehensive identity networking solution. Which of these statements is correct regarding user setup on ACS 4.0?

- A. Users are assigned to the default group.
- B. A user can belong to more than one group.
- C. The username can contain characters such as "#" and "?".
- D. The settings at the group level override the settings configured at the user level

**Answer:** A


**QUESTION 3**

Please study the exhibit carefully, and then answer the following question: .

Home Configure Monitor Refresh Save Search Help

### About Your Router

Host Name: R1



**Cisco 2811**

Hardware	More ...	Software	More ...
<b>Model Type:</b>	Cisco 2811	<b>IOS Version:</b>	12.4(24)T3
<b>Available / Total Memory(MB):</b>	76/256 MB	<b>SDM Version:</b>	2.5
<b>Total Flash Capacity:</b>	61 MB		

Feature Availability: IP ✔ Firewall ✔ VPN ✔ IPS ✔ NAC ✔

### Configuration Overview

[View Running Config](#)

**Interfaces and Connections** Up (1) Down (11)

<b>Total Supported LAN:</b>	2	<b>Total Supported WAN:</b>	6
<b>Configured LAN Interface:</b>	2	<b>Total WAN Connections:</b>	0
<b>DHCP Server:</b>	Not Configured		

**Firewall Policies** Active

Zone Pair's	Source Zone	Destination Zone	Policy Name
sdm-zp-self-out	self	out-zone	sdm-permit-icmpreply
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	sdm-inspect

**VPN** Up (0)

<b>IPSec (Site-to-Site):</b>	0	<b>GRE over IPSec:</b>	0
<b>Xauth Login Required:</b>	0	<b>Easy VPN Remote:</b>	0
<b>No. of DMVPN Clients:</b>	0	<b>No. of Active VPN Clients:</b>	0

**Routing**

<b>No. of Static Route:</b>	1
<b>Dynamic Routing Protocols:</b>	None

**Intrusion Prevention**

<b>Total Active Signatures:</b>	558
<b>No. of IPS-enabled Interfaces:</b>	2
<b>Signature Version:</b>	9516.0

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
      - HTTP
      - IM
      - P2P
      - SMTP
      - RPC
      - IMAP
      - POP3
  - Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

**HTTP Protocol Application Service Groups** Add... Edit... Delete

Class Map Name	Used By
http-url-length	http-url-length

Details of Class Map: http-url-length

Item Name	Item Value
Request	
Port Misuse	Disabled
URI	Length > 600
Response	
Req-Resp	
Protocol Violation	Disabled

Home | Configure | Monitor | Refresh | Save | Search | Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Firewall**

Create Firewall | **Edit Firewall Policy**

Traffic Classification					Action	Rule Options
ID	Source	Destination	Service			
<b>sdm-permit-icmpreply ( self to out-zone)</b>						
1	any	any	icmp tcp udp	Permit Firewall		
2	Unmatched Traffic			Permit ACL		
<b>sdm-permit ( out-zone to self)</b>						
1	Unmatched Traffic			Drop		
<b>sdm-inspect ( in-zone to out-zone)</b>						
1	100		any	Drop	Log	
	<ul style="list-style-type: none"> <li>255.255.255.255 -&gt; any</li> <li>127.0.0.0/0.255.255.255 -&gt; any</li> <li>10.0.0.0/0.0.0.255 -&gt; any</li> </ul>					
2	any	any	sdm-cls-insp-traffic	Permit Firewall		
3	any	any	http	Permit Firewall		
4	192.168.10.0	10.0.0.0	http	Permit Firewall	Options	
5	any	any	h323 skinny sip	Permit Firewall		
6	Unmatched Traffic			Permit ACL		

Rule Flow Diagram

self ← [Router] → out-zone

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
    - Parameter Map
      - Inspect**
      - Protocol Info
      - URL Filtering
      - Regular Expression
  - Configuration Management
    - Config Editor
    - Reset to factory default

**Inspect Settings Parameter Maps** Add... Edit... Delete

Parameter Map Name	Used By
TESTPM	sdm-inspect

Details of Parameter Map: TESTPM

Item Name	Item Value
Alert	On
Audit trail	Off
TCP Syn-wait timeout	30
TCP Fin-wait timeout	5
TCP idle timeout	3600
UDP idle timeout	35
DNS timeout	5
ICMP idle timeout	10

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs**
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspectio
- Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

Zone Pair	Source	Destination	Policy
sdm-zp-self-out	self	out-zone	sdm-permit-icmp
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	TESTPM

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mapping
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Parameter Map
  - Inspect
  - Protocol Info
  - URL Filtering

**HTTP Policy Maps** Add... Edit... Delete

Policy Map Name	Description
http-url-length	

Details of Policy Map: http-url-length

Match Class Name	Action	Log
http-url-length	Reset	Disabled

The screenshot shows the Cisco IOS SDM interface. The left sidebar contains navigation icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. The main area is divided into 'Tasks' and 'Additional Tasks'. The 'Additional Tasks' tree view shows a hierarchy of configuration options, with 'Protocol Inspection' selected. The right pane displays the configuration for the 'TESTPM' policy map.

**Protocol Inspection Policy Maps**

Policy Map Name	Description
TESTPM	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

**Details of Policy Map: TESTPM**

Match Class Name	Action
TESTPM	Inspect

Refer to the appropriate SDM screen(s), which two statements correctly describe the Cisco IOS Zone-Based Firewall configuration? (Choose two)

- A. The "reset" action is applied to any HTTP request sourced from the "in" zone and destined to the "out" zone, which also has a request Uniform Resource Identifier (URI) that is greater than 500 bytes in length.
- B. The "inspect" action is applied to Internet Control Message Protocol (ICMP) traffic sourced from the "in" zone and destined to the "out" zone.
- C. The "http-policy" inspection policy map is applied to all HTTP and HTTPS traffic sourced from the "in" zone and destined to the "out" zone.
- D. The "testpm" inspection policy map is applied to the inout zone-pair.

**Answer: AD**


#### QUESTION 4

Refer to the appropriate SDM screen(s), what is the User Datagram Protocol (UDP) idle time set for any HTTP traffic that is sourced from the "in" zone and destined to the "out" zone?

Home    Configure    Monitor    Refresh    Save    Search    Help

---

**About Your Router** Host Name: R1



**Cisco 2811**

Hardware	Software
<b>Model Type:</b> Cisco 2811	<b>IOS Version:</b> 12.4(24)T3
<b>Available / Total Memory(MB):</b> 76/256 MB	<b>SDM Version:</b> 2.5
<b>Total Flash Capacity:</b> 61 MB	

Feature Availability: IP ✔ Firewall ✔ VPN ✔ IPS ✔ NAC ✔

---

**Configuration Overview** View Running Config

**Interfaces and Connections** Up (1)    Down (11)

<b>Total Supported LAN:</b>	2	<b>Total Supported WAN:</b>	6
<b>Configured LAN Interface:</b>	2	<b>Total WAN Connections:</b>	0
<b>DHCP Server:</b>	Not Configured		

**Firewall Policies** Active

Zone Pair's	Source Zone	Destination Zone	Policy Name
sdm-zp-self-out	self	out-zone	sdm-permit-icmpreply
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	sdm-inspect

**VPN** Up (0)

<b>IPSec (Site-to-Site):</b>	0	<b>GRE over IPSec:</b>	0
<b>Xauth Login Required:</b>	0	<b>Easy VPN Remote:</b>	0
<b>No. of DMVPN Clients:</b>	0	<b>No. of Active VPN Clients:</b>	0

<b>Routing</b>	<b>Intrusion Prevention</b>	
<b>No. of Static Route:</b>	1	
<b>Dynamic Routing Protocols:</b>	None	
	<b>Total Active Signatures:</b>	558
	<b>No. of IPS-enabled Interfaces:</b>	2
	<b>Signature Version:</b>	9516.0

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
      - HTTP
      - IM
      - P2P
      - SMTP
      - RPC
      - IMAP
      - POP3
  - Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

**HTTP Protocol Application Service Groups** Add... Edit... Delete

Class Map Name	Used By
http-url-length	http-url-length

Details of Class Map: http-url-length

Item Name	Item Value
Request	
Port Misuse	Disabled
URI	Length > 600
Response	
Req-Resp	
Protocol Violation	Disabled

Home | Configure | Monitor | Refresh | Save | Search | Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Firewall**

Create Firewall | **Edit Firewall Policy**

+ Add | Edit | Delete | Move Up | Move Down | Cut | Copy | Paste | Rule Diagram

Traffic Classification					Action	Rule Options
ID	Source	Destination	Service			
<b>sdm-permit-icmpreply ( self to out-zone)</b>						
1	any	any	icmp tcp udp	Permit Firewall		
2	Unmatched Traffic			Permit ACL		
<b>sdm-permit ( out-zone to self)</b>						
1	Unmatched Traffic			Drop		
<b>sdm-inspect ( in-zone to out-zone)</b>						
1	100		any	Drop	Log	
	<ul style="list-style-type: none"> <li>255.255.255.255 -&gt; any</li> <li>127.0.0.0/0.255.255.255 -&gt; any</li> <li>10.0.0.0/0.0.0.255 -&gt; any</li> </ul>					
2	any	any	sdm-cls-insp-traffic	Permit Firewall		
3	any	any	http	Permit Firewall		
4	192.168.10.0	10.0.0.0	http	Permit Firewall	Options	
5	any	any	h323 skinny sip	Permit Firewall		
6	Unmatched Traffic			Permit ACL		

Rule Flow Diagram

self ← [Router] → out-zone

Apply Changes | Discard Changes

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
  - Parameter Map
    - Inspect**
    - Protocol Info
    - URL Filtering
    - Regular Expression
- Configuration Management
  - Config Editor
  - Reset to factory default

**Inspect Settings Parameter Maps** Add... Edit... Delete

Parameter Map Name	Used By
TESTPM	sdm-inspect

Details of Parameter Map: TESTPM

Item Name	Item Value
Alert	On
Audit trail	Off
TCP Syn-wait timeout	30
TCP Fin-wait timeout	5
TCP idle timeout	3600
UDP idle timeout	35
DNS timeout	5
ICMP idle timeout	10

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs**
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspectio
- Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

Zone Pairs Add... Edit... Delete

Zone Pair	Source	Destination	Policy
sdm-zp-self-out	self	out-zone	sdm-permit-icmp
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	TESTPM

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mapping
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Parameter Map
  - Inspect
  - Protocol Info
  - URL Filtering

**HTTP Policy Maps** Add... Edit... Delete

Policy Map Name	Description
http-url-length	

Details of Policy Map: http-url-length

Match Class Name	Action	Log
http-url-length	Reset	Disabled

The screenshot shows the Cisco SDM interface. The left sidebar contains various task categories like 'Interfaces and Connections', 'Firewall and ACL', 'VPN', 'Security Audit', 'Routing', 'NAT', 'Intrusion Prevention', 'Quality of Service', and 'NAC'. The main area is titled 'Additional Tasks' and shows a tree view of configuration options. The 'Protocol Inspection' option is selected. On the right, the 'Protocol Inspection Policy Maps' table is displayed, showing a policy map named 'TESTPM' with three entries: 'sdm-permit-icmpreply', 'sdm-permit', and 'sdm-inspect'. Below this, the 'Details of Policy Map: TESTPM' table shows a match class named 'TESTPM' with the action 'Inspect'.

Policy Map Name	Description
TESTPM	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

Match Class Name	Action
TESTPM	Inspect

- A. 10 seconds
- B. 15 seconds
- C. 30 seconds
- D. 35 seconds

**Answer: D**


#### QUESTION 5

Refer to the appropriate SDM screen(s), what is the reason that outside hosts can't initiate Telnet (port 23) traffic to the 172.16.1.10 inside host?

Home    Configure    Monitor    Refresh    Save    Search    Help

---

**About Your Router** Host Name: R1



**Cisco 2811**

Hardware	Software
<b>Model Type:</b> Cisco 2811	<b>IOS Version:</b> 12.4(24)T3
<b>Available / Total Memory(MB):</b> 76/256 MB	<b>SDM Version:</b> 2.5
<b>Total Flash Capacity:</b> 61 MB	

Feature Availability: IP ✔ Firewall ✔ VPN ✔ IPS ✔ NAC ✔

---

**Configuration Overview** View Running Config

**Interfaces and Connections** Up (1)    Down (11)

<b>Total Supported LAN:</b>	2	<b>Total Supported WAN:</b>	6
<b>Configured LAN Interface:</b>	2	<b>Total WAN Connections:</b>	0
<b>DHCP Server:</b>	Not Configured		

**Firewall Policies** Active

Zone Pair's	Source Zone	Destination Zone	Policy Name
sdm-zp-self-out	self	out-zone	sdm-permit-icmpreply
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	sdm-inspect

**VPN** Up (0)

<b>IPSec (Site-to-Site):</b>	0	<b>GRE over IPSec:</b>	0
<b>Xauth Login Required:</b>	0	<b>Easy VPN Remote:</b>	0
<b>No. of DMVPN Clients:</b>	0	<b>No. of Active VPN Clients:</b>	0

<b>Routing</b>	<b>Intrusion Prevention</b>	
<b>No. of Static Route:</b>	1	
<b>Dynamic Routing Protocols:</b>	None	
	<b>Total Active Signatures:</b>	558
	<b>No. of IPS-enabled Interfaces:</b>	2
	<b>Signature Version:</b>	9516.0

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
      - HTTP
      - IM
      - P2P
      - SMTP
      - RPC
      - IMAP
      - POP3
  - Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

**HTTP Protocol Application Service Groups** Add... Edit... Delete

Class Map Name	Used By
http-url-length	http-url-length

Details of Class Map: http-url-length

Item Name	Item Value
Request	
Port Misuse	Disabled
URI	Length > 600
Response	
Req-Resp	
Protocol Violation	Disabled

Home | Configure | Monitor | Refresh | Save | Search | Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Firewall**

Create Firewall | **Edit Firewall Policy**

+ Add | Edit | Delete | Move Up | Move Down | Cut | Copy | Paste | Rule Diagram

Traffic Classification				Action	Rule Options
ID	Source	Destination	Service		
<b>sdm-permit-icmpreply ( self to out-zone)</b>					
1	any	any	icmp tcp udp	Permit Firewall	
2	Unmatched Traffic			Permit ACL	
<b>sdm-permit ( out-zone to self)</b>					
1	Unmatched Traffic			Drop	
<b>sdm-inspect ( in-zone to out-zone)</b>					
1	100		any	Drop	Log
	<ul style="list-style-type: none"> <li>255.255.255.255 -&gt; any</li> <li>127.0.0.0/0.255.255.255 -&gt; any</li> <li>10.0.0.0/0.0.0.255 -&gt; any</li> </ul>				
2	any	any	sdm-cls-insp-traffic	Permit Firewall	
3	any	any	http	Permit Firewall	
4	192.168.10.0	10.0.0.0	http	Permit Firewall	Options
5	any	any	h323 skinny sip	Permit Firewall	
6	Unmatched Traffic			Permit ACL	

Rule Flow Diagram

self ← [Router] → out-zone

Apply Changes | Discard Changes

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
  - Class Map
    - QoS Class Map
    - Inspection
    - Deep Packet Inspection
    - Parameter Map
      - Inspect**
      - Protocol Info
      - URL Filtering
      - Regular Expression
  - Configuration Management
    - Config Editor
    - Reset to factory default

**Inspect Settings Parameter Maps** Add... Edit... Delete

Parameter Map Name	Used By
TESTPM	sdm-inspect

Details of Parameter Map: TESTPM

Item Name	Item Value
Alert	On
Audit trail	Off
TCP Syn-wait timeout	30
TCP Fin-wait timeout	5
TCP idle timeout	3600
UDP idle timeout	35
DNS timeout	5
ICMP idle timeout	10

Home    Configure    Monitor    Refresh    Save    Search    Help

---

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs**
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspectio
- Parameter Map
- Configuration Management
  - Config Editor
  - Reset to factory default

Add...    Edit...    Delete

Zone Pair	Source	Destination	Policy
sdm-zp-self-out	self	out-zone	sdm-permit-icmp
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	TESTPM

Home
Configure
Monitor
Refresh
Save
Search
Help

**Tasks**

- Interfaces and Connections
- Firewall and ACL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

**Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mapping
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
  - QoS Policy Map
  - Protocol Inspection
  - Application Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Class Map
  - QoS Class Map
  - Inspection
  - Deep Packet Inspection
    - HTTP
    - IM
    - P2P
    - SMTP
    - RPC
    - IMAP
    - POP3
- Parameter Map
  - Inspect
  - Protocol Info
  - URL Filtering

**HTTP Policy Maps** Add... Edit... Delete

Policy Map Name	Description
http-url-length	

Details of Policy Map: http-url-length

Match Class Name	Action	Log
http-url-length	Reset	Disabled

The screenshot shows the Cisco IOS configuration interface. The top navigation bar includes Home, Configure, Monitor, Refresh, Save, Search, and Help. The left sidebar contains various task categories: Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, Quality of Service, and NAC. The 'Additional Tasks' menu is expanded, showing a tree structure of configuration options. The 'Protocol Inspection Policy Maps' section is selected, displaying a table of policy maps and a details view for the 'TESTPM' policy map.

Policy Map Name	Description
TESTPM	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

Match Class Name	Action
TESTPM	Inspect

- A. The implicit deny access control list (ACL) entry on the inbound ACL is applied to the outside interface.
- B. Static NAT is not correctly enabled to translate the 172.16.1.10 inside host address.
- C. There is no zone-based firewall policy applied to the traffic sourced from the "out" zone and destined to the "in" zone.
- D. The implicit deny access control list (ACL) entry on the inbound ACL is applied to the outside interface.

**Answer: C**

#### QUESTION 6

Which two category types are associated with 5.x signature use in Cisco IOS IPS? (Choose two.)

- A. basic
- B. advanced
- C. attack-drop
- D. built-in

**Answer: AB**

### QUESTION 7

Select two issues that you should consider when implementing IOS Firewall IDS. (Choose two)

- A. The memory usage
- B. The number of DMZs
- C. The signature coverage
- D. The number of router interfaces

**Answer: AC**


### QUESTION 8

You are the Cisco Configuration Assistant in your company. Which command is used to support 802.1X guest VLAN functionality based on the following configuration?

```

aaa new model
aaa authentication dot1x default group radius
aaa authentication network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting system default start-stop group radius
radius-server host 10.1.1.1 auth-port 1812 acct-po
radius-server key cisco123

```



- A. aaa authorization network default group radius
- B. aaa authentication dot1x default group radius
- C. aaa accounting dot1x default start-stop group radius
- D. aaa accounting system default start-stop group radius

**Answer: A**

### QUESTION 9

You are in charge of Securing Networks Cisco Routers and Switches in your company. Why is the Cisco IOS Firewall authentication proxy not working based on the following configuration?

```

aaa new model
aaa authentication login default group tacacs
aaa authentication auth-proxy default group tacacs+
aaa accounting auth-proxy default start-stop group tacacs+ enable password
TeSt_123
ip auto-proxy name pxy http
ip auto-proxy auth-proxy-banner
interface Ethernet0/1
  ip address 192.168.1.1 255.255.255.0
  ip auto-proxy pxy
no ip http server
tacacs-server host 192.168.123.14
tacacs-server key Cisco
[Output omitted]

```

- A. The aaa authentication auth-proxy default group tacacs+ command is missing
- B. The router local username and password database is not configured.
- C. You forgot to enable HTTP server and AAA authentication
- D. Cisco IOS authentication proxy not support TACACS+.

**Answer: C**

**QUESTION 10**

Which advantage can be obtained by implementing the Cisco IOS Firewall feature?

- A. provides data leakage protection capabilities
- B. integrates multiprotocol routing with security policy enforcement
- C. is easily deployed and managed by the Cisco Adaptive Security Device Manager
- D. acts primarily as a dedicated firewall device

**Answer: B**