

Managing a Secure Network

Question 1

For the following attempts, which one is to ensure that no employee becomes a pervasive security threat, that data can be recovered from backups, and that information system changes do not compromise a system's security?

Operations security

Question 2

Which three options are network evaluation techniques? (Choose three)

Scanning a network for active IP addresses and open ports on those IP addresses

Using password-cracking utilities

Performing virus scans

Question 3

Which is the main difference between host-based and network-based intrusion prevention?

Network-based IPS can provide protection to desktops and servers without the need of installing specialized software on the end hosts and servers.

Question 4

The enable secret password appears as an MD5 hash in a router's configuration file, whereas the enable password is not hashed (or encrypted, if the password-encryption service is not enabled). What is the reason that Cisco still support the use of both enable secret and enable passwords in a router's configuration?

The enable password is present for backward compatibility.

Question 5

Which type of MAC address is dynamically learned by a switch port and then added to the switch's running configuration?

Sticky secure MAC address

Question 6

Which are the best practices for attack mitigations?

Keep patches up to date

Inform users about social engineering

Develop a dynamic security policy

Disable unnecessary services

Question 7

Which one of the Cisco IOS commands can be used to verify that either the Cisco IOS image, the configuration files, or both have been properly backed up and secured?

show secure bootset

Question 8

Which name is of the e-mail traffic monitoring service that underlies that architecture of IronPort?

SenderBase

Question 9

Based on the username global configuration mode command displayed in the exhibit. What does the option secret 5 indicate about the enable secret password? Router# show run | include username
Username test secret 5 \$1\$knm. \$GOGQBIL8TK77POLWxvX400

It is hashed using MD5.

Question 10

What will be disabled as a result of the no service password-recovery command?

ROMMON

Implementing Virtual Private Networks

Question 1

You work as a network engineer, do you know an IPsec tunnel is negotiated within the protection of which type of tunnel?

ISAKMP tunnel

Question 2

For the following items, which one acts as a VPN termination device and is located at a primary network location?

Headend VPN device

Cryptographic Systems

Question 1

Please choose the correct matching relationships between the cryptography algorithms and the type of algorithm.

3DES

RSA

Diffie-Hellman

AES

IDEA

Elliptical Curve

Symmetric – 3DES, AES, IDEA

Asymmetric – RSA, Diffie-Hellman, Elliptical Curve

Question 2

What is the objective of Diffie-Hellman?

Used to establish a symmetric shared key via a public key exchange process

Question 3

Which description about asymmetric encryption algorithms is correct?

They use different keys for encryption and decryption of data

Question 4

Regarding constructing a good encryption algorithm, what does creating an avalanche effect indicate?

Changing only a few bits of a plain-text message causes the ciphertext to be completely different

Question 5

Stream ciphers run on which of the following?

Individual digits, one at a time, with the transformations varying during the encryption

Question 6

Which description is true about ECB mode?

ECB mode uses the same 56-bit key to serially encrypt each 64-bit plain-text block.

Question 7

Which example is of a function intended for cryptographic hashing?

MD5

Question 8

What is the MD5 algorithm used for?

takes a variable-length message and produces a 128-bit message digest

Question 9

Which algorithm was the first to be found suitable for both digital signing and encryption?

RSA

Question 10

Before a Diffie-Hellman exchange may begin, the two parties involved must agree on what?

Two nonsecret numbers

Question 11

Which item is the correct matching relationships associated with IKE Phase?

Perform a Diffie-Hellman exchange

Establish Ipsec SAs

Negotiate Ipsec security policies

Negotiate IKE policy sets and authenticate peers

Perform an optional Diffie-Hellman exchange

IKE Phase 1 – Perform a Diffie-Hellman exchange | Negotiate IKE policy sets and authenticate peers

IKE Phase 2 – Establish Isec SAs | Negotiate Isec security policies | Perform an optional Diffie-Hellman exchange

Question 12

Which three are distinctions between asymmetric and symmetric algorithms? (Choose all that apply)

Asymmetric algorithms are based on more complex mathematical computations.

Only asymmetric algorithms have a key exchange technology built in.

Asymmetric algorithms are used quite often as key exchange protocols for symmetric algorithms.

Question 13

For the following statements, which one is the strongest symmetrical encryption algorithm?

AES

Question 14

Which Public Key Cryptographic Standards (PKCS) defines the syntax for encrypted messages and messages with digital signatures?

PKCS #7

Storage Area Network SAN

Question 1

Which two primary port authentication protocols are used with VSANs? (Choose two.)

CHAP

DHCHAP

Securing Local Area Networks

Question 1

You suspect an attacker in your network has configured a rogue layer 2 device to intercept traffic from multiple VLANs, thereby allowing the attacker to capture potentially sensitive data. Which two methods will help to mitigate this type of activity? (Choose two)

Disable DTP on ports that require trunking

Question 2

In an IEEE 802.1x deployment, between which two devices EAPOL messages typically are sent?

Between the supplicant and the authenticator

Implementing Intrusion Prevention

Question 1

When configuring Cisco IOS login enhancements for virtual connections, what is the “quiet period”?

The period of time in which virtual login attempts are blocked, following repeated failed login attempts

Question 2

Which result is of securing the Cisco IOS image by use of the Cisco IOS image resilience feature?

The Cisco IOS image file will not be visible in the output from the show flash command.

Question 3

Which description is true about the show login command output displayed in the exhibit?

Router# show login

A default login delay of 1 seconds is applied.

No Quiet-Mode access list has been configured.

All successful login is logged and generate SNMP traps.

All failed login is logged and generate SNMP traps.

Router enabled to watch for login Attacks.

If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.

Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.

Denying logins from all sources.

Three or more login requests have failed within the last 100 seconds.

Question 4

After enabling port security on a Cisco Catalyst switch, what is the default action when the configured maximum of allowed MAC addresses value is exceeded?

The port is shut down.

Question 5

When configuring SSH, which is the Cisco minimum recommended modulus value?

1024 bits

Question 6

Examine the following options , which Spanning Tree Protocol (STP) protection mechanism disables a switch port if the port receives a Bridge Protocol Data Unit (BPDU)?

BPDU Guard

Question 7

For the following options, which feature is the foundation of Cisco Self-Defending Network technology?

secure network platform

Question 8

Which type of intrusion prevention technology will be primarily used by the Cisco IPS security appliances?

signature-based

Question 9

What will be enabled by the scanning technology – The Dynamic Vector Streaming (DVS)?

Signature-based spyware filtering

Question 10

Which statement is not a reason for an organization to incorporate a SAN in its enterprise infrastructure?

To decrease the threat of viruses and worm attacks against data storage devices

Question 11

Which two functions are required for IPsec operation? (Choose two)

using Diffie-Hellman to establish a shared-secret key

using IKE to negotiate the SA

Question 12

In your company's network, an attacker who has configured a rogue layer 2 device is intercepting traffic from multiple VLANS to capture potentially sensitive data. How to solve this problem? (Choose two)

Disable DTP on ports that require trunking

Set the native VLAN on the trunk ports to an unused VLAN

Security Device Manager SDM

Question 1

For the following options, which one accurately matches the CU command(s) to the equivalent SDM wizard that performs similar configuration functions?

auto secure exec command and the SDM One-Step Lockdown wizard

Question 2

Which three statements are valid SDM configuration wizards? (Choose three)

Security Audit

VPN

NAT

Question 3

Which two protocols enable Cisco SDM to pull IPS alerts from a Cisco ISR router? (Choose two)

HTTPS
SDEE

Question 4

When using the Cisco SDM Quick Setup Site-to-Site VPN wizard, which three parameters do you configure? (Choose three)

Interface for the VPN connection
IP address for the remote peer
Source interface where encrypted traffic originates

Explanation

The image below shows parameters when using Cisco SDM Quick Setup Site-to-Site VPN wizard

The screenshot shows the 'Site-to-Site VPN Wizard' configuration window. The 'VPN Connection Information' section has a dropdown menu set to 'Serial0/1/0'. The 'Peer Identity' section has a dropdown menu set to 'Peer with static IP address' and a text box containing '192.168.1.2'. The 'Authentication' section has the 'Pre-shared keys' radio button selected. The 'Traffic to encrypt' section has a 'Source' dropdown menu set to 'FastEthernet0/0' and a 'Destination' section with an IP address of '10.1.1.0' and a Subnet Mask of '255.255.255.0' or '24'. Navigation buttons at the bottom include '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Question 5

If you click the Configure button along the top of Cisco SDM's graphical interface, which Tasks button permits you to configure such features as SSH, NTP, SNMP, and syslog?

Additional Tasks

Question 6

Cisco SDM (Security Device Manager) is a Web-based device management tool for Cisco routers that can simplify router deployments and reduce ownership costs. Select two protocols from the following to enable Cisco SDM to pull IPS alerts from a Cisco ISR router. (Choose two)

SDEE
HTTPS

Question 7

Refer to the exhibit. You are the network security administrator responsible for router security. Your network uses internal IP addressing according to RFC 1918 specifications. From the default rules shown, which access control list would prevent IP address spoofing of these internal networks?

Name/Number	Used by	Type	Description
SDM_DEFAULT_189		Extended	permit PPTP passthrough
SDM_DEFAULT_190		Extended	permit IPSec VPN pass-through, IPSec NAT
SDM_DEFAULT_191		Extended	permit DNS traffic
SDM_DEFAULT_192		Extended	permit SMTP traffic
SDM_DEFAULT_193		Extended	permit FTP traffic
SDM_DEFAULT_194		Extended	permit HTTPS traffic
SDM_DEFAULT_195		Extended	permit HTTP traffic
SDM_DEFAULT_196		Extended	deny local loopback
SDM_DEFAULT_197		Extended	deny broadcast
SDM_DEFAULT_198		Extended	deny private address space
SDM_DEFAULT_199		Extended	Broadcast that includes DHCP

Action	Source	Destination	Service	Log	Attributes
✓ Permit	any	172.16.0.0/0.0.255.255	tcp		
✓ Permit	any	any	gre		

SDM_Default_198

Explanation

Click on each access-list, in the SDM_DEFAULT_198 you will see something like this

Name/Number	Used by	Type	Description
SDM_DEFAULT_189		Extended	permit PPTP passthrough
SDM_DEFAULT_190		Extended	permit IPSec VPN pass-through, IPSec NAT
SDM_DEFAULT_191		Extended	permit DNS traffic
SDM_DEFAULT_192		Extended	permit SMTP traffic
SDM_DEFAULT_193		Extended	permit FTP traffic
SDM_DEFAULT_194		Extended	permit HTTPS traffic
SDM_DEFAULT_195		Extended	permit HTTP traffic
SDM_DEFAULT_196		Extended	deny local loopback
SDM_DEFAULT_197		Extended	deny broadcast
SDM_DEFAULT_198		Extended	deny private address space
SDM_DEFAULT_199		Extended	Broadcast that includes DHCP

Action	Source	Destination	Service	Log	Attributes
Deny	0.0.0.0/0.255.255.255	any	ip		
Deny	127.0.0.0/0.255.255.255	any	ip		
Deny	10.0.0.0/0.255.255.255	any	ip		
Deny	172.16.0.0/0.15.255.255	any	ip		
Deny	192.168.0.0/0.0.255.255	any	ip		
Deny	224.0.0.0/15.255.255.255	any	ip		
Deny	255.255.255.255	any	ip		
Permit	any	any	ip		

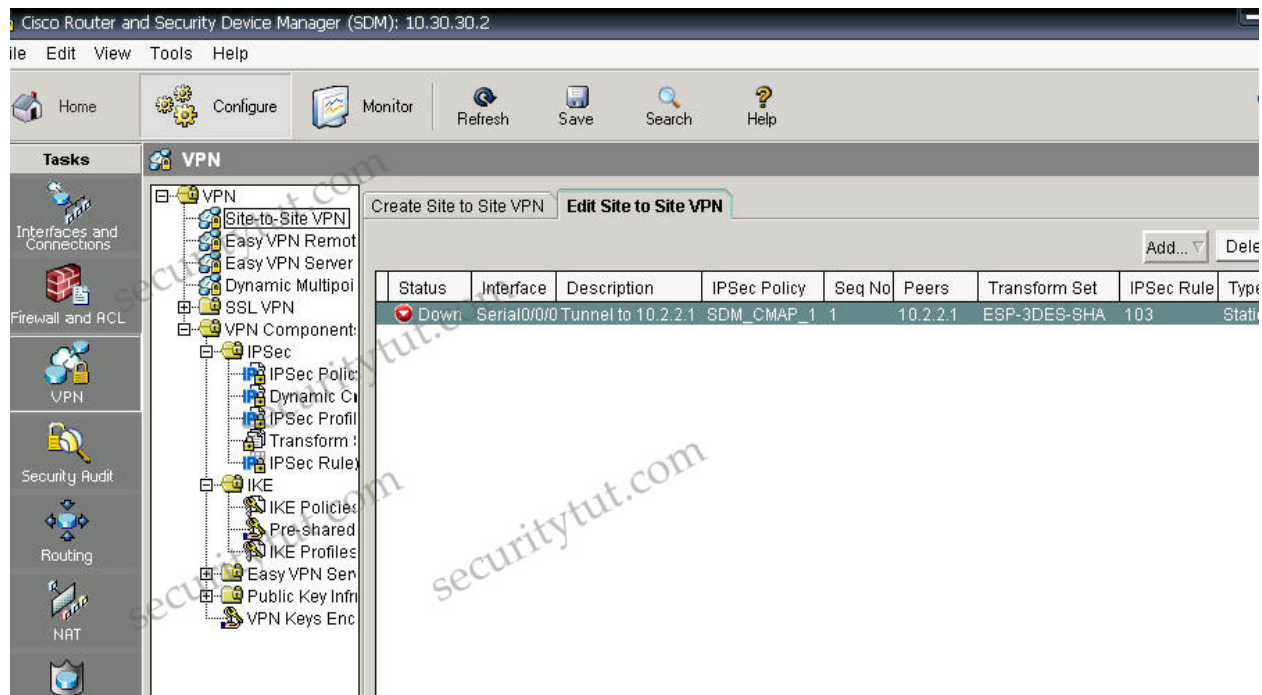
To mitigate IP address spoofing, do not allow any IP packets containing the source address of any internal hosts or networks inbound to our private network. The SDM_DEFAULT_198 denies all packets containing the following IP addresses in their source field:

- + Current network 0.0.0.0/8 (only valid as source address)
- + Any local host addresses (127.0.0.0/8)
- + Any reserved private addresses (RFC 1918, Address Allocation for Private Internets)
- + Any addresses in the IP multicast address range (224.0.0.0/4)

Note: 0.0.0.0/8: addresses in this block refer to source hosts on "this" network.
For your information, we will apply this access list to the external interface of the router.

Question 8

Refer to the exhibit. Based on the VPN connection shown, which statement is true?



Traffic that matches access list 103 will be protected.

IPsec Questions

Question 1

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec operation requires which two functions? (Choose two)

- using IKE to negotiate the SA
- using Diffie-Hellman to establish a shared-secret key

Question 2

With which three tasks does the IPS Policies Wizard help you? (Choose three)

- Selecting the interface to which the IPS rule will be applied
- Selecting the direction of traffic that will be inspected
- Selecting the Signature Definition File (SDF) that the router will use

Question 3

Examine the following options, when editing global IPS settings, which one determines if the IOS-based IPS feature will drop or permit traffic for a particular IPS signature engine while a new signature for that engine is being compiled?

Enable Engine Fail Closed

Question 4

Based on the following items, which two types of interfaces are found on all network-based IPS sensors? (Choose two)

Monitoring interface

Command and control interface

Implementing Firewall Technologies

Question 1

Which kind of table will be used by most firewalls today to keep track of the connections through the firewall?

state

Question 2

On the basis of the show policy-map type inspect zone-pair session command output provided in the exhibit. What can be determined about this Cisco IOS zone based firewall policy?

Class-map: TEST-Class (match-all)

Match: access-group 110

Match: protocol http

Inspect

Established Sessions

Session 643BCF88 (10.0.2.12:3364) =>(172.26.26.51:80) http SIS_OPEN

Created 00:00:10, Last heard 00:00:00

Bytes sent (initiator, responder) [1268:64324]

Session 643BB9C8 (10.0.2.12:3361) =>(172.26.26.51:80) http SIS_OPEN

Created 00:00:16, Last heard 00:00:06

Bytes sent (initiator, responder) [2734:38447]

Session 643BD240 (10.0.2.12:3362) =>(172.26.26.51:80) http SIS_OPEN

Created 00:00:14, Last heard 00:00:07

Bytes sent (initiator, responder) [2219:39813]

Session 643BBF38 (10.0.2.12:3363) =>(172.26.26.51:80) http SIS_OPEN

Created 00:00:14, Last heard 00:00:06

Bytes sent (initiator, responder) [2106:19895]

Class-map: class-default (match-any)

Match: any

Drop (default action)

58 packets, 2104 bytes

Stateful packet inspection will be applied only to HTTP packets that also match ACL 110.

Question 3

Which statement best describes Cisco IOS Zone-Based Policy Firewall?

The pass action works in only one direction.

Question 4

When configuring Cisco IOS Zone-Based Policy Firewall, what are the three actions that can be applied to a traffic class? (Choose three)

Pass
Inspect
Drop

Question 5

Which type of firewall is needed to open appropriate UDP ports required for RTP streams?

Stateful firewall

Question 6

What is a static packet-filtering firewall used for ?

It analyzes network traffic at the network and transport protocol layers.

Question 7

Which information is stored in the stateful session flow table while using a stateful firewall?

the source and destination IP addresses, port numbers, TCP sequencing information, and additional flags for each TCP or UDP connection associated with a particular session

Question 8

Which firewall best practices can help mitigate worm and other automated attacks?

Set connection limits

Question 9

Refer to Cisco IOS Zone-Based Policy Firewall, where will the inspection policy be applied?

to the zone-pair

Question 10

Which two actions can be configured to allow traffic to traverse an interface when zone-based security is being employed? (Choose two)

Inspect
Pass

Question 11

Which feature is a potential security weakness of a traditional stateful firewall?

It cannot detect application-layer attacks

Authentication Authorization & Accounting

Question 1

How do you define the authentication method that will be used with AAA?

With a method list

Question 2

What is the objective of the aaa authentication login console-in local command?

It specifies the login authentication method list named console-in using the local user database on the router

Question 3

Which one of the following commands can be used to enable AAA authentication to determine if a user can access the privilege command level?

aaa authentication enable default

Question 4

Which two ports are used with RADIUS authentication and authorization? (Choose two)

UDP port 1645

UDP port 1812

Question 5

Which two statements about configuring the Cisco ACS server to perform router command authorization are true? (Choose two)

In the ACS User Group setup screen, use the Shell Command Authorization Set options to configure which commands and command arguments to permit or deny.

When adding the router as an AAA client on the Cisco ACS server, choose the TACACS+ (Cisco IOS) protocol.

Question 6

What should be enabled before any user views can be created during role-based CLI configuration?

aaa new-model command

Question 7

For the following statements, which one is perceived as a drawback of implementing Fibre Channel Authentication Protocol (FCAP)?

It relies on an underlying Public Key Infrastructure (PKI)

Question 8

Has no option to authorize router commands

Encrypts the entire packet

Combines authentication and authorization functions

Uses TCP port 49

TACACS+ – Encrypts the entire packet | Uses TCP port 49

RADIUS – Has no option to authorize router commands | Combines authentication and authorization functions

Question 9

Which statement is correct regarding the aaa configurations based on the exhibit provided?

R(config)# username admin privilege level 15 secret hardtOcRackPw

R(config)# aaa new-model

```
R(config)# aaa authentication login default tacacs+
R(config)# aaa authentication login test tacacs+ local
R(config)# line vty 0 4
R(config-line)# login authentication test
R(config-line)# line con 0
R(config-line)# end
```

The authentication method list used by the vty port is named test

Question 10

Which one of the aaa accounting commands can be used to enable logging of both the start and stop records for user terminal sessions on the router?

aaa accounting exec start-stop tacacs+

Question 11

For the following items ,which one can be used to authenticate the IPsec peers during IKE Phase 1?

pre-shared key

Question 12

Which statement is true about a certificate authority (CA)?

A trusted third party responsible for signing the public keys of entities in a PKIbased system

Question 13

In computer security, AAA commonly stands for “authentication, authorization and accounting”. Which three of the following are common examples of AAA implementation on Cisco routers? (Choose three)

**authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
authenticating administrator access to the router console port, auxiliary port, and vty ports
performing router commands authorization using TACACS+**

Question 14

When configuring AAA login authentication on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can log in to the router in case the external AAA server fails?

**Local
Enable**

Securing Network Devices

Question 1

As a network engineer at securitytut.com, you are responsible for the network. Which one will be necessarily taken into consideration when implementing Syslogging in your network?

Synchronize clocks on the network with a protocol such as Network Time Protocol.

Answer: D

Question 2

Which description is correct when you have generated RSA keys on your Cisco router to prepare for secure device management?

The SSH protocol is automatically enabled.

Question 3

As a candidate for CCNA examination, when you are familiar with the basic commands, if you input the command “enable secret level 5 password” in the global mode, what does it indicate?

The enable secret password is for accessing exec privilege level 5.

Question 4

Please choose the correct description about Cisco Self-Defending Network characteristics.

INTEGRATED – Enabling elements in the networks to be a point of policy enforcement

COLLABORATIVE – Interaction amongst services and devices to mitigate attacks

ADAPTIVE – Security technologies that evolve with emerging attacks

Question 5

Which three items are Cisco best-practice recommendations for securing a network? (Choose three)

Routinely apply patches to operating systems and applications.

Disable unneeded services and ports on hosts.

Require strong passwords, and enable password expiration.

Question 6

Given the exhibit below. You are a network manager of your company. You are reading your Syslog server reports. On the basis of the Syslog message shown, which two descriptions are correct? (Choose two)

Feb 1 10:12:08 PST: %SYS-5-CONFIG_1: Configured from console by vty0 (10.2.2.6)

This message is a level 5 notification message.

Service timestamps have been globally enabled.

Question 7

Examine the following items, which one offers a variety of security solutions, including firewall, IPS, VPN, antispypware, antivirus, and antiphishing features?

Cisco ASA 5500 series security appliance

Question 8

For the following items, which management topology keeps management traffic isolated from production traffic?

OOB

Question 9

Information about a managed device resources and activity is defined by a series of objects. What defines the structure of these management objects?

MIB

Question 10

Which item is correct regarding Cisco IOS IPS on Cisco IOS Release 12.4(11)T and later?

uses Cisco IPS 5.x signature format

Question 11

If a switch is working in the fail-open mode, what will happen when the switch's CAM table fills to capacity and a new frame arrives?

A copy of the frame is forwarded out all switch ports other than the port the frame was received on.

Question 12

What is the purpose of the secure boot-config global configuration?

takes a snapshot of the router running configuration and securely archives it in persistent storage

Question 13

What Cisco Security Agent Interceptor is in charge of intercepting all read/write requests to the rc files in UNIX?

Configuration interceptor

Question 14

Which two statements are correct regarding a Cisco IP phone's web access feature? (Choose two)

It is enabled by default.

It can provide IP address information about other servers in the network.

Question 15

When configuring role-based CLI on a Cisco router, which action will be taken first?

Enable the root view on the router

Question 16

Which key method is used to detect and prevent attacks by use of IDS and/or IPS technologies?

Signature-based detection

Question 17

Which one of the following items may be added to a password stored in MD5 to make it more secure?

Salt

Modern Network Security Threats

Question 1

Which item is the great majority of software vulnerabilities that have been discovered?

Buffer overflows

Question 2

Which statement is true about vishing?

Influencing users to provide personal information over the phone

Question 3

In a brute-force attack, what percentage of the keyspace must an attacker generally search through until he or she finds the key that decrypts the data?

Roughly 50 percent

Question 4

Observe the following options carefully, which two attacks focus on RSA? (Choose all that apply.)

BPA attack

Adaptive chosen ciphertext attack

Drag and Drop Questions

Question 1

On the basis of the description of SSL-based VPN, place the correct descriptions in the proper locations.

The authentication process uses hashing technologies

You can also use the application programming interface to extensively modify the SSL client software for use in special applications

Asymmetric algorithms are used for authentication and key exchange

SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router

Symmetric algorithms are used for bulk encryption

SSL-based VPNs

Place here

Place here

Place here

Answer:

- + The authentication process uses hashing technologies.
- + Asymmetric algorithms are used for authentication and key exchange.
- + Symmetric algorithms are used for bulk encryption.

Question 2

Which three common examples are of AAA implementation on Cisco routers? Please place the correct descriptions in the proper locations.

- performing router commands authorization using TACACS+
- authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- tracking Cisco Netflow accounting statistics
- securing the router by locking down all unused services
- implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
- authenticating administrator access to the router console port, auxiliary port, and vty ports

The common examples of AAA implementation

- Place here*
- Place here*
- Place here*

Answer:

- + performing router commands authorization using TACACS+
- + authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- + authenticating administrator access to the router console port, auxiliary port, and vty ports

Question 3

Drag two characteristics of the SDM Security Audit wizard on the above to the list on the below.

requires users to first identify which router interfaces connect to the inside network and which connect to the outside network

has two modes of operation interactive and non-interactive

uses interactive dialogs and prompts to implement role-based CLI

automatically enables Cisco IOS firewall and Cisco IOS IPS to secure the router

displays a screen with Fix-it check boxes to let you choose which potential security-related configuration changes to implement

Drag the items to the proper locations

Place here

Place here

Answer:

+ requires users to first identify which router interfaces connect to the inside network and which connect to the outside network

+ displays a screen with Fix-it check boxes to let you choose which potential security-related configuration changes to implement

Question 4

On the basis of the Cisco IOS Zone-Based Policy Firewall, by default, which three types of traffic are permitted by the router when some interfaces of the routers are assigned to a zone?

Drag three proper characterizations on the above to the list on the below.

- traffic flowing to the zone member interface that is returned traffic
- traffic flowing among the interfaces that are members of the same zone
- traffic flowing among the interfaces that are not assigned to any zone
- traffic flowing to and from the router interfaces (the self zone)
- traffic flowing between a zone member interface and any interface that is not a zone member

Drag the items to the proper locations

- Place here
- Place here
- Place here

Answer:

- + traffic flowing among the interfaces that are members of the same zone
- + traffic flowing among the interfaces that are not assigned to any zone
- + traffic flowing to and from the router interfaces (the self zone)

Question 5

Drag three proper statements about the IPsec protocol on the above to the list on the below.

IPsec is a framework of open standards.

IPsec is bound to specific encryption algorithms, such as 3DES and AES.

IPsec ensures data integrity by using checksums.

IPsec authenticates users and devices that can carry out communication independently.

IPsec is implemented at Layer 4 of the OSI model.

IPsec uses digital certificates to guarantee confidentiality.

Drag the items to proper locations

Place here

Place here

Place here

Answer:

Three correct statements are:

- + IPsec is a framework of open standards.
- + IPsec ensures data integrity by using checksums.
- + IPsec authenticates users and devices that can carry out communication independently.

Access list Questions

Question 1

Which statement best describes the Turbo ACL feature? (Choose all that apply)

The Turbo ACL feature processes ACLs into lookup tables for greater efficiency.

The Turbo ACL feature leads to reduced latency, because the time it takes to match the packet is fixed and consistent.

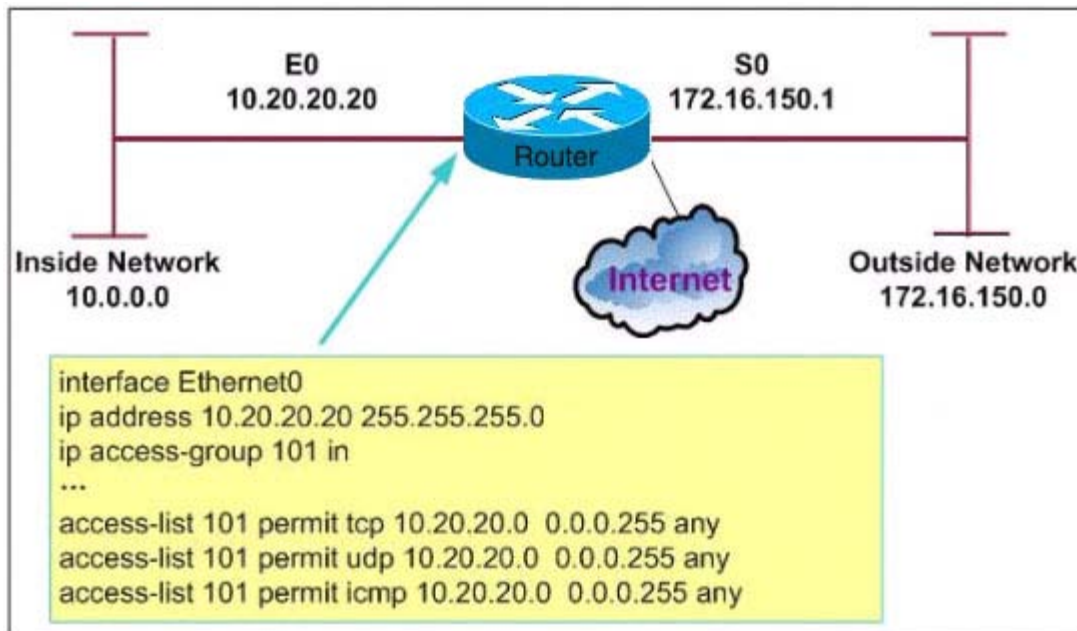
Question 2

Which statement best describes configuring access control lists to control Telnet traffic destined to the router itself

The ACL should be applied to all vty lines in the in direction to prevent an unwanted user from connecting to an unsecured port.

Question 3

Which description is correct based on the exhibit and partial configuration?



Access-list 101 will prevent address spoofing from interface E0.

Question 4

Examine the following options, which access list will permit HTTP traffic sourced from host 10.1.129.100 port 3030 destined to host 192.168.1.10

access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 3030 192.168.1.0 0.0.0.15 eq www

Question 5

Which three statements about applying access control lists to a Cisco router are true? (Choose three)

Place more specific ACL entries at the top of the ACL.

Router-generated packets cannot be filtered by ACLs on the router.

If an access list is applied but is not configured, all traffic will pass.

Question 6

A standard access control list has been configured on a router and applied to interface Serial 0 in an outbound direction. No ACL is applied to Interface Serial 1 on the same router. What will happen when traffic being filtered by the access list does not match the configured ACL statements for Serial0?

The traffic is dropped.

Question 7

Which location will be recommended for extended or extended named ACLs?

a location as close to the source traffic as possible

Security Fundamentals

Question 1

Which classes does the U.S. government place classified data into? (Choose three)

Confidential

Secret

Top-secret

Question 2

Which method is of gaining access to a system that bypasses normal security measures?

Creating a back door

Question 3

Which statement is true about a Smurf attack?

It sends ping requests to a subnet, requesting that devices on that subnet send ping replies to a target system.

Question 4

With the increasing development of network, various network attacks appear. Which statement best describes the relationships between the attack method and the result?

Ping Sweep – Determine live hosts | Identify devices

Port Scan – Identify operating systems | Determine potential vulnerabilities | Identify active services

Question 5

Which one is the most important based on the following common elements of a network design?

Business needs

Question 6

How does CLI view differ from a privilege level?

A CLI view supports only commands configured for that specific view, whereas a privilege level supports commands available to that level and all the lower levels.

Question 7

What are four methods used by hackers? (Choose four)

social engineering attack

Trojan horse attack

privilege escalation attack

footprint analysis attack

Question 8

Which protocol will use a LUN as a way to differentiate the individual disk drives that comprise a target device

SCSI

Question 9

Which VoIP components can permit or deny a call attempt on the basis of a network's available bandwidth?

Gatekeeper

Question 10

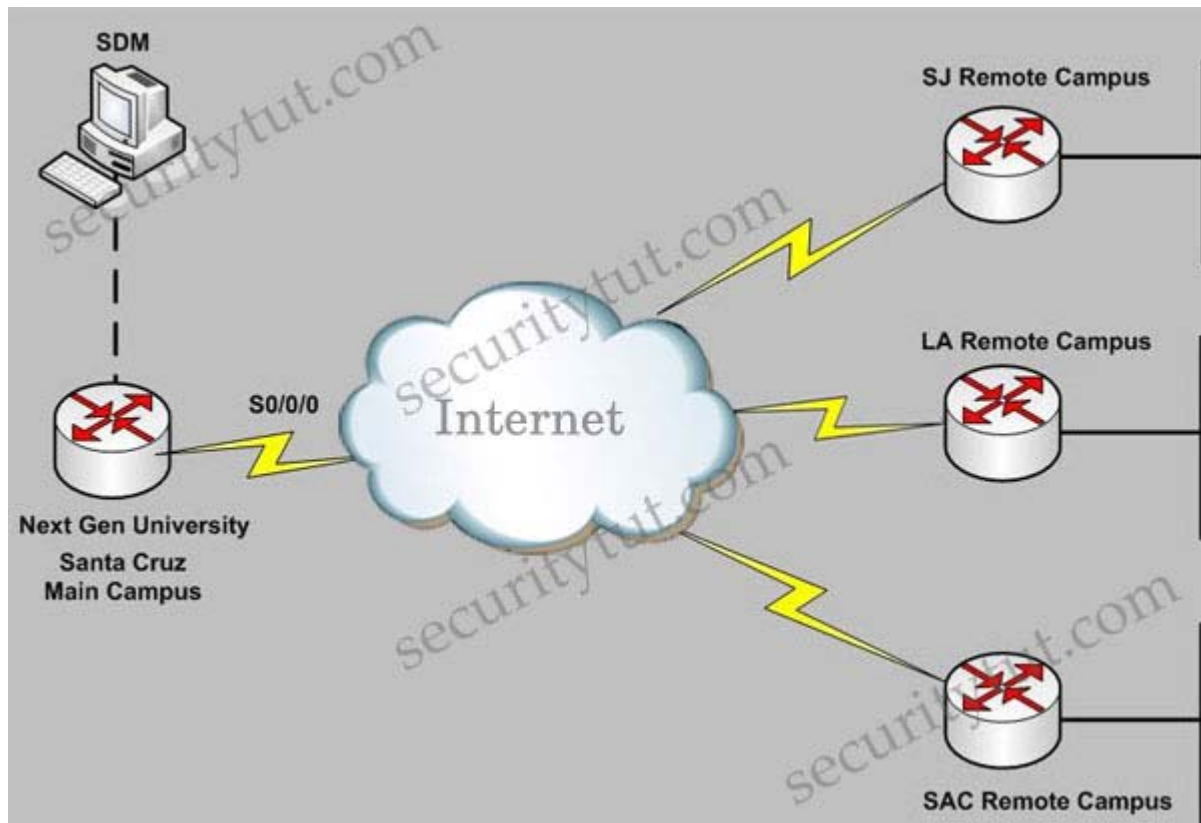
Which option ensures that data is not modified in transit

Integrity

LabSim Category

Site-to-site VPN SDM Lab Sim

Question



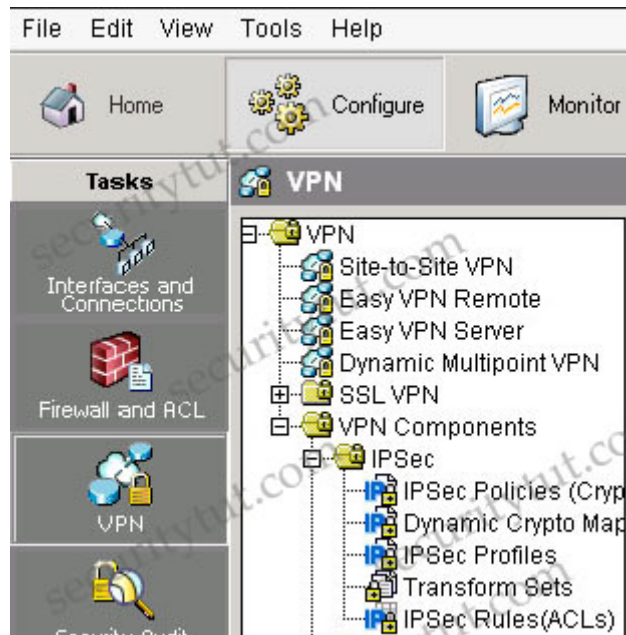
Next Gen University main campus is located in Santa Cruz. The University has recently established various remote campuses offering e-learning services. The University is using Ipsec VPN connectivity between its main and remote campuses San Jose(SJ), Los Angeles(LA), Sacramento(SAC). As a recent addition to the IT/Networking team, you

have been tasked to document the Ipsec VPN configurations to the remote campuses using the Cisco Router and SDM utility. Using the SDM output from VPN Tasks under the Configure tab to answer this question.

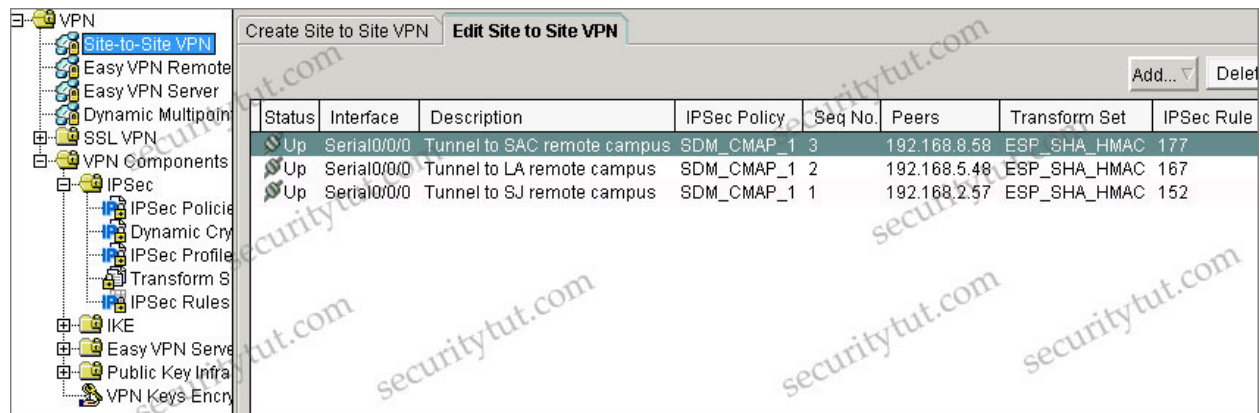
Note:

Before reading the answers and explanations, you can try answering these 4 questions. Below are the screenshots that are necessary to answer all the questions.

Click on the Configure tab on the top menu and then click on the VPN tab on the left-side menu to see these tabs



+ Tab VPN\Site-to-Site VPN (notice: you have to click on the “Edit Site to Site VPN” tab to see the image below



+ Tab VPN\VPN Components\IPsec\IPsec Policies

VPN

IPSec Policies [Add...] [Edit...] [Delete]

Name	Type
SDM_CMAP_1	IKE

Crypto Maps in this IPSec Policy

Name	Seq No	Peers	Transform Set	IPSec Rule	PFS
SDM_CMAP_1	3	192.168.8.58	ESP-3DES-SHA2	177	
SDM_CMAP_1	2	192.168.5.48	ESP-3DES-SHA1	167	
SDM_CMAP_1	1	192.168.2.57	ESP-3DES-SHA	152	

Dynamic Crypto Map Sets in this IPsec Policy

Dynamic Crypto Map Set Name	Seq No.	Type

- + Tab Dynamic Crypto is empty so there is no screenshot for this tab
- + Tab IPSec Profiles is empty so there is no screenshot for this tab
- + Tab VPN\VPN Components\IPSec\Transform Sets

VPN

Transform Set

Name	ESP Encryption	ESP Integrity	AH Integrity	IP Compression	Mode	Type
ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC			TUNNEL	User Defined
ESP-3DES-SHA2	ESP_3DES	ESP_SHA_HMAC			TUNNEL	User Defined
ESP-3DES-SHA1	ESP_3DES	ESP_SHA_HMAC			TUNNEL	User Defined

+ Tab VPN\VPN Components\IPSec\IPSec Rules

The screenshot shows the Cisco VPN configuration interface. On the left is a tree view of the VPN configuration hierarchy, with 'IPSec Rules(ACLs)' selected. The main area displays the 'IPSec Rules' configuration table. Below the table is a summary table showing the rule's action, source, destination, and service.

Name/Number	Used by	Type	Description
152	crypto map SDM_CMAP_1 1	Extended	
167	crypto map SDM_CMAP_1 2	Extended	
177	crypto map SDM_CMAP_1 3	Extended	

Action	Source	Destination	Service	Log	Attributes	Description
✓ Permit	10.10.10.0/0.0.0.255	10.2.54.0/0.0.0.255	ip			IPsec Rule

The screenshot shows the Cisco VPN configuration interface with a different rule selected. The tree view on the left is the same, but the main area shows a different rule configuration. The summary table below the table indicates the rule's action, source, destination, and service.

Name/Number	Used by	Type	Description
152	crypto map SDM_CMAP_1 1	Extended	
167	crypto map SDM_CMAP_1 2	Extended	
177	crypto map SDM_CMAP_1 3	Extended	

Action	Source	Destination	Service	Log
✓ Permit	192.168.8.58	10.8.75.0/0.0.0.255	ip	

Question 1

Which one of these statements is correct in regards to Next Gen University Ipsec tunnel between its Santa Cruz main campus and its SJ remote campus?

It is using Ipsec tunnel mode to protect the traffic between the 10.10.10.0/24 and the 10.2.54.0/24 subnet.

Explanation

From the Site-to-site VPN tab, we specify that the SJ's IP address is 192.168.2.57 with IPsec Rule of 152. Click on the IPsec Rules group to see what rule 152 is -> rule 152 is permit source 10.10.10.0/24 to destination 10.2.54.0/24.

Status	Interface	Description	IPsec Policy	Seq No.	Peers	Transform Set	IPsec Rule
Up	Serial0/0/0	Tunnel to SAC remote campus	SDM_CMAP_1	3	192.168.8.58	ESP_SHA_HMAC	177
Up	Serial0/0/0	Tunnel to LA remote campus	SDM_CMAP_1	2	192.168.5.48	ESP_SHA_HMAC	167
Up	Serial0/0/0	Tunnel to SJ remote campus	SDM_CMAP_1	1	192.168.2.57	ESP_SHA_HMAC	152

Name/Number	Used by	Type	Description
152	crypto map SDM_CMAP_1 1	Extended	
167	crypto map SDM_CMAP_1 2	Extended	
177	crypto map SDM_CMAP_1 3	Extended	

Action	Source	Destination	Service	Log	Attributes	Description
Permit	10.10.10.0/0.0.0.255	10.2.54.0/0.0.0.255	ip			IPsec Rule

Also, in the description of the above tab, we can see "Tunnel to SJ remote campus" -> it uses Tunnel mode (although it is only the description and can be anything but we can believe it uses Tunnel mode). If you don't want to accept this explanation then have a look at the IPsec Policy & Seq No. columns, which are SDM_CMAP_1 & 1. Click on the VPN Components\IPsec\IPsec Policies group we will learn the corresponding Transform Set is ESP-3DES-SHA. Then click on the Transform Sets group we can see the corresponding mode is TUNNEL.

Question 2

Which one of these statements is correct in regards to Next Gen University Ipsec tunnel between its Santa Cruz main campus and its SAC remote campus?

Only the ESP protocol is being used; AH is not being used.

Explanation

“Only the ESP protocol is being used; AH is not being used” is correct as we can see there is no AH configured under AH Integrity column in the VPN Components\IPSec\Transform Sets group (while in the ESP Integrity column it is ESP_SHA_HMAC).

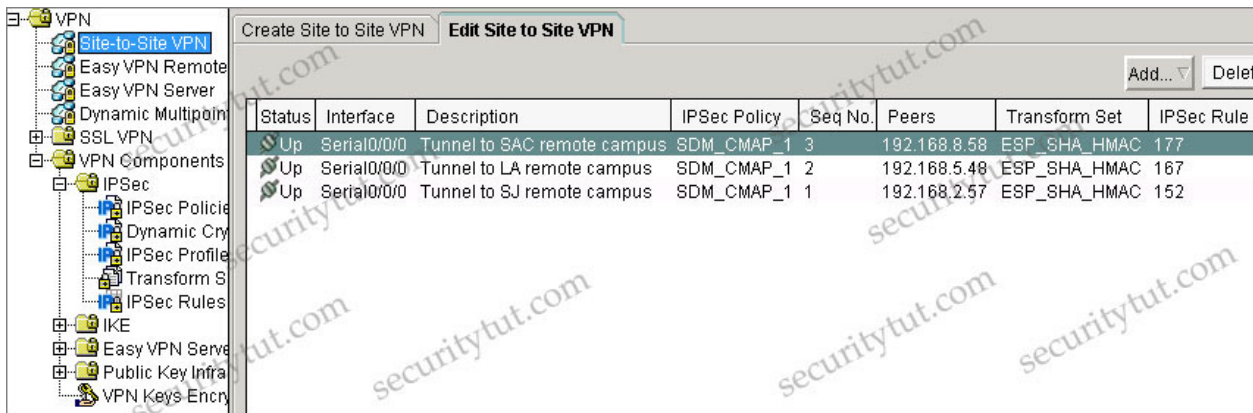
Question 3

Which of these is used to define which traffic will be protected by IPsec between the Next Gen University Santa Cruz main campus and its SAC remote campus?

ACL 177

Explanation

In the VPN\Site-to-site-VPN group we can easily see the SAC remote campus is protected by IPsec rule 177, which is an access-list



The screenshot shows the Cisco VPN configuration interface. On the left is a tree view with 'VPN' expanded to 'Site-to-Site VPN'. The main pane shows a table of tunnels under the 'Edit Site to Site VPN' tab.

Status	Interface	Description	IPSec Policy	Seq No.	Peers	Transform Set	IPSec Rule
Up	Serial0/0/0	Tunnel to SAC remote campus	SDM_CMAP_1	3	192.168.8.58	ESP_SHA_HMAC	177
Up	Serial0/0/0	Tunnel to LA remote campus	SDM_CMAP_1	2	192.168.5.48	ESP_SHA_HMAC	167
Up	Serial0/0/0	Tunnel to SJ remote campus	SDM_CMAP_1	1	192.168.2.57	ESP_SHA_HMAC	152

Question 4

The Ipsec tunnel to the SAC remote campus terminates at which IP address, and what is the protected subnet behind the SAC remote campus router? (Choose two)

192.168.8.58

10.8.75.0/24

Explanation

The screenshot shows the Cisco SDM VPN configuration interface. On the left is a tree view of VPN components, with 'IPSec Rules(ACLs)' selected. On the right, the 'IPSec Rules' table is displayed. Below the table is a detailed view of a selected rule.

Name/Number	Used by	Type
152	crypto map SDM_CMAP_1 1	Extended
167	crypto map SDM_CMAP_1 2	Extended
177	crypto map SDM_CMAP_1 3	Extended

Action	Source	Destination	Service	Log
✓ Permit	192.168.8.58	10.8.75.0/0.0.0.255	ip	

Zone-based Firewall SDM Simlet

Instructions

To access the Cisco Router and Security Device Manager(SDM) utility click on the console host icon that is connected to a ISR router. You can click on the grey buttons below to view the different windows. Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar. The "Tab" key and most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation.

Question 1

Which two options correctly identify the associated interface with the correct security zone? (Choose two)

- FastEthernet0/1 is associated to the "out-zone" zone.**
- FastEthernet0/0 is associated to the "in-zone" zone.**

Explanation

Under the Additional Tasks, click on the Zones group. At the right side box we will see the FastEthernet0/0 is assigned to the in-zone and the FastEthernet0/1 is assigned to the out-zone.

Name	Associated Interfaces	Associated Zone Pairs
Outside		
out-zone	FastEthernet0/1	sdm-zp-self-out, sdm-zp-out-self, sdm-zp-in-out
in-zone	FastEthernet0/0	sdm-zp-in-out
Inside		

(Notice: In the real exam, you might see more zones than the image above)

Question 2

Which statement is correct regarding the “sdm-permit” policy map?

Traffic matching the “sdm-access” traffic class will be inspected.

or

Traffic matching the “SDM_CA_SERVER” traffic class will be dropped.

Explanation

This class-map will drop all the traffic that is not matched with the SDM_CA_SERVER class-map (it works in the same way as the implicit “deny all” line at the end of each access list). Therefore traffic not matched by any of the class maps within that policy map will be dropped.

Question 3

Which three protocols are matched by the “sdm-cls-insp-traffic” class map? (Choose three)

sql-net

pop3

ftp

Explanation

Click on the C3PL\Class Map\Inspection group and click on the sdm-cls-insp-traffic line at the upper right side box to see which protocols are matched by the “sdm-cls-insp-traffic” class map.

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
Class Map
QoS Class Map
Inspection
Deep Packet Inspection
Parameter Map
Configuration Management

Inspect Class Maps Add...

Class Map Name	Used By
sdm-protocol-imap	sdm-inspect
sdm-access	
sdm-cls-protocol-im	
sdm-protocol-im	sdm-inspect
sdm-cls-insp-traffic	
CLASS_MAP_IN_TO_OUT	POLICY_MAP_IN_TO_OUT
sdm-protocol-http	sdm-inspect
sdm-icmp-access	sdm-permit-icmpreply

Details of Class Map: sdm-cls-insp-traffic

Item Name	Item Value
Match Protocol	dns
Match Protocol	https
Match Protocol	icmp
Match Protocol	imap
Match Protocol	pop3
Match Protocol	tcp
Match Protocol	udp
Match Protocol	sql-net
Match Protocol	cuseeme
Match Protocol	h323
Match Protocol	netshow
Match Protocol	shell
Match Protocol	realmedia
Match Protocol	rtsp
Match Protocol	sntp
Match Protocol	streamworks
Match Protocol	tftp
Match Protocol	vdolive
Match Protocol	ftp

Question 4

Within the “sdm-permit” policy map, what is the action assigned to the traffic class “class-default”?

drop

Explanation

Under the C3PL\Policy Map\Protocol Inspection group we can see the policy maps, which class-maps and which actions are assigned to the class-maps.

Additional Tasks

Protocol Inspection Policy Maps

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

Details of Policy Map: sdm-permit

Match Class Name	Action
SDM_CA_SERVER	Pass
class-default	Drop

Question 5

Which policy map is associated to the “sdm-zp-in-out” security zone pair?

sdm-inspect

Explanation


There are 2 places where you can get information about the policy map associated to the “sdm-zp-in-out” security zone pair:

+ At the “Home” tab (you might click on the to see the Firewall policies)

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

About Your Router Host Name: R6



Cisco 3725

Hardware		Software	
More ...		More ...	
Model Type:	Cisco 3725	IOS Version:	12.4(15)T7
Available / Total Memory(MB):	2/128 MB	SDM Version:	2.4
Total Flash Capacity:	16 MB		
Feature Availability: ✔ Firewall ✔ VPN ✔ IPS ✔ NAC ✔			

Configuration Overview [View Running Config](#)

Interfaces and Connections ✔ Up (2) ✘ Down (0)

Total Supported LAN: 2 **Total Supported WAN:** 0
Configured LAN Interface: 2 **Total WAN Connections:** 0
DHCP Server: 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

+ At the Zone-pair group in the Additional Tasks

Additional Tasks

Zone Pairs Add..

Zone Pair	Source	Destination	Policy
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

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

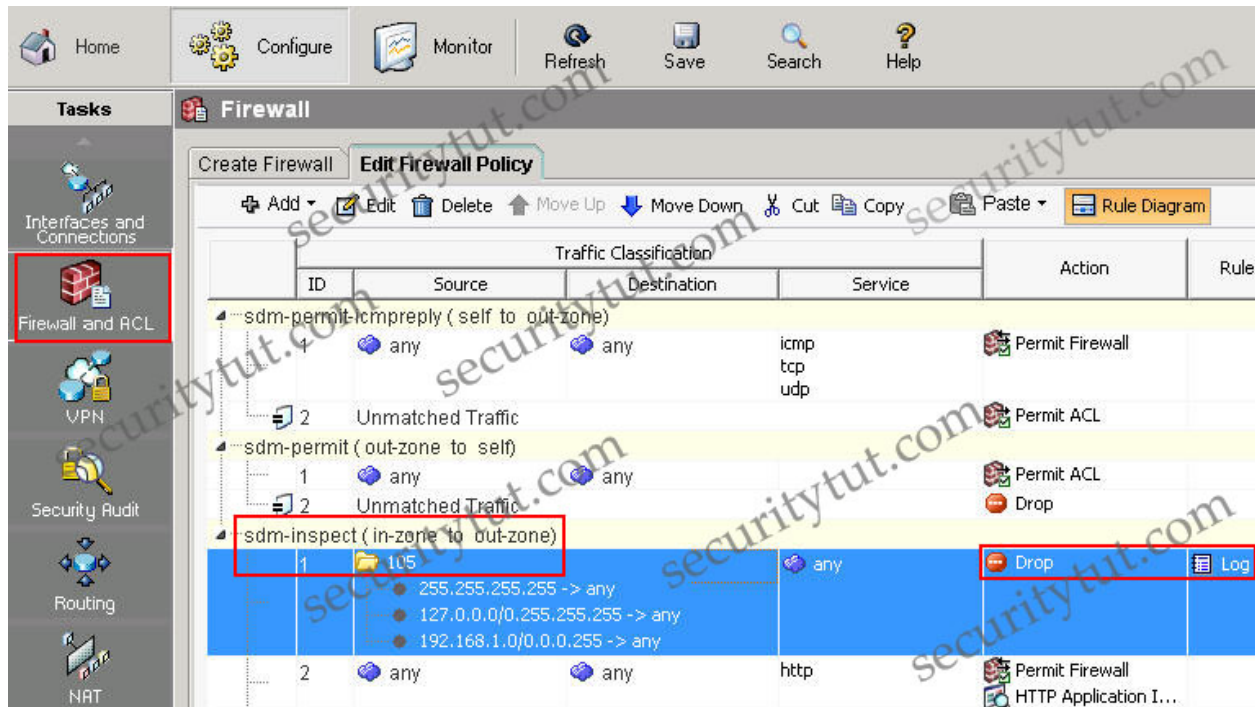
Question 6

Within the “sdm-inspect” policy map, what is the action assigned to the traffic class “sdm-invalid-src”, and which traffic is matched by the traffic class “sdm-invalid-src” ? (Choose two)

**traffic matched by ACL 105
 drop/log**

Explanation

Under the “Firewall and ACL” tab, search for the “sdm-inspect” policy map we can see the access list 105 is used by this policy map. We can also see the action assigned to the traffic class “sdm-invalid-src” (drop/log).



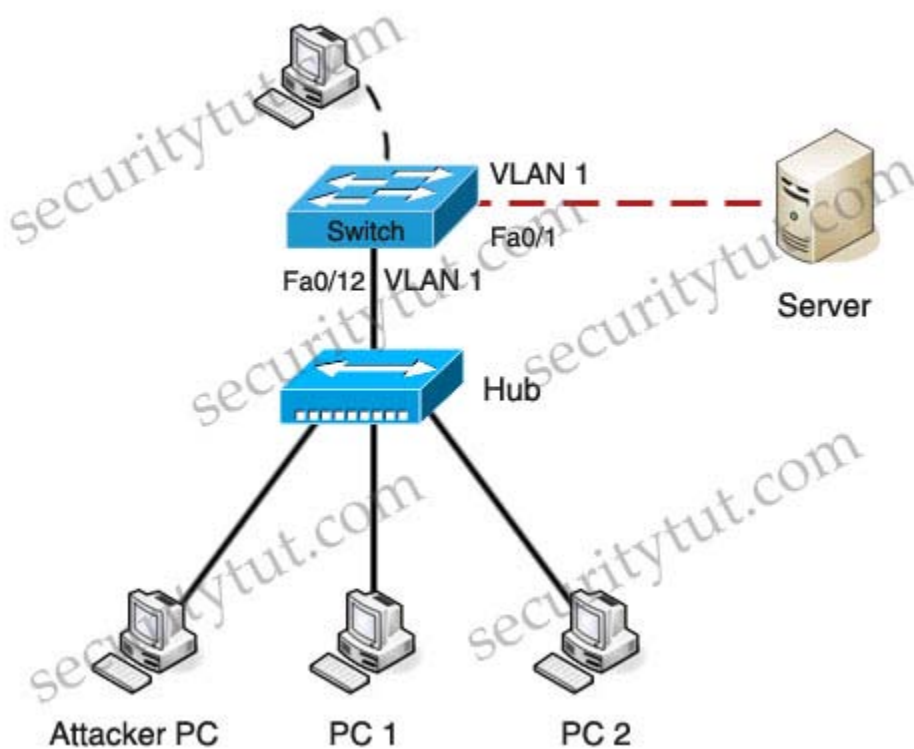
Notice that the Access list number can be also seen in the C3PL\Class Map\Inspection and the Drop/log action can be seen in the C3PL\Policy Map\Protocol Inspection group.

Port Security Lab Sim

Question

You are the network security administrator for Big Money Bank Co. You are informed that an attacker has performed a CAM table overflow attack by sending spoofed MAC addresses on one of the switch ports. The attacker has since been identified and escorted out of the campus. You now need to take action to configure the switch port to protect against this kind of attack in the future.

For purposes of this test, the attacker was connected via a hub to the Fa0/12 interface of the switch. The topology is provided for your use. The enable password of the switch is cisco. Your task is to configure the Fa0/12 interface on the switch to limit the maximum number of MAC addresses that are allowed to access the port to two and to shutdown the interface when there is a violation.



Answer and Explanation

The purpose of this sim is straightforward:
Limit the maximum number of MAC addresses that are allowed to access the port to two.
Shutdown the interface when there is a violation.

Please remember that we have to access interface Fa0/12 to fulfill the requirements. Before making any configuration, we should use the show running-config to check the status of interface Fa0/12

```
Switch>enable  
Password: cisco
```

```
Switch#show running-config
```

```
Switch#show running-config  
<output omitted>  
!  
Interface FastEthernet0/12  
!  
<output omitted>
```

The interface Fa0/12 hasn't been configured with anything.

```
Switch#configure terminal
Switch(config)#interface fa0/12
Switch(config-if)#switchport mode access
```

First, enable the “port security” feature on this interface:

```
Switch(config-if)#switchport port-security
```

Set the maximum number of secure MAC addresses for this interface to 2:

```
Switch(config-if)#switchport port-security maximum 2
```

Shutdown if the security is violated:

```
Switch(config-if)#switchport port-security violation shutdown
Switch(config-if)#no shutdown
Switch(config-if)#end
```

Now you should check if the configuration is correct or not by typing the command show port-security interface fa0/12

```
Switch#show port-security interface fa0/12
```

```
Switch# show port-security interface fa0/12
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 2
```

Notice that the parameters should be like this:

- + Port Security: Enabled
- + Violation Mode: Shutdown
- + Maximum MAC Address: 2

Save the configuration

```
Switch#copy running-config startup-config
```

Just for your information, when the security is violated the port is in the error-disabled state. We can bring it out of this state by entering the “errdisable recovery cause psecure-violation” global configuration command or we can manually re-enable it by entering the “shutdown” and “no shutdown” commands in the interface configuration.

Prepared by: venerzky

