642-511 (CSVPN)

TestKing's Cisco Secure Virtual Private Networks

Version 23.0

Important Note, Please Read Carefully

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.

Further Material
For this test TestKing also plans to provide:
* Online Testing. Check out an Online Testing at
http://www.testking.com/index.cfm?pageid=724

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 your member zone at TestKing an update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to www.testking.com
2. Click on **Member zone/Log in**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

For most updates, it is enough just to print the new questions at the end of the new version, not the whole document.

Feedback
Feedback on specific questions should be send to feedback@testking.com. You should state: Exam number and version, question number, and login ID.

Our experts will answer your mail promptly.

Copyright

Table of contents

Total number of questions: 256

Topic 1, Overview of Virtual Private Networks and IPSec Technologies (24 questions)

Section 1: Cisco products enable a secure VPN (2 questions)

QUESTION NO: 1
What is the maximum number of simultaneous sessions that can be supported when doing encryption in hardware within the Cisco VPN Concentrator series of products?

A. 100
B. 1500
C. 5000
D. 10000
E. infinite

Answer: D
Explanation:

The Cisco VPN 3000 Series Concentrator comes in a variety of models that can support small offices of 100 of fewer VPN connections to large enterprises of 10,000 or more simultaneous VPN connections. Redundant and nonredundant configuration are available to help ensure the high reliability of these devices.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.30

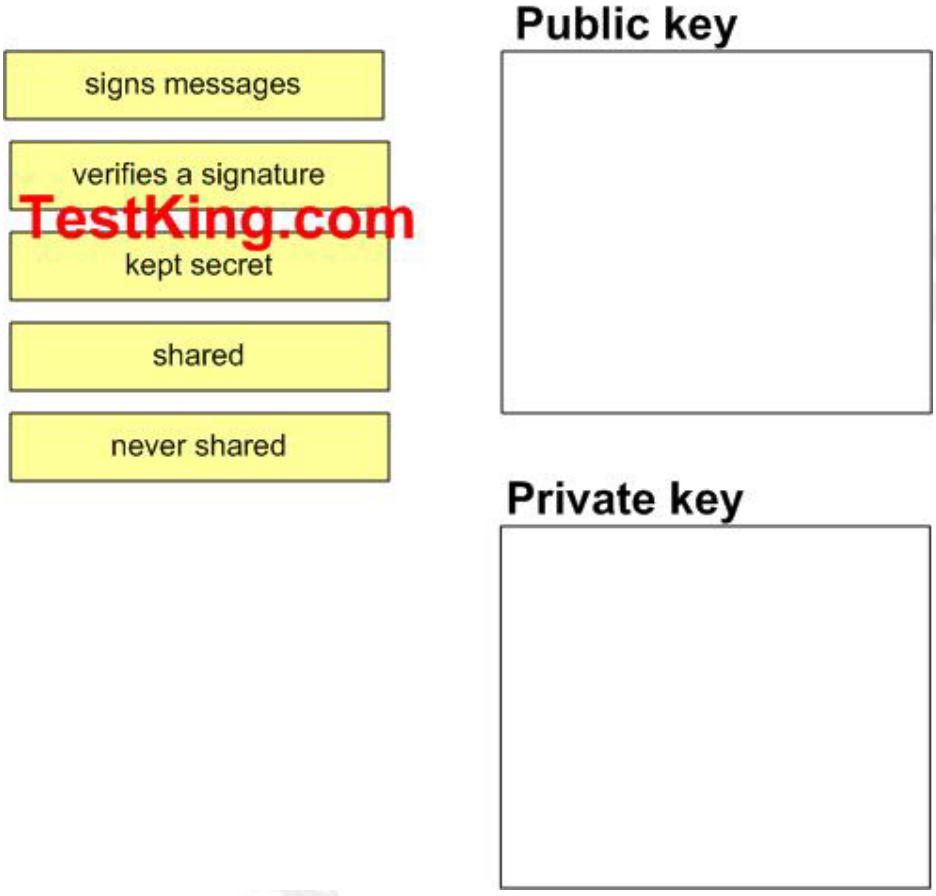
QUESTION: 2
Which of the following operating systems can run the software VPN client? Choose all that apply.

A. linux
B. mac
C. windows
D. solaris

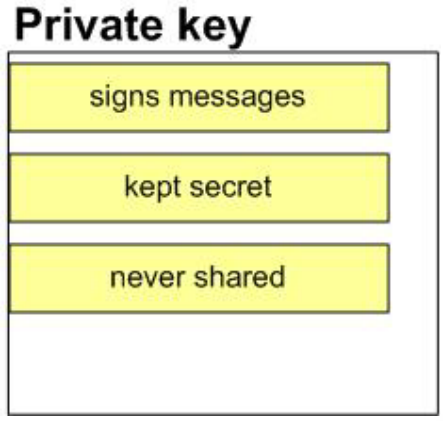
Answer: A,B,C,D
Explanation:
There are VPN software clients available for Windows, Solaris, Linux, and Macintosh.

Section 2: IPSec overview (9 questions)

QUESTION NO:1
Jason from the security department was given the assignment to match the Cisco VPN key with its description.



Answer:



Explanation:
The Diffie-Hellman (D-H) key agreement is a public key encryption method that provides a way for two IPSec peers to establish a shared secret key that only they know, although they communicating over an insecure channel.
With D-H, each peer generates a public and private key pair. The private key generated by each peer is kept secret and never shared. The public key is calculated from the private key by each peer and is exchanged over the insecure channel. Each peer combines the other's public key with its own private and computes the shared secret key number exchanged over the insecure channel.

Reference: Cisco Secure Virtual Private Network (Ciscopress) page 18-20

QUESTION NO: 2
John asked Kathy from the security department about authentication and encryption. John wants to know when both authentication and encryption are selected in the virtual IP address, which is performed first at the originating end. What was Kathy's answer?

A. Encryption was Kathy's answer
B. Tunnel was Kathy's answer.

C. Transport was Kathy's answer
D. Authentication was Kathy's answer

Answer: A
Explanation:
When both encryption and authentication are selected, encryption is performed frist, before authentication. One reason for this order of processing is that it facilitates rapid detection and rejection of replayed or bogus packets by the receiving node.

Reference: Cisco Secure Virtual Private Networks (Ciscopress) page 15

QUESTION NO: 3
James the security administrator at Testking Inc. is working on encryption. He needs to know what type of keys does DES and 3DES require for encryption and decryption.

A. DES and 3DES require Elliptical curve keys for encryption and decryption
B. DES and 3DES require Exponentiation keys for encryption and decryption
C. DES and 3DES require Symmetrical keys for encryption and decryption
D. DES and 3DES require Asymmetrical keys for encryption and decryption

Answer: C
Explanation:
des
3des

Specifies the symmetric encryption algorithm used to protect user data transmitted between two IPSec peers. The default is 56-bit DES-CBC, which is less secure and faster than the alternative.

QUESTION NO: 4
Which of the following are the types of keys RSA use for encryption and decryption?

A. exponentiation keys
B. symmetrical keys
C. asymmetrical keys
D. elliptical curve keys

Answer: C
Explanation: There are two types of cryptographic keys; public keys -- sometimes called asymmetric key -- and symmetric keys. RSA and Diffie-Hellman are common public key algorithms and RC4, DES and IDEA common symmetric key algorithms. You cannot directly compare public key lengths (for example RSA keys) with symmetric key lengths (DES, RC4); this is an important point which confuses many people

QUESTION NO: 5
Which Cisco VPN feature will permit the sender to encrypt packets before transmitting them across a network?

A. The anti-replay feature
B. The data confidentially feature
C. The data integrity feature
D. The data original authentication feature

Answer: B
Explanation:

Data Confidentiality.The IPSec **sender** can **encrypt** packets **before transmitting** them **across** a **network**.

- Data Integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that the data has not been altered during transmission.
- Data Origin Authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service is dependent upon the data integrity service.
- Anti-Replay—The IPSec receiver can detect and reject replayed packets.
  With IPSec, data

QUESTION NO: 6
What AES encryption bits lengths can you use on your Concentrator ESP IPSEC VPN? Choose all that apply.

A. 56
B. 128
C. 192
D. 256
E. 1024

Answer: B,C,D
Explanation:
Advanced Encryption Standard (AES) can be used in 128, 192, and 256 bit encryption lengths in ESP when using IPSEC on your Concentrator.

QUESTION NO: 7

Which of the following are ISAKMP hash protocols? Choose all that apply.

A. NAT
B. IKE
C. DES
D. SHA
E. MD5

Answer: D,E
Explanation:
You can use SHA and MD5 for HMAC authentication.

QUESTION NO: 8
Which of the following can be IPSEC termination endpoints? Choose all that apply.

A. IOS Router
B. PIX Firewall
C. Concentrator
D. IDS Sensor

Answer: A,B,C
Explanation:
These Cisco products can all terminate IPSEC, meaning they are actually involved in the IPSEC encryption/decryption process, not just passing VPN encrypted traffic.

QUESTION: 9
What size is the encryption key used in 3DES?

A. 128 bits
B. 168 bits
C. 128 bytes
D. 168 bytes

Answer: B
Explanation:
3DES uses a 56 bit key, 3 times, for an effective throughput of 168 bits encryption.

Section 3: IPSec protocol framework (7 questions)

QUESTION NO: 1
Which of the following has the lowest encryption bit length?

A. SHA
B. MD5
C. DES
D. AES
E. ESP

Answer: C
Explanation:
Data Encryption Standard (DES) uses only a 56 bit key to encrypt data, and is easily broken.

QUESTION NO: 2
What is the key size of Diffie-Hellman group 2?

A. 128 bits
B. 256 bits
C. 512 bits
D. 1024 bits

Answer: D
Explanation:
Diffie-Hellman is used to create a completely secure secret key, over a completely insecure link, using highly complex mathematical algorithms safe from brute force even if sniffers are on the line

QUESTION NO: 3
What benefit does ESP have, that AH does not?

A. authentication
B. encryption
C. tunnel mode
D. md5 hash

Answer: B
Explanation:
Authentication Header does not have any way of encrypting data, ESP does.

QUESTION NO: 4
Using which of the following protocols with AH will cause packet failure?

A. AYT
B. VRRP
C. NAT
D. CDP

Answer: C
Explanation:
You cannot translate an IP address in AH authenticated packet because AH uses that field when calculating authentication. This will cause then other end of the VPN tunnel to drop all packets because they will not authenticate properly.

QUESTION NO: 5
How big is the SPI field in an IPSEC header?

A. 2 bytes
B. 4 bytes
C. 8 bytes
D. 24 bytes

Answer: B
Explanation:
The Security Parameter Index (SPI) field identifies a Security Association between two IPSEC endpoints. The field is 32 bits long (4 bytes).

QUESTION NO: 6
Which of the following peer authentication methods scales the worst?

A. digital certificates
B. SCEP
C. preshared keys
D. encrypted nonces

Answer: C
Explanation:
A preshared key peer authentication method does not scale well because each key needs to be entered manually at each peer participating in the VPN.

QUESTION NO: 7
What is the protocol number that denotes AH is in use?

A. 17
B. 51
C. 89
D. 123

Answer: B
Explanation:
The Authentication Header protocol is protocol number 51.

Section 4: How IPSec works (6 questions)

QUESTION NO: 1
Jason the security administrator at Testking Inc. was given the assignment to match the following order.
In IPSec main mode, match the two-way exchange between the initiator and receiver with their descriptions.

Answer:

Explanation:
Main Mode

Main mode provides a way to establish the first phase of an IKE SA, which is then used to negotiate future communications. The first step, securing an IKE SA, occurs in three two-way exchanges between the sender and the receiver. In the first exchange, the sender and receiver agree on basic algorithms and hashes. In the second exchange, public keys are sent for a Diffie-Hellman exchange. Nonces (random numbers each party must sign and return to prove their identities) are then exchanged. In the third exchange, identities are verified, and each party is assured that the exchange has been completed.

Reference: Reference: Cisco Secure Virtual Private Network (Ciscopress) page 27

QUESTION NO: 2
James the security administrator for Testking Inc. is working with IKE. His job is to know what the three functions of IKE Phase 2 are. (Choose three)

A. IKE uses aggressive mode.
B. IKE can optionally performs an additional DH exchange.
C. IKE periodically renegotiates IPSec SAs to ensure security.
D. IKE Negotiates IPSec SA parameter protected by an existing IKE SA.
E. IKE verifies the other side's identity.
F. IKE uses main mode.

Answer: B C D
Explanation:
Step 2 Determine IPSec (IKE Phase Two) Policy
- Negotiates IPSec SA parameters protected by an existing IKE SA
- Establishes IPSec security associations
- Periodically renegotiates IPSec SAa to ensure security
- Optionally performs an additional Diffie-Hellman

Reference: Cisco Secure Virtual Private Networks (Ciscopress) page 28

QUESTION NO: 3
Jane is the security administrator at Testking Inc. and is working on understanding more about IPSec. Jane wants to know what IPSec does at the network layer?

A. IPSec at the network layer enables Cisco VPN.
B. IPSec at the network layer generates a private DH key.
C. IPSec at the network layer encrypts traffic between secure IPSec gateways.
D. IPSec at the network layer protects and authenticates IP packets between IPSec devices.

Answer: D
Explanation:
IPSec protects sensitive data that travels across unprotected networks. IPSec security services are provided at the network layer, so you do not have to configure individual workstations, PCs, or applications.

QUESTION NO: 4
Which of the following functions are fulfilled by IPSec at the network layer?

A. enables Cisco VPN
B. generates a private DH key
C. encrypts traffic between secure IPSec gateways
D. protects and authenticates IP packets between IPSec devices

Answer: D
Explanation:

Once the IPSec SAs have been established , secured traffic can be exchanged over the connection. IP packets across this IPSec tunnel are authenticated and/or encrypted, depending on the transform set selected.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.371

QUESTION NO: 5
What protocol number indicates ESP?

A. 50
B. 145
C. 429
D. 500

Answer: A
Explanation:
Encapsulating Security Payload uses protocol number 50.

QUESTION NO: 6
What is the UDP port used for ISAKMP?

A. 50
B. 51
C. 500
D. 510

Answer: C
Explanation:
ISAKMP uses UDP port 500.

Topic 2, Cisco Virtual Private Network 3000 Concentrator Series Hardware (20 questions)

Section 1: Overview of the Cisco VPN 3000 Concentrator Series (14 questions)

QUESTION NO: 1
James the security administrator for Testking Inc. is working on VPNs. IF the VPN is owned and managed by the Testking Inc. corporate security, which product would he choose?

A. 2900
B. 3030
C. 3660
D. PIX Firewall 500
E. PIX Firewall 515

Answer: E
Explanation:
A is clearly incorrect because the 2900 is a Catalyst Switch (Layer 2) and cannot offer any VPN functionality. B and E are the only options available, and D just refers to the 500 PIX, when there are different flavors of the 500, like the retired 520, 501, 506E, 515E, 525 and 535.

QUESTION NO: 2
James the security administrator for Testking Inc. is working on the Cisco VPN 3005. His job is to know the hardware and which feature is supported on the Cisco VPN 3005.

A. Cisco VPN 3005 supports up to 3 network ports.
B. Cisco VPN 3005 hardware is upgradeable.
C. Cisco VPN 3005 supports up to 100 sessions.
D. Cisco VPN 3005 64 MB of memory is standard.

Answer: C
Explanation:
Model 3005
- Software-based encryption
- Single power supply

- Expansion capabilities:
  -----Optional WAN interface module with dual T1/E1 ports
  All systems feature:
- 10/100Base-T Ethernet interfaces (autosensing)
  -----Model 3005: Two interfaces
  -----Models 3015-3080: Three interfaces
- Motorola® PowerPC CPU
- SDRAM memory for normal operation
- Nonvolatile memory for critical system parameters
- Flash memory for file management

QUESTION NO: 3
Jason the security administrator at Testking Inc. is working on the Cisco VPN Concentrator. His job is to know the Cisco VPN Concentrator series of products. He needs to know what is the maximum number of site-to-site tunnels supported.

A. 1500 site-to-site tunnels
B. 1000 site-to-site tunnels
C. 500 site-to-site tunnels
D. 100 site-to-site tunnels

Answer: B
Explanation:

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Maximum LAN-to-LAN Sessions	100	100	500	1000	1000

QUESTION NO: 4
James the security administrator at Testking Inc. is working on knowing the Cisco security products. He must choose what product fits best for Testking Inc. network. If the primary role of the VPN product is to perform remote access VPN with a few site-site connections, which product should James choose?

A. James will choose the PIX Firewall 515
B. James will choose the 2900
C. James will choose the 3030
D. James will choose the 3660

Answer: A
Explanation:

PIX Firewall 515

- Supports IKE and IPsec VPN standards
- Ensures data privacy/integrity and strong authentication to remote networks and remote users over the Internet
- Supports 56-bit DES, 168-bit 3DES, and up to 256-bit AES data encryption to ensure data privacy

This is the best answer. You would want to use a dedicated Firewall with VPN capabilities as the secondary use.

Note: If security manages the VPN, the PIX Firewall may be the solution of choice.

QUESTION NO: 5
How many connections can a Cisco VPN 3060 support simultaneously?

A. 100
B. 1000
C. 1500
D. 5000
E. none of the above

Answer: D
Explanation:

- VPN 3030 is for medium- to large-sized organizations with bandwidth requirements from full T1/E1 through T3/E3 (50 Mbps max. performance) and up to 1500 simultaneous sessions; field-upgradeable to the Cisco VPN 3060
- VPN 3060 is for large organizations, with high-performance, high-bandwidth requirements from fractional T3 through full T3/E3 or greater (100 Mbps max. performance) and up to 5000 simultaneous remote access sessions
- Both have specialized SEP modules to perform hardware-based acceleration

QUESTION NO: 6
What 3000 Series Concentrators are sold with unlimited VPN software client licenses? Choose all that apply.

A. 3015
B. 3030

C. 3060
D. 3080

Answer: A, B, C, D
Explanation: As long as you use the Cisco VPN client to connect to Cisco products, you can install it on an unlimited number of computers.
Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_user_guide_book09186a00800e6e04.html

QUESTION NO: 7
Which of the following is not a 3000 series Concentrator?

A. 3005
B. 3015
C. 3030
D. 3050
E. 3080

Answer: D
Explanation:
The five 3000 series Concentrator models are the 3005, 3015, 3030, 3060, and the 3080.

QUESTION NO: 8
Which of the following are NOT tabs under the 3000 series Concentrator Administration screen? Choose all that apply.

A. events
B. access rights
C. system reboot
D. encryption
E. logs
F. ping
G. software update

Answer: A,D,E
Explanation:
There are 8 tabs under the Administration screen. They are Administer Sessions, Software Update, System Reboot, Ping, Monitoring Refresh, Access Rights, File Management, and Certificate Management.

QUESTION NO: 9
Which of the following are Ethernet ports on a Concentrator? Choose all that apply.

A. Inside
B. Outside
C. Default
D. Internal
E. External
F. Public
G. Private

Answer: E,F,G
Explanation:
The three 10/100 mb Ethernet ports on a 3000 series Concentrator are Public, Private, and External.

QUESTION NO: 10
How much RAM does a 3080 Concentrator have?

A. 128mb
B. 192mb
C. 256mb
D. 384mb

Answer: C
Explanation:
A 3080 Concentrator comes standard with 256mb of RAM.

QUESTION NO: 11
How much Ethernet traffic is a 3060 Concentrator capable of encrypting in mb/second?

A. 4
B. 20
C. 50
D. 100

Answer: D
Explanation:
Using Scalable Encryption Processors (SEP) the 3060 and 3080 can encrypt up to 100mb/second Ethernet traffic.

QUESTION NO: 12
What is the maximum number of user sessions the 3080 Concentrator can simultaneously support?

A. 5,000
B. 10,000
C. 20,000
D. 50,000

Answer: B
Explanation:
The 3080 can support up to 10,000 user sessions (not tunnels).

QUESTION NO: 13
How many 10/100mb Ethernet ports are on the 3002 Hardware Client for local lan connections?

A. 4
B. 8
C. 12
D. 16

Answer: B
Explanation:
There are 8 10/100mb Ethernet ports for the local LAN users on the 3002 Hardware Client.

QUESTION NO: 14
How many SEP modules does a 3060 Concentrator ship with?

A. &#048
B. 1
C. 2
D. 3
E. 4

Answer: C
Explanation:
A 3060 comes standard with two Scalable Encryption Processors (SEP's).

Section 2: Cisco VPN 3000 Concentrator (4 questions)

QUESTION NO: 1
How do you enter interface IP addresses on a Concentrator?

A. configuration, system, interfaces
B. configuration, system, general
C. configuration, interfaces
D. configuration, system, general, interfaces

Answer: C
Explanation:
Concentrator interface configuration is done from configuration, interfaces.

QUESTION NO: 2
What are the hardware encryption modules used by 3000 series Concentrators?

A. AYT's
B. VRP's
C. PRI's
D. SEP's

Answer: D
Explanation:
The hardware encryption modules used by the 3000 series Concentrators are called Scalable Encryption Processors (SEP's).

QUESTION NO: 3
John the security administrator for Testking is working on SEP Redundancy. With SEP redundancy, of the top SEP fails and the bottom SEP takes over, which statement is true?

A. The true statement is all sessions are lost.
B. The true statement is the operator intervention is required.
C. The true statement is no sessions are lost.
D. The true statement is only the Cisco VPN 3080 supports SEP redundancy.

Answer: C
Explanation:
The VPN Concentrator can contain up to four SEP or SEP-E modules for maximum system throughput and redundancy. Two SEP modules provide maximum throughput; additional

modules provide redundancy in case of module failure. SEP redundancy requires no configuration: it is always enabled and completely automatic; no administrator action is required. If a SEP module fails, the VPN Concentrator automatically switches active sessions to another SEP module. If the system has only one SEP module and it fails, the sessions automatically use software cryptographic functions. Even if a SEP module fails, the VPN Concentrator supports the number of sessions for which it is licensed.

Reference: VPN 3000 Concentrator Ref Volume 2. Configuration 4.0.pdf

QUESTION NO: 4
John the security administrator at Testking Inc. is working on connections to the PIX. For SSH connections to the PIX which of the following are true?

A. PIX only supports SSH V.1
B. You must upgrade DES to 3DES
C. PIX only supports SSH V.2
D. PIX supports SSH V.1 & V.2
E. You must configure RSA keys to allow SSH

Answer: A

Section 3: Cisco VPN 3000 Concentrator Series Client support (2 questions)

QUESTION NO: 1
How many administrator levels is the Hardware Client capable of supporting?

A. 1
B. 2
C. 3
D. 4
E. 5

Answer: E
hardware client supports 5 administrator levels

QUESTION NO: 2
What is the maximum number of simultaneous sessions supported when doing encryption in software within a CPN Concentrator series of products?

A. 1
B. 100
C. 1500
D. 5000

Answer: B

Explanation:

The Cisco VPN 3000 Concentrator Series Supports the Entire Range of Enterprise Applications

	Cisco VPN 3005	Cisco VPN 3015	Cisco VPN 3020	Cisco VPN 3030	Cisco VPN 3060	Cisco VPN 3080
Simultaneous IPSec Remote Access Users[1]	200	100	750	1,500	5,000	10,000
Simultaneous WebVPN (Clientless) Users[2]	50	75	200	500	500	500
Maximum LAN-to-LAN Sessions	100	100	250	500	1,000	1,000
Encryption Throughput	4 Mbps	4 Mbps	50 Mbps	50 Mbps	100 Mbps	100 Mbps

Encryption Method	SW	SW	HW	HW	HW	HW
Available Expansion Slots	0	4	1	3	2	0
Encryption (SEP) Module	0	0	1	1	2	4
Redundant SEP	-	-	Option	Option	Option	Yes
System Memory	32/64 MB (fixed)	128 MB	256 MB	128/256 MB	256/512 MB	256/512 MB
Hardware Configuration	1U	Scalable 2U	Fixed 2U	Scalable 2U	Scalable 2U	Fixed 2U
Dual Power Supply	Single	Option	Option	Option	Option	Yes
Client License	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited

Topic 3: Configuring the Cisco VPN 3000 Series Concentrator for Remote Access Using Pre-shared Keys (35 questions)

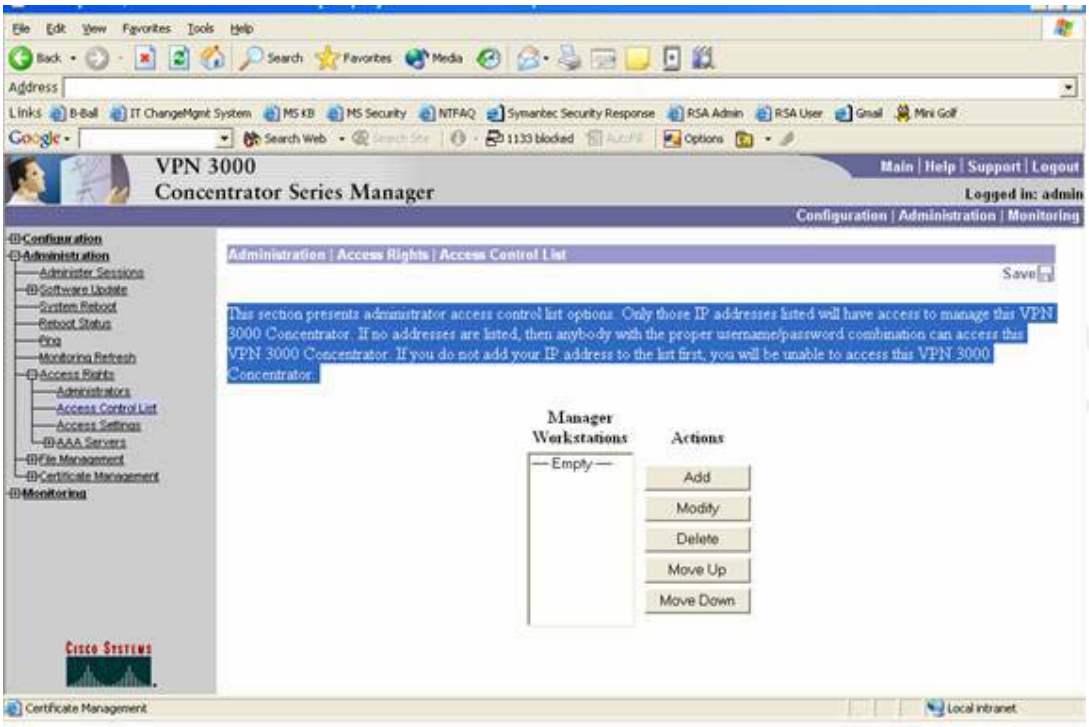
Section 1: Overview of remote access using pre-shared keys (1 question)

QUESTION NO: 1
Which of the following events follows a scenario where no systems are on the ACL of the Cisco 3000 VPN?

A. No access or rights are issued.
B. No management rights are invoked.
C. Anyone who knows the Cisco VPN 3000 Concentrator IP address and the administrator username and password combination can gain access.
D. No one who knows the Cisco VPN 3000 Concentrator IP address and the administrator username and password combination can gain access.

Answer: C

This section presents administrator access control list options. Only those IP addresses listed will have access to manage this VPN 3000 Concentrator. If no addresses are listed, then anybody with the proper username/password combination can access this VPN 3000 Concentrator. If you do not add your IP address to the list first, you will be unable to access this VPN 3000 Concentrator.


File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Links B-Ball IT ChangeMgmt System MS KB MS Security NTFAQ Symantec Security Response RSA Admin RSA User Gmail Mini Golf
Google Search Web 1133 blocked Options
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Administration
Administer Sessions
Software Update
System Reboot
Reboot Status
Ping
Monitoring Refresh
Access Rights
Administrators
Access Control List
Access Settings
AAA Servers
File Management
Certificate Management
Monitoring
Administration | Access Rights | Access Control List
Save
This section presents administrator access control list options. Only those IP addresses listed will have access to manage this VPN 3000 Concentrator. If no addresses are listed, then anybody with the proper username/password combination can access this VPN 3000 Concentrator. If you do not add your IP address to the list first, you will be unable to access this VPN 3000 Concentrator.
Manager Workstations
Actions
— Empty —
Add
Modify
Delete
Move Up
Move Down
Cisco Systems
Certificate Management
Local intranet

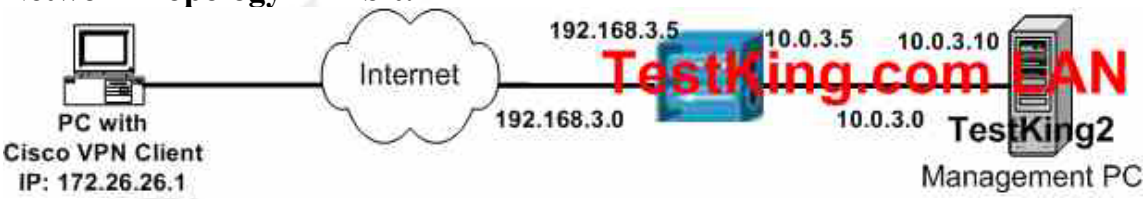
Section 2: Initial configuration of the Cisco VPN 3000 Concentrator Series for remote access (8 questions)

QUESTION NO: 1
What protocol restrictions does the Cisco VPN Concentrator impose in a background of configuring remote access protocols under quick configuration?

A. no protocol restrictions
B. IPSec plus one other access protocol
C. only one access protocol per group
D. any two access protocols per group

Answer: A
Configuration | Quick | Protocols
_ PPTP
_ L2TP
_ IPSec – Check to enable remote user connections via IPSec. LAN-to-LAN configurations are done outside of Quick Configuration.
-> All protocols are available in Quick Configuration (no restrictions -> A).
The only restriction is, that not all modes of the protocols (LAN-to-LAN on IPSec) are quick configurable.

QUESTION NO: 2
Network Topology Exhibit:



Parameter exhibit:

User name:	**TestKingCFO**
User password:	**cfotestking**
Group Name	**TestKing2**
Group Password	**TestKingGroup**
Filter	**Public**
Admin username	**testkingadmin**
Admin password	**testkingadmin**
Corporate Network	**10.0.3.0**
Subnet Mask	**255.255.255.0**
Bandwidth Policy Name	**TestKing Policy**
Bandwidth Reservation	**512 kbps**

Bandwidth Reservation Interface Public

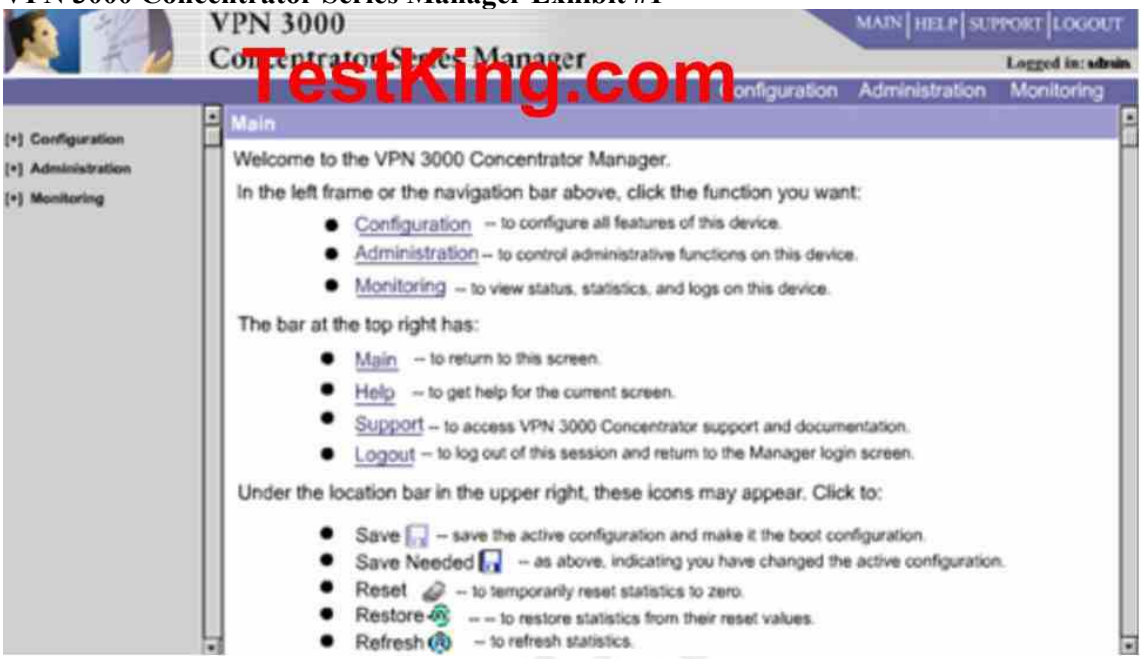
Scenario:

You work as a network administrator at the TestKing.com Rio de Janeiro office. TestKing uses a Cisco VPN 3000 Concentrator to provide remote access to the Rio de Janeiro employees. The CIO has decided that the company executives (CFOs) must be ensured to receive a minimum of bandwidth when they connect to the corporate TestKing network remotely.
You are required to configure a new group and a new user on the concentrator so that the CFOs receives a minimum amount of bandwidth when connecting to the TestKing corporate network. Furthermore, the configuration must be implemented at the group level and on the public interfaces.
If the devices are configured in an appropriate manner, you should be able to partly verify your configuration by establishing a tunnel from the Cisco VPN client to the TestKing corporate network.

To begin the simulation you launch the browser from the TestKing2 Management PC, then you enter the correct IP address in the browser to access the Concentrator.

Note: Not all functions of the concentrator are available in this simulation. Nevertheless, all functions to complete the required task are available.

VPN 3000 Concentrator Series Manager Exhibit #1



VPN 3000 Concentrator Series Manager Exhibit #2

VPN 3000 Concentrator Series Manager Exhibit #3

VPN 3000 Concentrator Series Manager Exhibit #4

VPN 3000 Concentrator Series Manager Exhibit #5

Answer:

1. Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add
 - Policy Name: TestKing Policy
 - Check: Bandwidth Reservation: 512kbps
 - Click "Add"
2. Configuration | Interfaces | Ethernet 2 | Bandwidth
 - Check: Bandwidth Management
 - Bandwidth Policy: Select "TestKing Policy" from the drop down.
 - Click "Apply"
3. Configuration | User Management | Users | Add
 - "testkingadmin" for user and "testkingadmin" for password
 - Group: Select "TestKing2" group from drop down.
4. Configuration | User Management | Groups | Highlight the "TestKing2" Group, click "Bandwidth Assignment"
 - Select "Ethernet 2"
 - Policy: Select "TestKing Policy" from the drop down.
 - Enter 512kpbs for "Bandwidth Aggregation"
 - Click "Apply"

QUESTION NO: 3
Study the Exhibit below carefully:

TestKing utilizes the Cisco VPN 3000 Concentrator to provide remote access to its employees. The decision has been made to allow the Executives of the company to connect to the Internet unencrypted while traffic destined for the corporate network will still need to be encrypted using the Cisco VPN Client Firewall is required on the Cisco VPN Client and the default CPP policy is enforced. These configuration features need to be implemented at the group level.

Your assignment is to configure the concentrator to accomplish this task. Make use of the following parameters when performing this task:

User Name—**CFO**
User Password—**password**
Group Name—**TK3**
Group Password—**TK3group**
Admin Username—**testking**
(Default)
Admin Password—**testking**

Corporate Network—**10.0.3.0**
Subnet Mask—**255.255.255.0**
Network List Name—**Corporate Network**
Firewall—**Cisco Integrated Client Firewall**
CPP Policy—**Firewall Filter for VPN client**

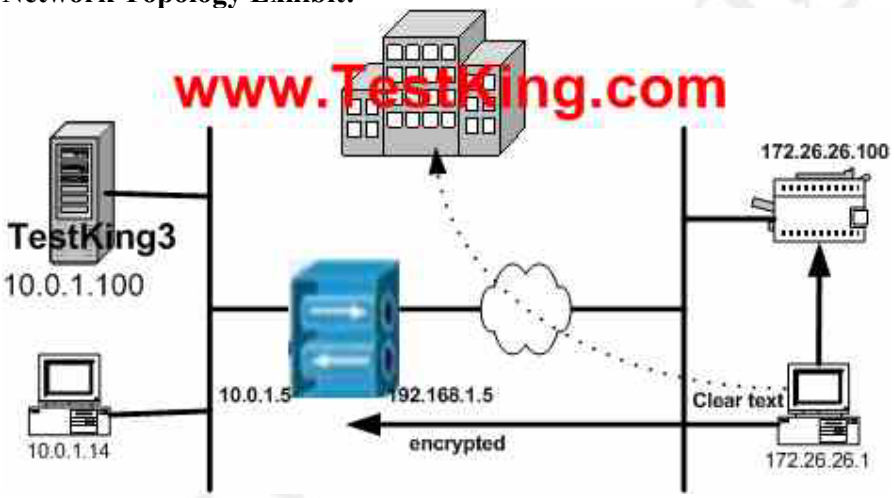
You may commence the simulation by launching the browser from the Management PC and entering the correct IP address in the browser to access the concentrator.
In this simulation not all functions on the concentrator are available, but all functions necessary to complete the task are implemented.

Answer:
Configuration|User Management|Groups
1. Click on add new group
2. Under Identity
   Group Name = TK3
   Password = TK3group
   Type = internal
3. Under General Tab check IPSEC and uncheck Inherit
4. Under IPSEC Tab choose Tunnel Type = Remote Access
   Mode Configuration = check
   Authentication = Internal
5. Under Client Config Tab
   Select Only Tunnel networks in the list
6. Under FW Tab
   Firewall required button
   Firwall = Cisco INtegrated Client Firewall

Vendor ID = 1
Product ID = 1
Firewall Policy = Policy Pushed
Select FIrewall Filter for VPN Client

7. Under HW Client Tab
   Check Required Individual User Authentication
8. Go to Configuration|User Management|Users
9. Click on Add
10. Under Identity
    User Name = CFO
    Password = password
    Group = TK3

QUESTION NO: 4
Network Topology Exhibit:



Network Lists Exhibits: *MISSING*

IP Addressing scheme Exhibit:

Home printer:	**172.26.26.100**
Concentrator public interface:	**192.168.1.5**
Concentrator private interface:	**10.0.1.5**
Corporate application server:	**10.0.1.100**

You work as a network administrator at the TestKing.com Madrid office. TestKing is migrating its Madrid-based traveling salesmen from dial-in to Virtual Private Networking (VPN). These traveling salesmen must be able to access

- **the TestKing corporate server via a secure link.**
  More specifically, they must be able to access the TestKing application server TestKing3, IP address 10.0.1.100, via an encrypted tunnel.

- **the local TestKing Madrid LAN via clear text.**
  More specifically, they must be able to access the TestKing home office printer, IP address 172.26.26.100, via clear text.
- **the web via clear text.**

TASK: You are required to configure the Cisco VPN 3000 Concentrator to meet the requirements of the TestKing Madrid traveling salesmen.

Answer:
1. Configuration | User Management | Groups | Add
2. Identity Tab: Group Name: TK_Madrid, password: tkpassword, Type: "Internal"
3. General Tab: IPSec, uncheck "Inherit"
4. IPSec Tab: Authentication: Internal, uncheck "Inherit"
5. Client Config Tab:
 - Split Tunnel Policy: Only Tunnel networks in the list, Uncheck "Inherit"
 - Split Tunneling Network List (missing exhibit) Pick the one that includes 10.0.1.x/24 network. Uncheck "Inherit"
6. Finally click on "Add"
** No mention of Firewall options in the question, so those options were ignored.

QUESTION NO: 5
Which of the following represents a limitation when using Quick Configuration?

A. It enables you to define attributes only on a global basis.

B. It enables you to define attributes only on an authentication server basis.

C. It enables you to define attributes only on an individual basis.

D. It enables you to define attributes only on a client basis.

Answer: A
Explanation:
Quick configuration supplies the minimal parameters needed to make the VPN Concentrator operational, while the Main menu lets you configure all the features of the VPN 3000 Concentrator. For example, a configured remote user with a PC and modem can use Microsoft PPTP (point-to-point tunneling protocol) and a local ISP to connect securely—in a VPN tunnel through the Internet—with resources on a private, internal corporate network.

QUESTION NO: 6
True or false: There is an out-of-band management channel?

A. True
B. False

Answer: A
Yes there is an RJ-45 console port with full RS-232 signals. The unit comes with cables and adapters for DB-25 and DB-9.

QUESTION NO: 7
What is the default username and password on a 3000 series Concentrator?

A. user, password
B. admin, password
C. it, login
D. admin, admin

Answer: D
Explanation:
The 3000 series Concentrator default login is username admin, password admin.

QUESTION NO: 8
Which method uses the Cisco VPN 3000 Concentrator to assign IP addresses from an internal pool when you have been asked to configure address assignments?

A. remote client pool
B. per-user
C. configured pool
D. DHCP pool

Answer: C
Explanation:

After you have selected the protocol to use, you must select the method the VPN concentrator is to use to assign an address to clients as they establish tunnels with the concentrator. You could select multiple methods; the concentrator tries each method in order until it is successful in assigning an address to the client.
The methods are tried in the order listed:

1) Client Specified
2) Per User
3) DHCP
4) Configured Pool

Reference: CCSP VPN Ciscopress p.148

Section 3: Browser configuration of the Cisco VPN 3000 Series Concentrator (3 questions)

QUESTION NO: 1
Greg the security administrator at Testking Inc. is working on configuring the group VPN Client attributes in the VPN Concentrator. He needs to know which three are the VPN Client firewall settings. (Choose three)

A. Click the radio button to select enable content filtering
B. Click the radio button to select enable CBAC
C. Click the radio button to select no firewall
D. Click the radio button to select enable authentication proxy
E. Click the radio button to select firewall required
F. Click the radio button to select firewall optional

Answer: C E F
Explanation:
Click the radio button to select a firewall setting:
• **No Firewall** = No firewall is required for remote users in this group.
• **Firewall Required** = All remote users in this group must use a specific firewall. Only those users with the designated firewall can connect.
• **Firewall Optional** = All remote users in this group can connect. Those that have the designated firewall can use it. Those who do not have a firewall receive a warning message.

Note If you require a firewall for a group, make sure the group does not include any clients other than Windows VPN Clients. Any other clients in the group (including VPN 3002 Hardware Clients) are unable to connect.

Reference: VPN 3000 Series Concentrator Reference Volume I: Configuration

QUESTION NO: 2
When logged into your 3000 series Concentrator via a web browser, what are the three main tabs?

A. administration
B. settings
C. protocols
D. monitoring
E. configuration
F. ipsec

Answer: A,D,E

Explanation:
There are three main tabs of your 3000 series Concentrator when logged in via a web browser. Configuration, Administration, and Monitoring.

QUESTION NO: 3
Jane the newly hired security administrator at Testking Inc. is working on setting up the Cisco VPN Client. Which statement about the Cisco VPN Client local LAN access feature is true?

A. The Cisco VPN Client local LAN access feature enables split tunneling.
B. The Cisco VPN Client local LAN access feature enables local LAN users access to the VPN tunnel.
C. The Cisco VPN Client local LAN access feature enables Cisco VPN Client to encrypt packets destined for the local LAN.
D. The Cisco VPN Client local LAN access feature enables and disables Cisco VPN Client access to the local LAN.

Answer: A
Explanation:
"Split Tunnelling Policy – Local LAN Option"
"Allow networks to bypass the tunnel" and select "VPN Client Local LAN (Default)" as the Split Tunnelling Network List.
-> Local LAN access is a simple split tunnelling feature, because by default all traffic is sent through the tunnel!

Section 4: Configure users and groups (12 questions)

QUESTION NO: 1
John and Kathy the security team at Testking Inc. is working on Cisco VPN. They need to choose three parameters sent from the Cisco VPN Concentrator to the remote Cisco VPN Client during tunnel establishment. Which are the three parameters? (Choose three)

A. Access priority
B. Split tunnel policy
C. Group name
D. Primary DNS address
E. Access priority level
F. Cisco VPN Client IP address

Answer: C D F
Explanation:
During IKE tunnel establishment, the peer provides its identity: either an IP address, a fully qualified domain name (FQDN), or a distinguished name (DN). It also presents a certificate, which contains none, some, or all of these fields. If IKE peer identity validation is enabled, the VPN Concentrator compares the peer's identity to the like field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the VPN Concentrator establishes the tunnel. If the information does not match, the VPN Concentrator drops the tunnel. This feature provides an additional level of security.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 2
Kathy is the security administrator at Testking Inc. is working on the Cisco VPN Concentrator. How can Kathy accommodate the different access needs in a Cisco VPN Concentrator?

A. By having Kathy configure rights and privileges parameters in the Cicso VPN Concentrator.
B. By having Kathy configure access and usage parameters in the Cisco VPN Concentrator.
C. By having Kathy configure rights and privileges in the network authentication server.
D. By having Kathy configure user and group parameters in the Cisco VPN Concentrator.

Answer: D
Explanation:
Configure groups and users with attributes that determine their access to and use of the VPN. Configuring groups and users correctly is essential for managing the security of your VPN.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
A TestKing trainee wants to know what is the type of authentication makes use of groups value in the Configuration | Quick | IPSec window. What will your reply be?

A. user
B. Cisco VPN Concentrator
C. NT Domain
D. RADIUS

Answer: B
Explanation: Configuring the IPSec Group
The Manager displays the Configuration | Quick | IPSec Group screen. This screen appears only when you select the IPSec tunneling protocol, and you must configure these parameters to complete quick configuration.

The remote-access IPSec client connects to the VPN Concentrator using this group name and password, which are automatically configured on the internal authentication server. This is the IPSec group that creates the tunnel. Users then log in, and are authenticated, through their usernames and passwords. (See Figure 3-14.)

QUESTION NO: 4
During tunnel establishment, during tunnel establishment, the Cisco VPN Client receives a list of split DNS names and a primary DNS server address from the Concentrator when working in a VPN Concentrator release 3.6 environment.

After the tunnel is established, when the VPN Client receives a DNS query, the query is compared with the split DNS names.

How will the VPN Client react to the results of the comparison?

A. A matching query will be encrypted then transmitted to the primary DNS server for address resolution.
B. A matching query will be transmitted in clear text to the ISP DNS server for address resolution.
C. A matching query will be transmitted in clear text to the primary DNS server for address resolution.
D. A matching query will be encrypted then transmitted to the ISP DNS server for address resolution.

Answer: A
…Query packets passing the comparison will have their destination IP address rewritten and tunneled using the primary DNS IP address configured on the concentrator…

QUESTION NO: 5
The newly appointed TestKing trainee technician wants to know which of the following Quick Configuration elements can be used in the configuration of IPSec group. What will your reply be? Choose two.

A. group access protocols
B. group server name
C. password
D. user name
E. group priority
F. group name

Answer: D, F
Explanation:

Configuring IPSec
The VPN 3002 connects to the remote VPN Concentrator using the IPSec remote server address, group name and password, and username and password. Note that these are the same group and usernames and
passwords that you configure on the central-site VPN Concentrator for this VPN 3002.If you are using digital certificates, the group name and group password are not required.
0

Step 1 In the IPSec Remote Server parameter, enter the IP address or hostname of the VPN Concentrator to which this VPN 3002 hardware client connects. Note that to enter a hostname, a DNS server must be configured.

> IPSec Remote Server
Quick -> [130.0.0.1]

Step 2 The system prompts you to enable or disable IPSec over TCP.
1) Enable IPSec over TCP
2) Disable IPSec over TCP
Quick -> [2]
At the cursor, enter 1 to enable IPSec over TCP, or accept the default, 2, to disable IPSec over TCP.

Step 3 The system prompts you to enter the IPSec group name.
> IPSec Group Name

Quick -> _
At the cursor, enter a unique name for this group. Maximum is 32 characters, case-sensitive; for

example, Group1.
Step 4 The system prompts you to enter the group password.
> IPSec Group Password
Quick -> _
At the cursor, enter a unique password for this group. Minimum is 4, maximum is 32 characters,
case-sensitive. The system displays only asterisks.
Step 5 The system prompts you to reenter the group password to verify it.
Verify -> _
At the cursor, reenter the group password. The system displays only asterisks.
Step 6 The system prompts you to enter a username.
> IPSec User Name
Quick -> _
Enter a unique name within the group for this user. Maximum is 32 characters, case-sensitive.

Step 7 The system prompts you to enter the user password. Minimum is 4, maximum is 32 characters,
case-sensitive. The system displays only asterisks.
> IPSec User P0assword
Quick -> _
Step 8 The system prompts you to reenter the user password.
Verify ->

QUESTION NO: 6
The newly appointed TestKing trainee wants to know which IKE proposal is supported by the certicom client when under the IKE active proposal list. What will your reply be?

A. IKE-3DES-MD5-RSA
B. IKE-3DES-MD5-DH7
C. CiscoVPNClient-3DES-MD5
D. IKE-3DES-MD5

Answer: B
Certicom client uses elliptical curve cryptography (ecc) for small processor devices.

QUESTION NO: 7
Which of the following group attributes are configurable in an environment where group attributes are being configured in the Cisco VPN Concentrator? (Select three options.)

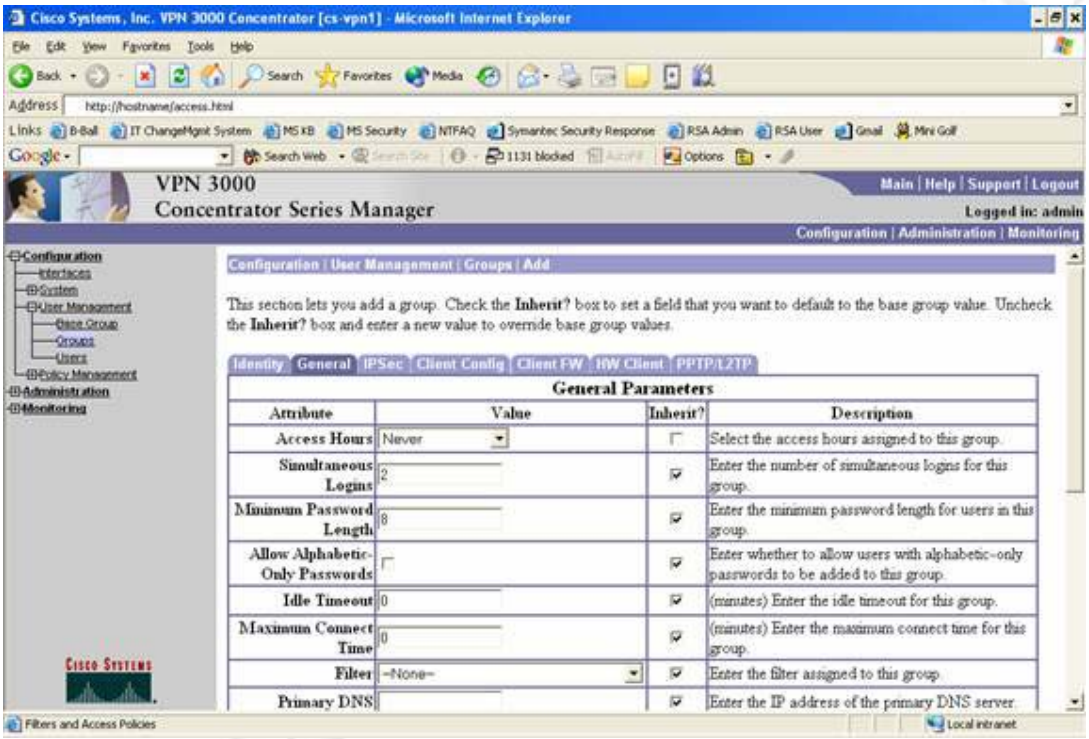
A. access hours
B. idle timeout
C. connection priority
D. maximum connect time
E. access level

F. TACACS+ server IP address

Answer: A, B, D
Source: Configuration | User Management | Groups | Modify a Group | General Tab

Access hours
Idle Timeout
Maximum Connect Time

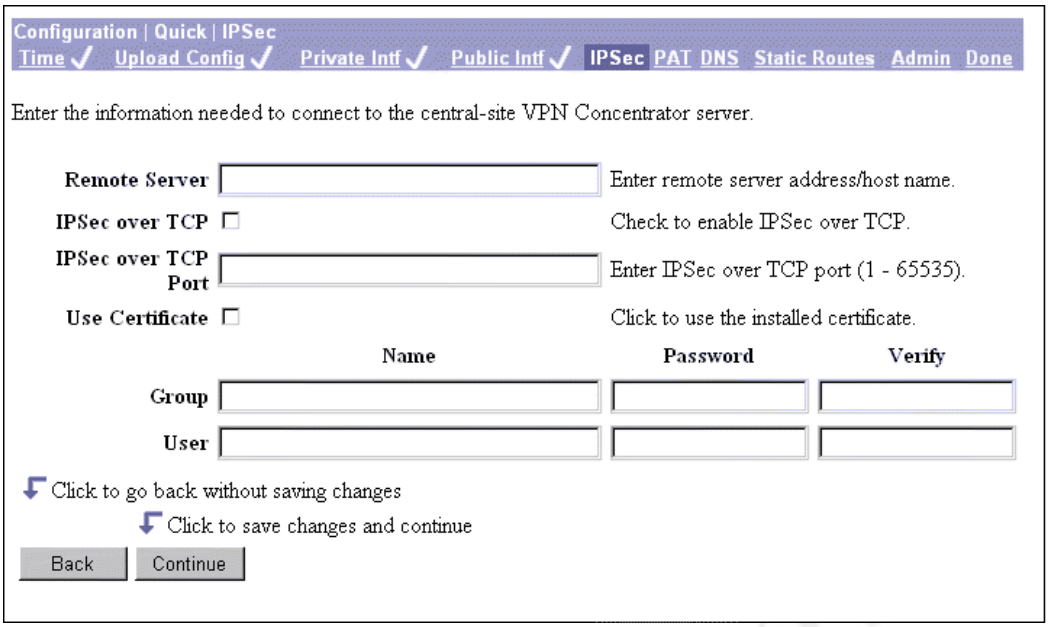
These 3 options are configurable from the Configuration | User Management | Groups | Add → General Tab



QUESTION NO: 8
Which of the following IP addresses should go in the remote server field in the Configuration | Quick | IPSec windows?

A. DCHP server
B. authentication server
C. central site Cisco VPN Concentrator
D. accounting server

Answer: C
Explanation:



In the Remote Server field, enter the IP address or hostname of the VPN Concentrator to which this VPN 3002 hardware client connects. Note that to enter a hostname, a DNS server must be configured.

QUESTION NO: 9
The Testking trainee technician wants to know which of the following IKE proposals can be used with digital certificates. What will your reply be?

A. IKE-3DES-MD5
B. IKE-3DES-MD5-DH7
C. IKE-3DES-MD5-RSA
D. IKE-AES-128-SHA

Answer: C
Source: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.240

QUESTION NO: 10
What is the 3000 series Concentrator group configuration screen tab that you enable split tunneling on?

A. client config
B. general
C. identity
D. setup

Answer: A
Explanation:
Split Tunneling configuration for a group is set under the client config tab from the 3000 series Concentrator configuration, user management, groups configuration screen.

QUESTION NO: 11
Which 3000 series Concentrator group configuration tab allows you to enable Interactive Hardware Authentication for remote 3002 Hardware Clients?

A. authentication
B. clients
C. hardware
D. hw client

Answer: D
Explanation:
The hw client tab under group configuration (configuration, user management, groups) allows enabling of Interactive Hardware Authentication. This essentially provides an extra level of security between the 3002 Hardware Client and the Head End Concentrator.

QUESTION: 12
What is the maximum combined number of users and groups that can be configured on a Concentrator?

A. 100
B. 200
C. 750
D. 1000

Answer: D
Explanation:
A Concentrator will allow a combined total of 1000 users and groups to be defined.

Section 5: More in-depth configuration information (8 questions)

QUESTION NO: 1
Jason the security administrator at Testking Inc. was given the assignment to match the severity level with the alarm level.

Answer:

Explanation:

Table 9-2: Event Severity Levels

Level	Category	Description
1	Fault	A crash or non-recoverable error.
2	Warning	A pending crash or severe problem that requires user intervention.
3	Warning	A potentially serious problem that may require user action.
4	Information	An information-only event with few details.
5	Information	An information-only event with moderate detail.

6	Information	An information-only event with greatest detail.
7	Debug	Least amount of debugging detail.
8	Debug	Moderate amount of debugging detail.
9	Debug	Greatest amount of debugging detail.
10	Packet Decode	High-level packet header decoding.
11	Packet Decode	Low-level packet header decoding.
12	Packet Decode	Hex dump of header.
13	Packet Decode	Hex dump of packet.

QUESTION NO: 2
John is the security administrator at Testking Inc. and he is troubleshooting the Cisco VPN Concentrator. The problem is a remote user exceeds the configured policing rate. What will the VPN Concentrator do when this happens?

A. The VPN Concentrator will allow exceeds of traffic to pass up to the configured normal burst size.
B. The VPN Concentrator logs the event, set the DE bit, and allow the traffic to pass.
C. All packets marked high priority are passed and all packets marked low priority are dropped on the VPN Concentrator
D. The VPN Concentrator will allow excess traffic to pass up to 1/8th of the CIR.

Answer: A
Explanation:
Bandwidth policing sets a maximum limit, a cap, on the rate of tunneled traffic. The VPN Concentrator transmits traffic it receives below this rate; it drops traffic above this rate. Because traffic is bursty, some flexibility is built into policing. Policing involves two thresholds: the *policing rate* and the *burst size*. The policing rate is the maximum limit on the rate of sustained tunneled traffic. The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped back to the policing rate. The VPN Concentrator allows for instantaneous bursts of traffic greater than the policing rate up

to the burst rate. But should traffic bursts consistently exceed the burst rate, the VPN Concentrator enforces the policing rate threshold.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
At which particular level in the Concentrator is NAT applied after NAT-transparency is configured on the Concentrator?

A. port level
B. group level
C. user level
D. system-wide level
E. none of the above

Answer: D
Explanation:

The functions that fall under the Configuration | System section have to do with configuring parameters for system-wide functions in the VPN concentrator. Configure | Policy Management is its subcategorie.
One of the Sections of Configure | Policy Management is NAT.
-NAT- The Cisco VPN 3000 Concentrators can perform Network Address Translation, which you would configure in this section.

Reference: CCSP VPN Ciscopress p.169-173

QUESTION NO: 4
Which of the following protocols can be used to download the event log file from a Concentrator? Choose 2.

A. http
B. smtp
C. ftp
D. scep

Answer: A,C
Explanation:
Download the event log file on a Concentrator with HTTP or FTP.

QUESTION NO: 5
Where can you configure your Concentrators hostname?

A. configuration, system, ip routing, setup
B. configuration, system, ip routing, identification
C. configuration, system, general, setup
D. configuration, system, general, identification

Answer: D
Explanation:
Use the configuration, system, general, identification Concentrator screen to set the hostname.

QUESTION NO: 6
Where is an SMTP server added to your Concentrator configuration?

A. configuration, policy management, traffic management, smtp servers
B. configuration, policy management, traffic management, servers
C. configuration, system, general, smtp servers
D. configuration, system, events, smtp servers

Answer: D
Explanation:
SMTP servers can be configured on your Concentrator from configuration, system, events, smtp servers.

QUESTION NO: 7
Where do you access DNS server configuration parameters on your Concentrator?

A. configuration, system, tunneling protocols, dns
B. configuration, system, servers, dns
C. configuration, system, ip routing, dns
D. configuration, system, management protocols, dns

Answer: C
Explanation:
DNS server configuration is set from the configuration, system, ip routing dns screen.

QUESTION NO: 8
On a Concentrator, where is the default gateway ip address entered?

A. configuration, system, ip routing, default gateways

B. configuration, system, tunneling protocols, default gateways
C. configuration, system, servers, default gateways
D. configuration, system, general, default gateways

Answer: A
Explanation:
The Concentrators default gateway can be configured from configuration, system, ip routing, default gateways.

Section 6: Configure the Cisco Windows VPN Software Client (3 questions)

QUESTION NO: 1
Which three files is necessary when pre-configuring a Cisco VPN client? (Select three options.)

A. unattended_setup.ini
B. user.pcf
C. data.ini
D. oem.ini
E. vpnclient.ini
F. client.ini

Answer: B, D, E

QUESTION NO: 2
In Cisco VPN 3000 releases 3.7, in the Cisco VPN client GUI is supported on which two operating systems. Select two.

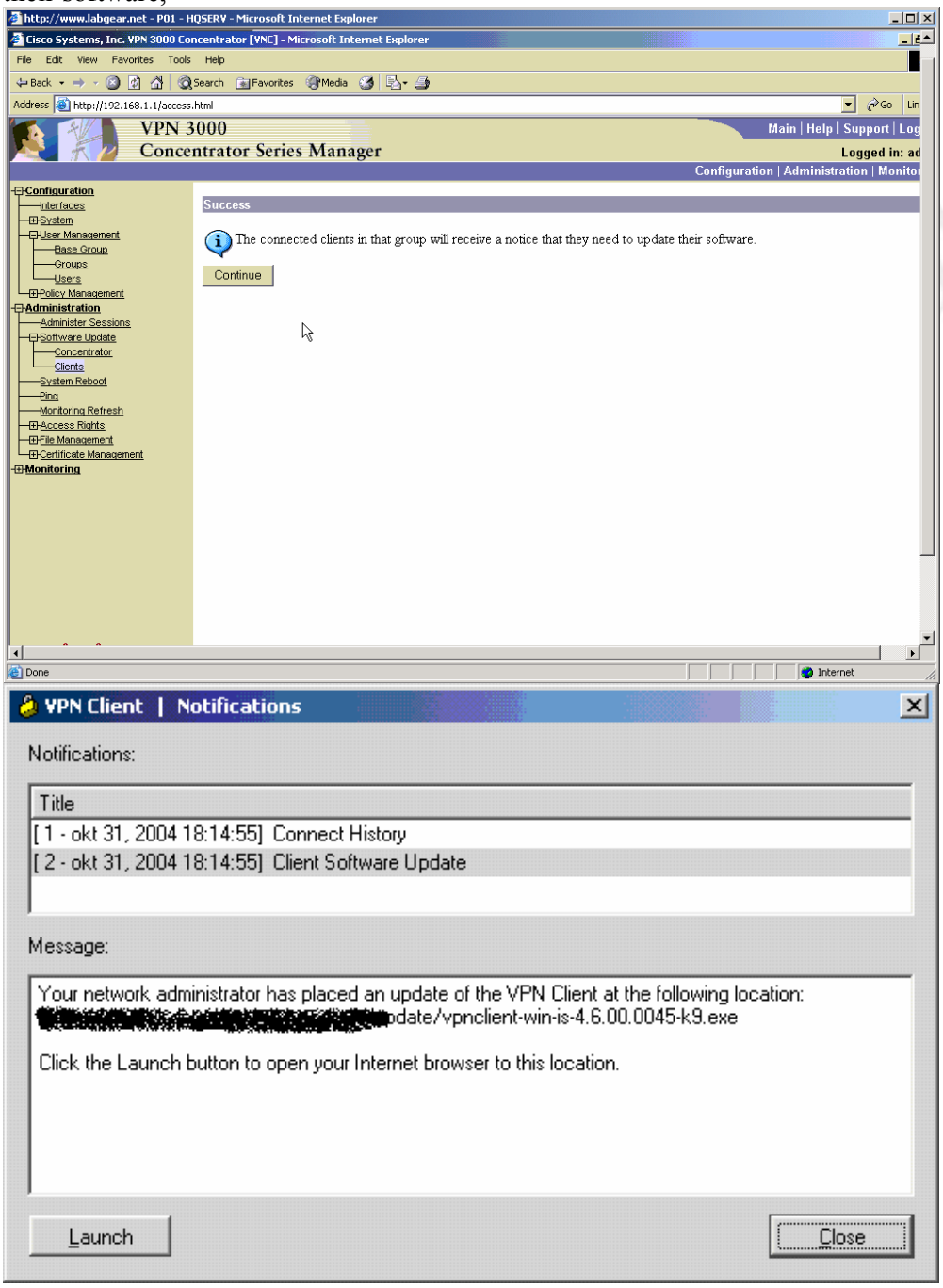
A. Windows
B. Linux
C. Macintosh
D. Solaris
E. HP-UX
F. IBM AIX

Answer: A. C

QUESTION NO: 3
Which of the following statements regarding Cisco VPN client software update is valid?

A. As a remote Cisco VPN Client connects to the Cisco VPN Concentrator, the remote Cisco VPN Client automatically downloads a new version of code from a configurable web site.
B. As a remote Cisco VPN Client connects to the Cisco VPN Concentrator, the remote Cisco VPN Client automatically downloads a new version of code from a configurable TFTP server.
C. As a remote Cisco VPN Client connects to the Cisco VPN Concentrator, the r Cisco VPN Concentrator automatically downloads a new version of the software.
D. As a remote Cisco VPN Client connects to the Cisco VPN Concentrator, the Cisco VPN Concentrator only sends an update notification to the remote Cisco VPN Client.

Answer: D
Explanation:
When you use the update software feature it will notify your client that they need to update their software,



Topic 4, Configure Cisco Virtual Private Network 3000 Series Concentrator for Remote Access Using Digital Certificates (27 questions)

Section 1: CA support overview (12 questions)

QUESTION NO: 1
Jacob the security administrator for Testking Inc. is exchanging certificates between a Cisco VPN client and a Cisco VPN Concentrator, the group information on Cicso VPN client and Cisco VPN Concentrator must match. Because there is no group field listed on the VPN client certificate manager enrollment form, which enrollment field will double as a group field?

A. Common name enrollment field
B. IP address enrollment field
C. Organization enrollment field
D. Department name enrollment field

Answer: D
Explanation:
Department—The name of the department to which you belong; for example, International Studies. This field correlates to the Organizational Unit (OU). The OU is the same as the Group Name configured in a VPN 3000 Series Concentrator, for example.

QUESTION NO: 2
Jason the security administrator at Testking Inc. is working on IKE. His assignment is to find out which three things the Cisco VPN 3000 Concentrator checks during the IKE negotiations, when an identity certificate is received from an IKE peer. (Choose three)

A. Has the CA expired?
B. Is the certificate still valid?
C. Has the CA been revoked?
D. Is the certificate signed by a trusted CA?
E. Is the certificate in the CRL?
F. Is the certificate FQDN valid?

Answer: B D E
Explanation:

During IKE tunnel establishment, the peer provides its identity: either an IP address, a fully qualified domain name (FQDN), or a distinguished name (DN). It also presents a certificate, which contains none, some, or all of these fields. If IKE peer identity validation is enabled, the VPN Concentrator compares the peer's identity to the like field in the certificate to see if the information matches. If the information matches, then the peer's identity is validated and the VPN Concentrator establishes the tunnel. If the information does not match, the VPN Concentrator drops the tunnel. This feature provides an additional level of security.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
Jason the security administrator for Testking Inc. was given the assignment to find out what the two purposes of the X.509 Certificate Serial Number are. (Choose two)

A. The purpose is it specifies the subject's public key and hashing algorithm.
B. The purpose is it specifies the start and expiration dates for the certificate.
C. The purpose is a unique certificate numerical identifier in the CA domain.
D. The purpose is the certificate number that is listed on the CRL when the certificate is revoked.
E. The purpose is it identifies the CA's public key and hashing algorithm.
F. The purpose is Private Key.

Answer: C D
Explanation:
A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to such things as a name change, change of association between the subject and the CA, and security compromise, the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed CRL, where each revoked certificate is identified by its serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the CRL to ensure that the certificate being verified has not been revoked.h

QUESTION NO: 4
Kathy the security administrator at Testking Inc. is working on certificates. She needs to know which information is included in the PKCS#10 request message. (Choose two)

A. PKCS#10 request message contains the encryption algorithm
B. PKCS#10 request message contains the validity dates
C. PKCS#10 request message contains the user information
D. PKCS#10 request message contains the key size
E. PKCS#10 request message contains the private key
F. PKCS#10 request message contains the authentication algorithm

Answer: C, D
Explanation:

Generating the PKCS#10 requires various user information inputs AND input for the key size of choice!

Note:
An enrollment request for an identity certificate consists of a base 64 encoded PKCS#10 file that the VPN Concentrator generates based on information you provide in the steps that follow.

You have generated a base 64 encoded PKCS#10 file (Public Key Certificate Syntax-10), which most CAs recognize or require. The system automatically saves this file in Flash memory with the filename shown in the browser (pkcs*NNNN*.txt).
In generating the request, the system also generates the private key used in the PKI process. That key remains on the VPN Concentrator in encrypted form.

QUESTION NO: 5
Which of the following features will permit automatic certificate enrollment with the CA?

A. Mode Configuration
B. Quick Configuration
C. VRRP
D. SCEP
E. RRI

Answer: D
Developed by Cisco, Verisign, Entrust, Microsoft, Netscape and Sun Simple Certificate Enrollment Protocol (SCEP) provides a way of managing the certificate. SCEP let you automatically provide your users with a way to enroll with the CA.

QUESTION NO: 6
What are the two types of certificate enrollment for the Cisco VPN Concentrator?

A. PKCS# 15enrollment process
B. PKCS#7 enrollment process
C. SCEP
D. certified enrollment process
E. CERTC enrollment process
F. File-based enrollment process

Answer: C, F

Explanation:

Configuring Digital Certificates: SCEP and Manual Methods

To use digital certificates for authentication, you first enroll with a Certificate Authority (CA), and obtain and install a CA certificate on the VPN Concentrator. Then you enroll and install an identity certificate from the same CA.
You can enroll and install digital certificates on the VPN Concentrator in either of two ways:

- Using Cisco's Simple Certificate Enrollment Protocol (SCEP).

SCEP is a secure messaging protocol that requires minimal user intervention. SCEP is the quicker method, and it lets you to enroll and install certificates using only the VPN Concentrator Manager. To use SCEP, you must enroll with a CA that supports SCEP, and you must enroll via the Internet.

- Manually, exchanging information with the CA directly.

The manual method involves more steps. You can do some of the steps using the Manager. Other steps require that you exchange information with the CA directly. You deliver your enrollment request and receive the certificate from the CA via the Internet, email, or a floppy disk.

Ref 2//

Enrollment Method

Choose an enrollment method:

- PKCS10 Request (Manual) = Enroll using the manual process.
- Certificate Name via SCEP = Enroll automatically using this SCEP CA.

Note If you install a CA certificate using the manual method, you must also use the manual method to request identity or SSL certificates from that CA. Conversely, to request identity and SSL certificates using SCEP, you must first use SCEP to obtain the CA certificate.

Tasks Summary

Whether you use SCEP or the manual method, you perform the following tasks to obtain and install certificates:
1. Obtain and install one or more CA certificate(s).
2. Create an enrollment request for one or more identity certificates.
3. Request an identity certificate from the same CA that issued the CA certificate(s).
4. Install the identity certificate on the VPN Concentrator.
5. Enable CRL checking and caching.
6. Enable certificates.

About the Documentation

The print version of this guide provides step-by-step examples of configuring digital certificates using SCEP and manually, and with both LAN-to-LAN and remote access connections, beginning with the next section, "1879871Managing Certificates with SCEP."

Ref 3://

Types of certificate enrollment in Cisco VPN contractor
You can enroll and install digital certificates on the VPN 3002 automatically or manually. The automatic method is a new feature that uses the Simple Certificate Enrollment Protocol (SCEP) to streamline enrollment and installation. SCEP is a secure messaging protocol that requires minimal user intervention. This method is quicker than enrolling and installing digital certificates manually, but it is available only if you are both enrolling with a CA that supports SCEP and enrolling via the web. If your CA does not support SCEP, or if you enroll with digital certificates by a means other than the web (such as through email or by a diskette), then you cannot use the automatic method; you must use the manual method.

An enrollment request for an identity certificate consists of a base 64 encoded PKCS#10 file that the VPN Concentrator generates based on information you provide in the steps that follow

QUESTION NO: 7
Which of the following will suffice as reasons for revoking a certificate? Choose two.

A. invalid time
B. Invalid date
C. change of association
D. compromised security
E. Invalid signature

Answer: C, D
Explanation:
A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to a name change, **change of association between the subject and the CA, security compromise,** etc., the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed certificate revocation list (CRL), where each revoked certificate is identified by its serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the CRL to ensure that the certificate being verified has not been revoked.
CAs use LDAP/HTTP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP/HTTP access.

QUESTION NO: 8
Which of the following statements regarding the digital signature process statement is valid?

A. The hash is encrypted with the public key and decrypted with the private key.
B. The hash is encrypted and decrypted with a shared secret key.
C. The hash is encrypted and decrypted with a symmetric key.
D. The hash is encrypted with the private key and decrypted with the public key.

Answer: C
Explanation:
VPNs encrypt transmissions using a mechanism of key exchanges and complicated hashing and encryption algorithms.

Key Generation and Management
Typically, a VPN uses a symmetric system to encrypt data and an asymmetric system to exchange keys. Asymmetric systems tend to be more secure, but symmetric systems perform better and have greater production value. Each side uses asymmetric key exchange to generate a private key, then derives a symmetric public key from the private one, and sends the public key to the other party. Each device now has its own private key and the other system's public key. Many network administrators configure the security association to periodically "time out," exchange a new set of keys, and thereby thwart a network cracker attempting to decode communications.

QUESTION NO: 9
What are the functions that a CA has to fulfill? (Select three options.)

A. The CA is responsible for revoking valid certificates
B. The CA is responsible for creating certificates
C. The CA is responsible for decrypting digital certificate
D. The CA is responsible for administering certificates
E. The CA is responsible for issues equipment certificates
F. The CA is responsible for revoking invalid certificates

Answer: B, D, F
Explanation: The CA creates, administers, and revokes invalid certificates.
Reference: Ciscopress CCSP Self Study, CSVPN Second edition Page: 142

QUESTION NO: 10
The TestKing CEO wants your opinion regarding the best PKI model for a large enterprise. What can you tell her?

A. Central
B. Flat

C. Hub and Spoke
D. Hierarchical

Answer: D
Explanation:
Going beyond the single-root CA, more complex topologies can be devised that involve multiple CAs within the same organization. One such topology is the hierarchical CA system, in which CAs no longer issue certificates to end users only, but also to subordinate CAs, who in turn issue their certificates to end-users and/or other CAs. In a hierarchical CA system, a tree of CAs and end users is built for which every CA can issue certificates to entities on the next lower level.

QUESTION NO: 11
Which of the following causes a certificate issued from a CA to become invalid? Choose all that apply.

A. certificate reaches expiration date
B. certificate listed on CRL
C. certificate not enrolled via SCEP
D. certificate requested via PKCS # 10

Answer: A,B
Explanation:
If a certificate is on the CA servers' Certificate Revocation List, (CRL) is should be considered invalid and not used. Also when the certificate is generated, it has a built-in expiration date, after which it will not work.

QUESTION NO: 12
Which of the following protocols automates the installation process of a digital certificate?

A. FTP
B. SCEP
C. VRRP
D. AH

Answer: B
Explanation:
You can automate the certificate request and installation process on your Concentrator by using Simple Certificate Enrollment Protocol (SCEP) with a CA.

Section 2: Certificate generation (3 questions)

QUESTION NO: 1
John the security administrator at Testking Inc. is working on installing certificates on the Cisco VPN 3000 Concentrator. Which two certificates does John need to install in the Cisco VPN 3000 Concentrator? (Choose two)

A. Root certificate needs to be installed
B. SSL certificate needs to be installed
C. Public certificate needs to be installed
D. Private certificate needs to be installed
E. Identity certificate needs to be installed
F. Trusted certificate needs to be installed

Answer: A E
"Concentrator Certificate Manual Loading Process"
Step 1: Generate the certificate request and upload it to the CA
Step 2: The CA generates the identity and root certificates.
Each downloaded to a PC.
Step 3: The certificates are loaded onto the Concentrator.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 2
Which pieces of information does the CA supply when it issues a digital certificate? Choose three.

A. user name
B. validity dates
C. User's private key information
D. private key
E. Issuer's name
F. CA signature algorithm

Answer: B, E, F
Explanation:

Certificate Fields

A certificate contains some or all of the following fields:

Field	Content

Subject	The person or system that uses the certificate. For a CA root certificate, the Subject and Issuer are the same.
Issuer	**The CA or other entity (jurisdiction) that issued the certificate. Subject and Issuer consist of a specific-to-general identification hierarchy: CN, OU, O, L, SP, and C. These labels and acronyms conform to X.520 terminology, and they echo the fields on the** Administration | Certificate Management | Enrollment screen.
CN	**Common Name: the name of a person**, system, or other entity. This is the lowest (most specific) level in the identification hierarchy. For the VPN Concentrator self-signed SSL certificate, the CN is the IP address on the Ethernet 1 (Private) interface at the time the certificate is generated. SSL compares this CN with the address you use to connect to the VPN Concentrator via HTTPS, as part of its validation.
OU	Organizational Unit: the subgroup within the organization (O).
O	Organization: the name of the company, institution, agency, association, or other entity.
L	Locality: the city or town where the organization is located.
SP	State/Province: the state or province where the organization is located.
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
Serial Number	The serial number of the certificate. Each certificate issued by a CA must be unique among all certificates issued by that CA. CRL checking uses this serial number.
Signing Algorithm	**The cryptographic algorithm that the CA or other issuer used to sign this certificate.**
Public Key Type	The algorithm and size of the certified public key.
Certificate Usage	The purpose of the key contained in the certificate, for example: digital signature, certificate signing, nonrepudiation, key or data encipherment, etc.
MD5 Thumbprint	A 128-bit MD5 hash of the complete certificate contents, shown as a 16-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a root certificate's authenticity, you can check this value with the issuer.
SHA1 Thumbprint	A 160-bit SHA-1 hash of the complete certificate contents, shown as a 20-byte string. This value is unique for every certificate, and it positively identifies the certificate. If you question a certificate's authenticity, you can check this value with the issuer.
Validity	**The time period during which this certificate is valid. Format is MM/DD/YYYY at HH:MM:SS to MM/DD/YYYY at HH:MM:SS.** Time uses 24-hour notation, and is local system time. The Manager checks the validity against the VPN Concentrator system clock, and it flags expired certificates by issuing event log entries.
Subject Alternative Name (Fully Qualified Domain Name)	The fully qualified domain name for this VPN Concentrator that identifies it in this PKI. The alternative name is an optional additional data field in the certificate, and it provides interoperability with many Cisco IOS and PIX systems in LAN-to-LAN connections.
CRL Distribution	All CRL distribution points from the issuer of this certificate.

Point

QUESTION NO: 3
Which of the following are the steps that are used when enrolling the file-based certificate? (Select three options.)

A. The identity certificate is loaded into the Cisco VPN Concentrator first.
B. The CA generates the root and identity certificates.
C. The root certificate is loaded into the Cisco VPN Concentrator second.
D. The root certificate is loaded into the Cisco VPN Concentrator first.
E. The Cisco VPN Concentrator generates a PKCS#7.
F. The Cisco VPN Concentrator generates a PKCS#10.

Answer: B, C, F

Section 3: Validating certificates (9 questions)

QUESTION NO: 1
James the security administrator at Testking Inc. is working on IKE certificates. What are three steps in the IKE certificate authentication process? (Choose three)

A. The identity certificate validity period is verified against the system clock of the Cisco VPN Concentrator.
B. The root certificate is not in the Cisco VPN Concentrator.
C. If enabled, the Cisco VPN Concentrator locates the CRL and validates the identity certificate.
D. Identity certificates are exchanged during IPSec negotiations.
E. The identity certificate signature is validated using the stored root certificate.
F. The signature is validated using the stored identity certificate.

Answer: A, C, E
Explanation:
Validating Certificates:
- Signed by a CA that is trusted. – Checks the signature. (E)
- Not expired. (A)
- Not revoked. (C)

Reference: Cisco Secure Virtual Private Networks (Ciscopress) page 236

QUESTION NO: 2
Janice the Testking Inc. security administrator is working on the CRL configuration. Which three statements about CRL configuration are true? (Choose three)

A. CRL checking is disabled by default.
B. The Cisco VPN Concentrator relies on LDAP access to procedure the CRL list.
C. CRL checking is enabled by default.
D. The Cisco VPN Concentrator relies on HTTP access to procedure the CRL list.
E. If the CRL distribution point is available in the certificate, you do not have to fill in most of the CRL configuration fields.
F. If the CRL distribution point is available in the certificate, you still have to fill in most of the CRL configuration fields.

Answer: A B E
Explanation:
F is incorrect, because you don't have to specify the CRL distribution point configuration fields, if the CRL distribution point URI comes with the certificate (-> E is the better choice).

Note 1:

CAs use LDAP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP access.

Step 1 On the Administration | Certificate Management screen, in the Certificate Authorities table, click **Configure** next to the CA certificate for which you want to enable CRL checking. The Manager displays the Administration | Certificate Management | Configure CA Certificate screen. For information on these fields, see the "Administration | Certificate Management | Configure CA Certificate" section or online Help.

Step 2 CRL checking is disabled by default. Choose the method to use to retrieve the CRL.
• If you choose to use CRL distribution points specified in the certificate being checked, be sure to specify the distribution point protocols for retrieving CRLs. If you choose the LDAP protocol, be sure to specify the LDAP distribution point defaults.
• If you choose to use static CRL distribution points, be sure to enter them under Static CRL Distribution Points further down.
Step 3 To enable CRL caching, check the **Enabled** check box. In the **Refresh Time** field, specify a time period for updating the CRL.
Step 4 Check the appropriate check boxes to indicate whether you want to accept Subordinate CA Certificates or accept Identity Certificates signed by this issuer.
Step 5 Click **Apply**. The Manager displays the Administration | Certificate Management screen.

Note: D is also true, because the concentrator can use LDAP and HTTP to get CRLs (see also Explanations for QUESTION NO 90). The problem is, that there are only three selections possible.

QUESTION NO: 3
Which of the following represents a correctly defined static CRL distribution point?

A. TFTP://10.0.1.21/CertEnroll/TestKing.crl
B. FTP://10.0.1.21/CertEnroll/TestKing.crl
C. HTTP://10.0.1.21/CertEnroll/TestKing.crl
D. HTTPS://10.0.1.21/CertEnroll/TestKing.crl

Answer: C
Static CRL Distribution Points
Enter HTTP or LDAP URLs that identify CRLs located on external servers. If you chose a CRL Retrieval Policy that uses static distribution points, you must enter at least one (and not more than five) valid URLs. Enter each URL on a single line. (Scroll right to enter longer values.) Examples of valid URLs are:

HTTP URL: http://1.1.1.2/CertEnroll/TestCA6-8.crl

LDAP URL: ldap://100.199.7.6:389/CN=TestCA6-8,CN=2KPDC,CN=CDP,CN=Public Key

Services,CN=Services,CN=Configuration,DC=qa2000,DC=com?certficateRevocation List?base?objectclass=cRLDistributionPoint

QUESTION NO: 4
The VPN Concentrator retrieves and examines CRLs when CRL checking is enabled. CRLs can be cached locally to mitigate potential timeout problems due to network congestion and delay. In which location are CRLs cached?

A. on a pre-defined TFTP server on the local private network
B. on a pre-defined FTP server on the local private network
C. in the VPN Concentrator's volatile memory
D. in the VPN Concentrator's non volatile memory

Answer: C

Since the system has to retrieve and examine the CRL from a network distribution point, enabling CRL checking might slow system response times. Also, if the network is slow or congested, CRL checking might fail. To mitigate these potential problems, you can enable CRL caching. This stores the retrieved CRLs in local volatile memory, thus allowing the VPN Concentrator to verify the revocation status of certificates more quickly.

QUESTION NO: 5
Which of the following protocols can be utilized by VPN Concentrator in an attempt to retrieve Certificate Revocation Lists? (Select two options.)

A. SSL
B. SSH
C. LDAP
D. HTTP
E. FTP
F. TFTP

Answer: C, D
Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.237

QUESTION NO: 6
In which location can the Cisco VPN Concentrator find the CRL in an environment where CRL checking is enabled on the Cisco VPN Concentrator?

A. The Cisco VPN Concentrator polis the CA for an updated list at a predefined rate.
B. The CA sends a CRL to the Cisco VPN Concentrator directly at least once a week.
C. The CRL distribution point is listed on the identity certificate.
D. The CRL is sent, out-of-band, to the administrator biweekly.

Answer: A
Answer A seems most likely.

A certificate is normally expected to be valid for its entire validity period. However, if a certificate becomes invalid due to such things as a name change, change of association between the subject and the CA, and security compromise, the CA revokes the certificate. Under X.509, CAs revoke certificates by periodically issuing a signed CRL, where each revoked certificate is identified by its serial number. Enabling CRL checking means that every time the VPN Concentrator uses the certificate for authentication, it also checks the CRL to ensure that the certificate being verified has not been revoked.

CAs use Lightweight Directory Access Protocol (LDAP)/HTTP databases to store and distribute CRLs. They might also use other means, but the VPN Concentrator relies on LDAP/HTTP access.

HTTP CRL checking is introduced in VPN Concentrator version 3.6 or later. However, LDAP based CRL checking was introduced in the earlier 3.x releases. This document only discusses CRL checking using HTTP.

Incorrect answer.
Answer B seems unlikely since the CA doesn't have a way of knowing where to send the updated CRL, maybe a TFTP server? Still, I don't see the CA being proactive about eh updated CRL. The concentrator should have to go to the CA for the updated CRL.

Answer C I believe in incorrect since the specific information from the CA

D is not an option. It's not a proactive act by the CA.

QUESTION NO: 7
How do you configure your Concentrator to use a digital certificate for authentication?

A. configuration, system, management protocols
B. configuration, system, general, sessions
C. configuration, policy management, traffic management, rules
D. configuration, policy management, traffic management, security associations

Answer: D
Explanation:
When authenticating IPSEC on your 3000 series Concentrator, you can use a digital certificate by configuring it from the configuration, policy management, traffic management, security associations screen.

QUESTION NO: 8
How are IKE policies modified on a 3000 series Concentrator?

A. configuration, system, tunneling protocols, ipsec, ike proposals

B. configuration, system, ip routing, ipsec, ike proposals
C. configuration, system, events, ipsec, ike proposals
D. configuration, system, management protocols, ipsec, ike proposals

Answer: A
Explanation:
3000 series Concentrator IPSEC IKE proposals are created from configuration, system, tunneling protocols, ipsec, ike proposals.

QUESTION NO: 9
What does a Certificate Authority (CA) issue that invalidates digital certificates?

A. CDP
B. CRL
C. CMA
D. CSY

Answer: B
Explanation:
A Certificate Authority (CA) will issue a Certificate Revocation List (CRL) which identifies the digital certificates it has issued that are no longer valid. They are invalidated for usually one of two reasons: They have expired, or the key is thought to be compromised.

Section 4: Configuring the Cisco VPN 3000 Concentrator Series for CA support (3 questions)

QUESTION NO: 1
Kathy the security administrator at Testking Inc. is working on IPSec. She has to know what is true about IPSec SA, when the IPSec client-to-LAN applications are changed from pre-shared keys to digital certificates.

A. Kathy must make sure the SA IKE authentication method should be changed.
B. SA IPSec authentication method should be changed.
C. When the digital certificate is validated, the IPSec SA template automatically is updated.
D. When the digital certificates are activated, the IPSec SA template is automatically updated.

Answer: A
Explanation:
Using digital certificates, clients establish a secure tunnel over the Internet to the enterprise. A certification authority (CA) issues a digital certificate to each client for device authentication. VPN Clients may either use static IP addressing with manual configuration or dynamic IP addressing with IKE Mode Configuration. The CA server checks the identity of remote users, then authorizes remote users to access information relevant to their function. Extranet VPNs with the Cisco Secure VPN Client are addressed in "Configuring Digital Certification." Static and dynamic IP addressing is addressed in "Configuring Dynamic IP Addressing."

QUESTION NO: 2
Jacob is the security administrator at Testking Inc. is working on the Cisco VPN concentrator. The VPN Concentrator authenticates a remote peer during IKE negotiations by extracting the group information from a certificate. Prior to VPN Concentrator release 3.6, which certificate field had to match the VPN Concentrator's group name?

A. Is it the CN field
B. It is the OU field
C. Is it the O field
D. Is it the L field

Answer: B
Explanation:
Enter a unique name for this specific group. The maximum name length is 64 characters. Entries are case-sensitive. Changing a group name automatically updates the group name for all users in the group. If you are setting up a group for remote access users connecting with digital certificates, first find out the value of the Organizational Unit (OU) field of the user's identity certificate. (Ask your certificate administrator for this information.) The group name

you assign must match this value exactly. If some users in the group have different OU values, set up a different group for each of these users. If the Group Name field configured here and the OU field of the user's identity certificate do not match, when the user attempts to connect, the VPN Concentrator considers the user to be a member of the base group. The base group parameter definitions might be configured differently than the user wants or expects. If the base group does not support digital certificates, the connection fails.

Reference: VPN 3000 Concentrator Ref Volume 1. Config 3.5.pdf

QUESTION NO: 3
Which of the following certificates are needed by the Cisco VPN Concentrator and the PC when configuring IPSec client-to-LAN? Choose two.

A. CA
B. identity certificate
C. public certificate
D. Private certificate
E. Root certificate
F. DSA certificate

Answer: B, E
Source: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.241

Topic 5, Configure the Cisco Virtual Private Network Firewall Feature for IPSec Software Client (25 questions)

Section 1: Overview of software client's firewall feature (9 questions)

QUESTION NO: 1
Kathy is the security administrator at Testking Inc. and is working with the Cisco VPN Client. Her job today is to know which firewall is supported by the Cisco VPN Client *are you there* feature.

A. Supported by Zone Labs
B. Supported by Cisco Integrated Client firewall
C. Supported by Cyberguard
D. Supported by Symantec

Answer: A
Explanation:
The VPN Client on the Windows platform includes a stateful firewall that incorporates Zone Labs technology. This firewall is used for both the Stateful Firewall (Always On) feature and the Centralized Protection Policy (see "Centralized Protection Policy (CPP)").

Reference: VPN Client Administrator Guide 4.0

QUESTION NO: 2
Fred the security manager is working on Cisco VPN 3000. He is looking to in Cisco VPN 3000, release 3.6, where the AES encryption on the VPN Concentrator is performed.

A. It is performed in an AIM-VP module.
B. It is performed in a VAM module.
C. It is performed in a SEP module.
D. It is performed in VPN Concentrator software.

Answer: D
Explanation:
Note AES encryption algorithms work only with VPN Concentrator software versions 3.6 and later.

Note: AES can be performed in software or SEP-E Modules. SEP modules (listed in the question) only support DES and 3DES

Reference: VPN 3000 Series Concentrator Reference Volume I: Configuration

QUESTION NO: 3
Greg the security administrator for Testking Inc. is working on the Cisco VPN Client to interoperate with the Cisco VPN 3000. What is the minimum version of the Cisco VPN 3000 for the Cisco VPN Client to interoperate with the Cisco VPN 3000?

A. Must be running 2.5 or later
B. Must be running 2.6 or later
C. Must be running 3.0 or later
D. Must be running 3.1 or later

Answer: C
Explanation:
To interoperate with a VPN 3002, the VPN 3000 Series Concentrator to which it connects must:
• Be running software version 3.0 or later.
• Configure IPSec group and user names and passwords for this VPN 3002.
• For a VPN 3002 running in PAT mode, enable a method of address assignment: DHCP, address pools, per user, or authentication server address.
• For a VPN 3002 running in Network Extension mode, configure either a default gateway or a static route to the private network of the VPN 3002.

Reference: Release Notes for Cisco VPN 3002 Hardware Client Release 3.1

QUESTION NO: 4
Which four of the following DH-Groups are supported by the 3000 series concentrators? (Select four.)

A. 1
B. 2
C. 3
D. 4
E. 5
F. 6
G. 7
H. 8

Answer: A, B, E, G
Groups 1, 2, 5 and 7 are selectable -> supported!

QUESTION NO: 5
Which two DH groups does the VNP3000 Concentrator support for key exchange? (Select two options.)

A. 2
B. 3
C. 4
D. 5
E. 6

Answer: A, D
, the 3000 concentrator support DH group 1,2,5 and 7 for key exchange,.Group 5 and 7 are the defaults in the IPSec SA

QUESTION NO: 6
Which two DH groups for the purposes of key exchange are supported by the Cisco VPN3000 Concentrator? (Select two options.)

A. 3
B. 4
C. 5
D. 6
E. 7

Answer: C, E
Explanation:
This question must be wrong, the 3000 concentrator support DH group 1,2,5 and 7 for key exchange.

QUESTION NO: 7
Where do you enable or disable the VPN software client Stateful firewall?

A. options, settings, firewall
B. options, settings, stateful firewall
C. options, firewall
D. options, stateful firewall

Answer: D
Explanation:
From your VPN client software main screen, choose the options tab, then stateful firewall, to toggle the feature on and off.

QUESTION NO: 8
What are the three tabs of the VPN software client?

A. setup
B. firewall
C. monitoring
D. statistics
E. general

Answer: B,D,E
Explanation:
While connected to a Concentrator, you can open the VPN status screen, which has three mains tabs, Firewall, Statistics, and General.

QUESTION NO: 9
What is this minimum software version needed to run AES encryption as your ESP protocol?

A. 2.9
B. 3.2
C. 3.6
D. 4.0

Answer: C
Explanation:
To use AES instead of DES encryption, you must be running software version 3.6 or later.

Section 2: Software Client's Are You There feature (2 questions)

QUESTION NO: 1
James the security administrator is working with Kathy from the security department. They are currently working on the Cisco VPN Client together. They need to know what the three steps in the Are You There feature configuration are. (Choose three)

A. One of the steps is to select the firewall.
B. One of the steps is to select the firewall setting.
C. One of the steps is to enable the firewall virtual interface.
D. One of the steps is to select **you are there** on the firewall.
E. One of the steps is to select **are you there** on the Cisco VPN Client.
F. One of the steps is to select **are you there** on the Cisco VPN Concentrator.

Answer: A D F
Explanation:

F, not E: Are you there is a feature configured on the concentrator and fully pushed down to the client! Look at the client-side screenshot to this question – the client only shows the received configuration but allows no client-side settings.

Note:

The Firewall tab displays information about the VPN Client's firewall configuration, including the firewall policy and the configured firewall product. The remaining contents of the Firewall tab depend on these two configured options.

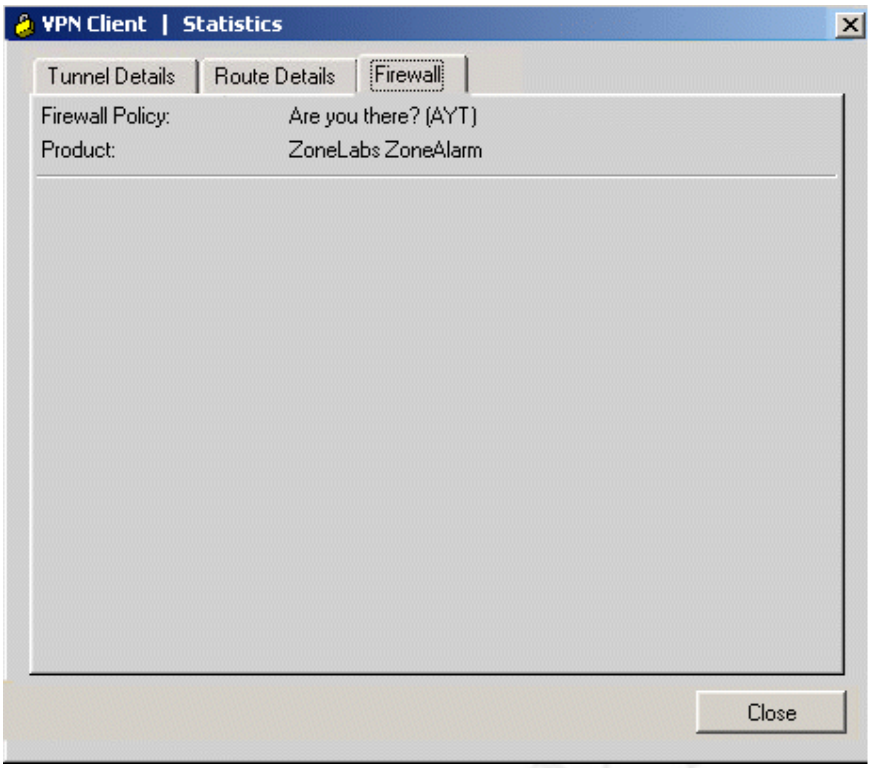
The information shown on this tab varies according to your firewall policy.

- **AYT**—When the Are You there (AYT) is the supported capability, the Firewall tab shows only the firewall policy (AYT) and the name of the firewall product AYT enforces the use of a specific personal firewall but does not require you to have a specific firewall policy.

AYT Firewall Tab

The Firewall tab shows that AYT is running and displays the name of the firewall product that supports AYT. AYT is used in conjunction with Cisco Intrusion Prevention Security Agent or Zone Labs Zone Alarm or Zone Alarm Pro to ensure that the firewall is enabled and running on a system, but not to confirm that a specific policy is enforced.

Firewall Tab for AYT capability



QUESTION NO: 2
When will a VPN software client send an AYT messages to the local firewall?

A. every 5 seconds
B. every 20 seconds
C. every 30 seconds
D. every 60 seconds
E. every 2 minutes

Answer: C
Explanation:
The Are You There (AYT) poll is sent from the VPN software client to the pc's third party firewall every 30 seconds. If there is no response to the poll, the VPN client will drop the tunnel to the Head End Concentrator.

Section 3: Software Client's Central Policy Protection feature (7 questions)

QUESTION NO: 1
When configuring CPP, which statement is true?

A. CPP is enabled in both the Cisco VPN Client and Cisco VPN Concentrator.
B. CPP is enabled in the Cisco VPN Client, Cisco VPN Concentrator, and firewall.
C. CPP is enabled on the Cisco VPN Concentrator only.
D. CPP is enabled in the Cisco VPN Concentrator and firewall.

Answer: C
Explanation:
Centralized Protection Policy (CPP)

Centralized Protection Policy (CPP) also known as firewall *push policy*, lets a network administrator define a set of rules for allowing or dropping Internet traffic while the VPN Client is tunneled in to the VPN Concentrator. A network administrator defines this policy on the VPN Concentrator, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the "Always On" option, any more restrictive rules are enforced for Internet traffic while the tunnel is established. Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. Cisco Integrated Client, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. CPP rules are in effect during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.

CPP provides more flexibility than the Stateful Firewall (Always On) feature, since with CPP, you can refine the ports and protocols that you want to permit.

Reference: VPN Client Administrator Guide 4.0

QUESTION NO: 2
Greg the security administrator for Testking Inc. is working on Cisco CPP custom policy. How does Greg activate a Cisco CPP custom policy?

A. Greg must enable custom CPP in the Cisco VPN Concentrator only.
B. Greg must enable custom CPP in the client and Cisco VPN Concentrator.
C. Greg must enable CPP in the Cisco VPN Concentrator and select the custom policy under policy management.
D. Greg must enable CPP in the Cisco VPN Concentrator and select the custom policy under the pushed policy drop-down menu.

Answer: D
Explanation:
Policy Pushed (CPP) = The VPN Concentrator enforces on the VPN clients in this group the traffic management rules defined by the filter you choose from the Policy Pushed (CPP) drop-down menu. The choices available on the menu are filters defined on this VPN Concentrator, including the default filters. Keep in mind that the VPN Concentrator pushes these rules down to the VPN client, so you should create and define these rules relative to the VPN client, not the VPN Concentrator. For example, "in" and "out" refer to traffic coming into the VPN Client or going outbound from the VPN Client.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
The new TestKing trainee technician wants to know which of the following filters are part of the Cisco CPP default policy. What will your reply be?

A. The block all inbound tunnel traffic not related to an outbound session filter.
B. The block all inbound Internet traffic not related to an outbound session filter.
C. The block al outbound tunnel traffic filter.
D. The block all outbound Internet traffic filter.

Answer: B
Explanation:

CPP lets an administrator define rules to enforce for inbound/outbound Internet traffic during split tunneling operation. Since tunnel everything already forces all traffic back through the tunnel, CPP is not used for tunnel everything.

Centralized Protection Policy (CPP)

Centralized Protection Policy (CPP) also known as firewall push policy, lets a network administrator define a set of rules for allowing or dropping Internet traffic while the VPN Client is tunneled in to the VPN Concentrator. A network administrator defines this policy on the VPN Concentrator, and the policy is sent to the VPN Client during connection negotiation. The VPN Client passes the policy to the Cisco Integrated Client, which then enforces the policy. If the client user has already selected the "Always On" option, any more restrictive rules are enforced for Internet traffic while the tunnel is established. Since CIC includes a stateful firewall module, most configurations block all inbound traffic and permit either all outbound traffic or traffic through specific TCP and UDP ports outbound. CIC, Zone Alarm, and Zone Alarm Pro firewalls can assign firewall rules. **CPP rules are in effect during split tunneling and help protect the VPN Client PC from Internet attacks by preventing servers from running and by blocking any inbound connections unless they are associated with outbound connections.**

CPP provides more flexibility than the Stateful Firewall (Always On) feature, since with CPP, you can refine the ports and protocols that you want to permit.

QUESTION NO: 4
Which of the following describes a consequence of transparent tunneling on the Cisco VPN Client?

A. Cisco VPN Client transmits traffic in clear text
B. data packets are wrapped in UDP
C. encryption is disabled on the Cisco VPN Client
D. Split tunneling is enabled on the Cisco VPN Client

Answer: B

Explanation:

Enabling Transparent Tunneling

Transparent tunneling allows secure transmission between the VPN Client and a secure gateway through a router serving as a firewall, which may also be performing Network Address Translation (NAT) or Port Address Translations (PAT). Transparent tunneling encapsulates Protocol 50 (ESP) traffic within UDP packets and can allow for both IKE (UDP 500) and Protocol 50 to be encapsulated in TCP packets before they are sent through the NAT or PAT devices and/or firewalls. The most common application for transparent tunneling is behind a home router performing PAT.
The VPN Client also sends keepalives frequently, ensuring that the mappings on the devices are kept active

C is wrong //
Transparent tunneling is a method for VPN clients to pass encrypted IPsec traffic through firewalls and network/port address translation devices (nat/pat) which are commonly found on the network. If you are behind a firewall, or are not on the UF network and have a private IP address (10.x.x.x, 172.16-31.x.x, or 192.168.x.x) you will need to use transparent tunneling. Luckily, the UF distribution of the vpn client has it turned on by default.

QUESTION NO: 5
The newly appointed TestKing trainee technician wants to know which of the following features will enable the Concentrator administrator to centrally define a set of rules for the Cisco VPN Client firewall. What will your reply be?

A. AYT
B. CIC Firewall

C. CPP

D. Stateful Firewall

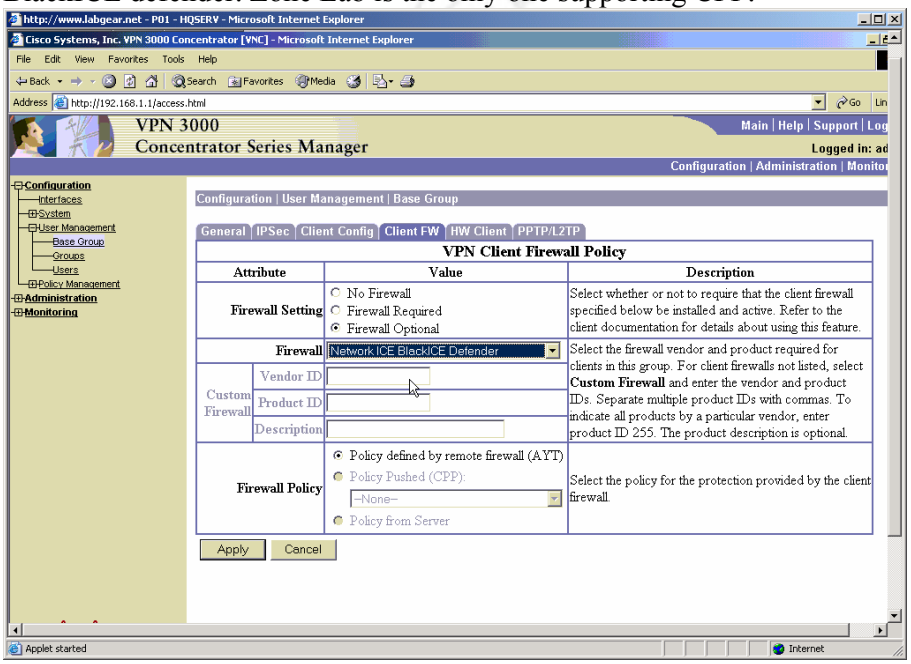
Answer: C
Explanation:
Central Policy Protection (CCP) is a state full firewall policy that leverages the Cisco Integrated Client (CIC) feature by letting the VPN concentrator manage the client firewall policies, the client firewall policies are managed by the administrator

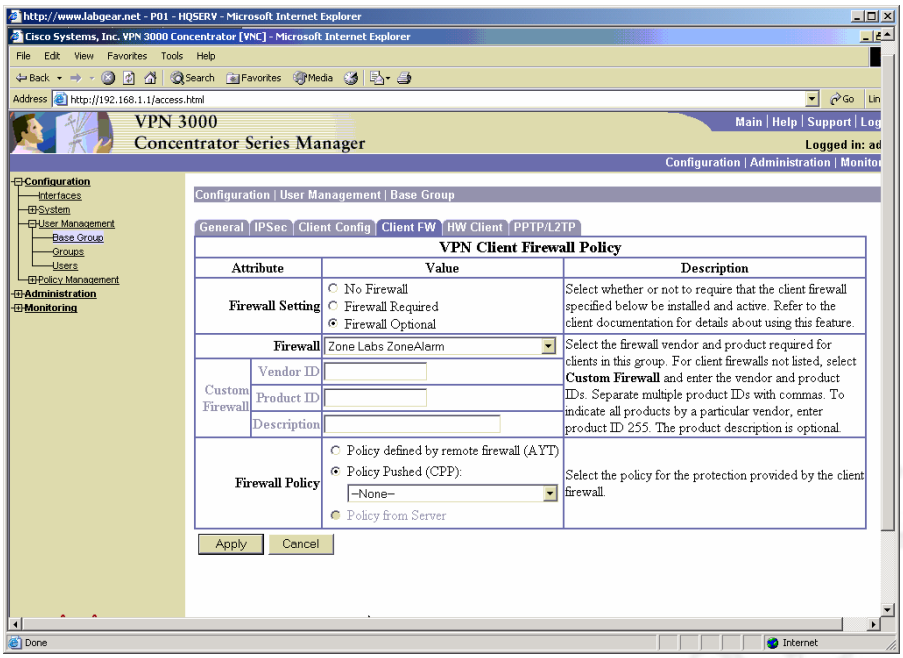
CCSP: All in one exam guide page 404

QUESTION NO: 6
Cisco Central Policy Protection is capable of supporting which of the firewalls?

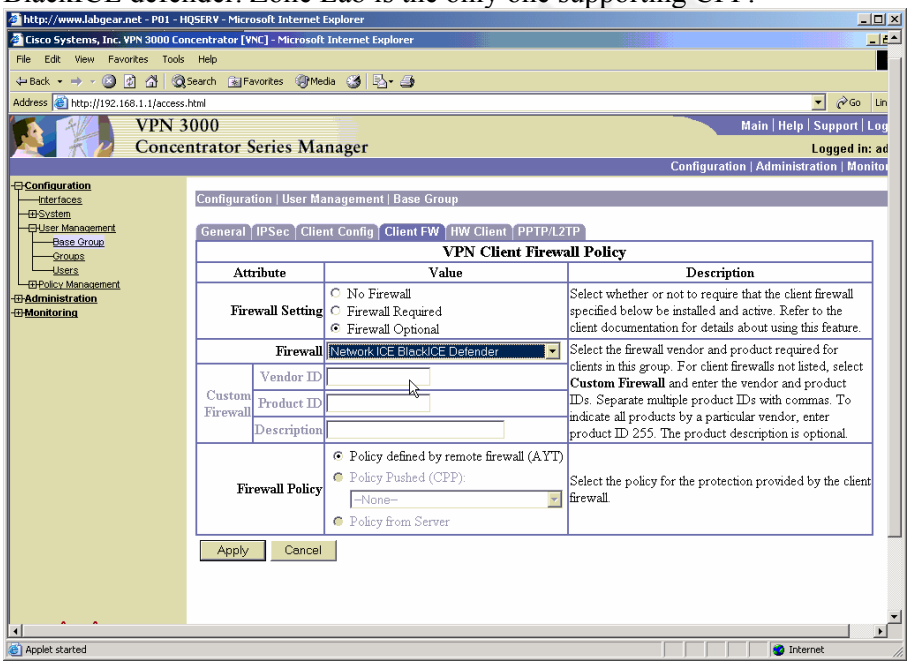
A. Symantec
B. Zone Labs
C. Cyberguard
D. Network Ice BlackICE defender

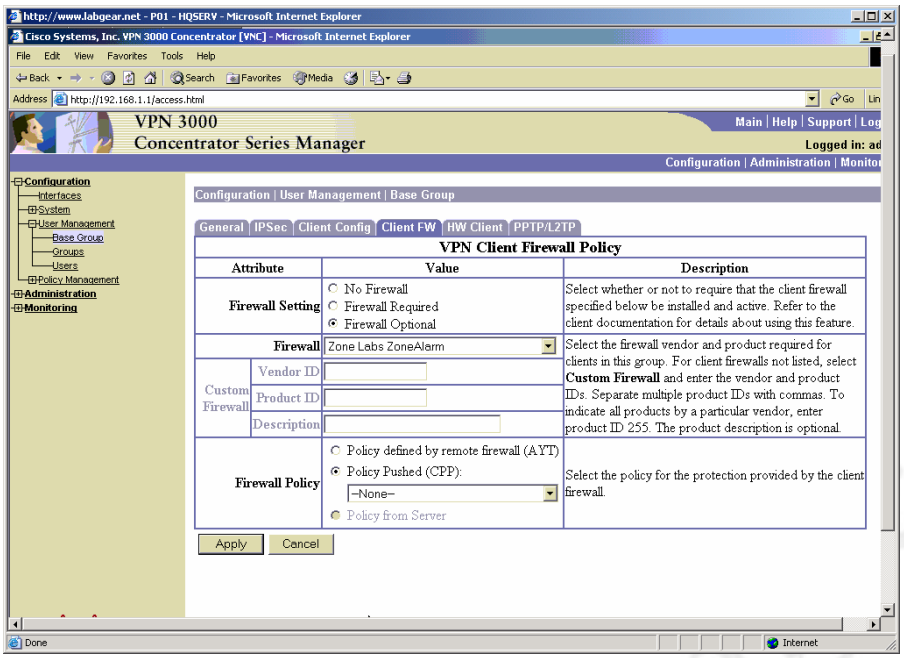
Answer: B
Explanation:
Symantec and Cyberguard is not an option, so we stand between Zone Labs and Network Ice BlackICE defender. Zone Lab is the only one supporting CPP.





Symantec and Cyberguard is not an option, so we stand between Zone Labs and Network Ice BlackICE defender. Zone Lab is the only one supporting CPP.





QUESTION NO: 7
Which of the following allows the Head End Concentrator to push a security policy to a remote VPN client?

A. FTP
B. LMI
C. CPP
D. AYT

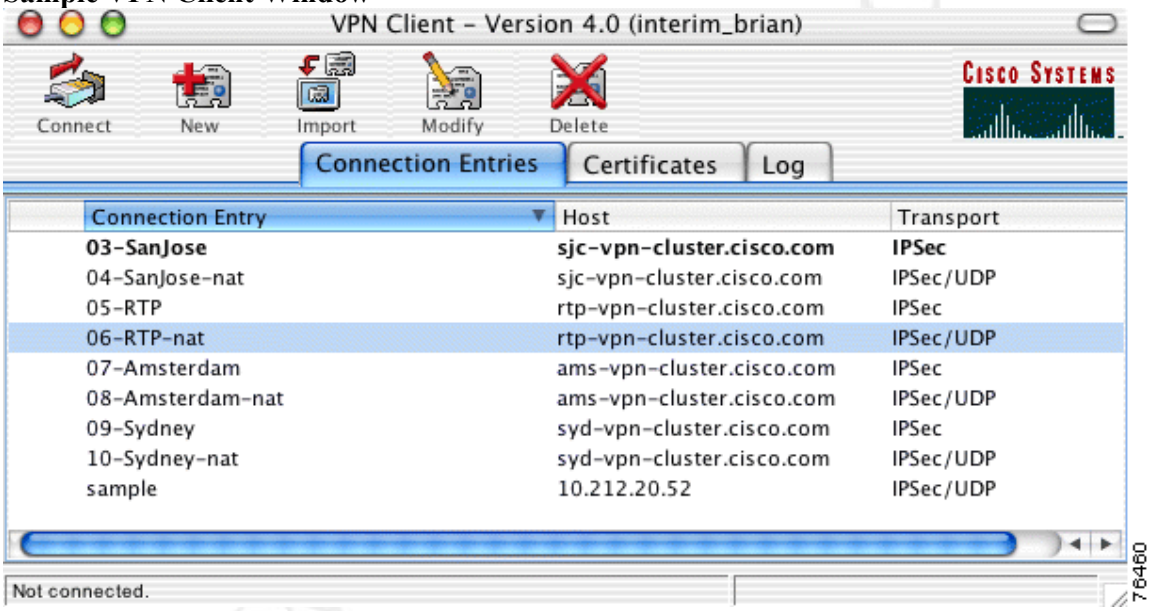
Answer: C
Explanation:
The Head End Concentrator can push a security policy to a remote client via Centralized Protection Policy (CPP).

Section 4: Software Client's firewall statistics (3 questions)

QUESTION NO: 1
Jason the security administrator for Testking Inc. is working on the Cisco VPN Client. How can Jason monitor IPSec sessions on the Cisco VPN Client?

A. Jason can monitor IPSec sessions in the Monitor-screen | Encryption
B. Jason can monitor IPSec sessions in the Cisco VPN Client Connection Status window
C. Jason can monitor IPSec sessions in the Monitor-Sessions screen
D. Jason can monitor IPSec sessions in the Monitor-Routing table

Answer: B
Explanation:
Sample VPN Client Window



QUESTION NO: 2
Under which VPN client status tab will show the encryption type used on the tunnel to the Concentrator?

A. firewall
B. statistics
C. general
D. options

Answer: C
Explanation:
The VPN software client tab General will show the encryption type used to connect to the Concentrator

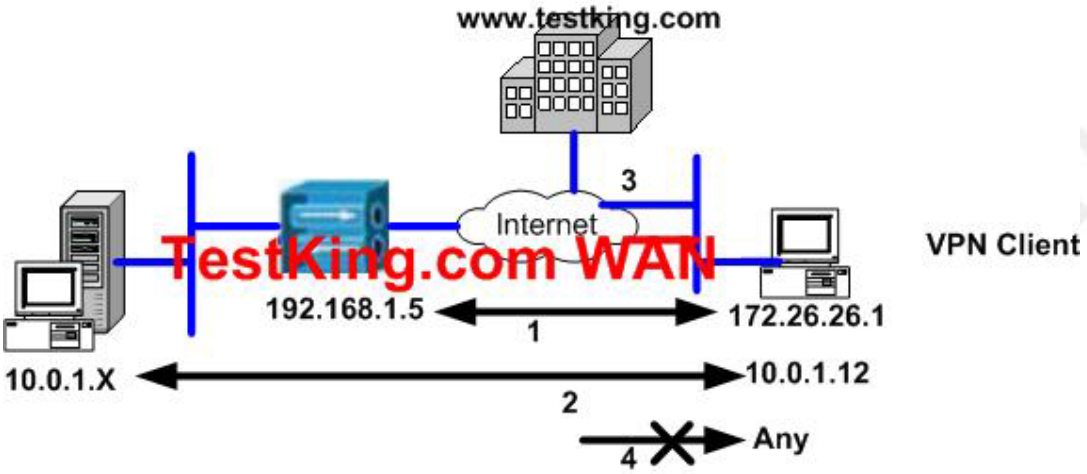
QUESTION NO: 3
What is the system tray icon for a VPN software client?

A. chain
B. lock
C. key
D. a red C

Answer: B
Explanation:
The system tray icon for a VPN software client is a padlock.

Section 5: Customizing firewall policy (4 questions)

QUESTION NO: 1
Exhibit:



Connection	Action	Direction	Source Address	Destination Address
1	10	Inbound	10	Local
	10	Outbound	Local	10
2	11	Inbound	11	Local
	11	Outbound	Local	11
3	12	Outbound	Local	12
4	13	Inbound	13	Local
	13	Outbound	Local	13

John the security administrator for Testking must troubleshoot a problem on the network. For connection 1 of the firewall policy chart, choose the action and IP addresses.

A. Action forward, source and destination address, 192.168.1.5
B. Action drop, source and destination address, 192.168.1.5
C. Action forward, source and destination address, 182.168.1.0
D. Action drop, source and destination address, 192.168.1.0

Answer: A
Explanation:
A firewall rule includes the following fields:

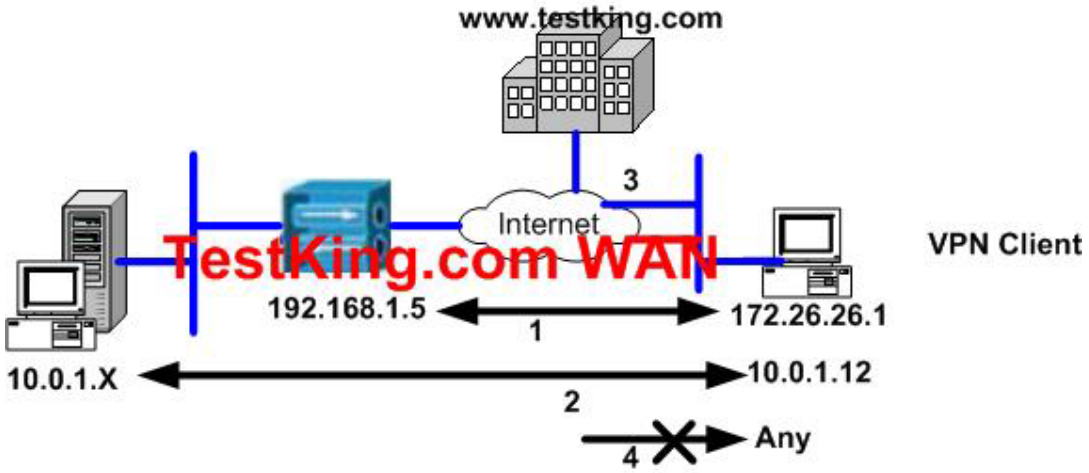
- **Action—The action taken if the data traffic matches the rule:**
  - Drop = Discard the session.
  - Forward = Allow the session to go through.

- **Direction—The direction of traffic to be affected by the firewall:**
  - Inbound = traffic coming into the PC, also called local machine.

- Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.

- **Source Address—The address of the traffic that this rule affects:**
  - Any = all traffic; for example, drop any inbound traffic.
  - This field can also contain a specific IP address and subnet mask.
  - Local = the local machine; if the direction is Outbound then the Source Address is local.
- **Destination Address—The packet's destination address that this rule checks (the address of the recipient).**
  - Any = all traffic; for example, forward any outbound traffic.
  - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- **Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).**
- **Source Port—Source port used by TCP or UDP.**
- **Destination Port—Destination port used by TCP or UDP.**

QUESTION NO: 2
Exhibit:



Connection	Action	Direction	Source Address	Destination Address
1	10	Inbound	10	Local
	10	Outbound	Local	10
2	11	Inbound	11	Local
	11	Outbound	Local	11
3	12	Outbound	Local	12
4	13	Inbound	13	Local
	13	Outbound	Local	13

Jason the security administrator for Testking Inc. is troubleshooting the network. For connection 2 of the firewall policy chart, Jason must choose the action and the IP addresses.

A. Action drop, source and destination address, 10.0.1.0
B. Action forward, source and destination address, 10.0.1.0

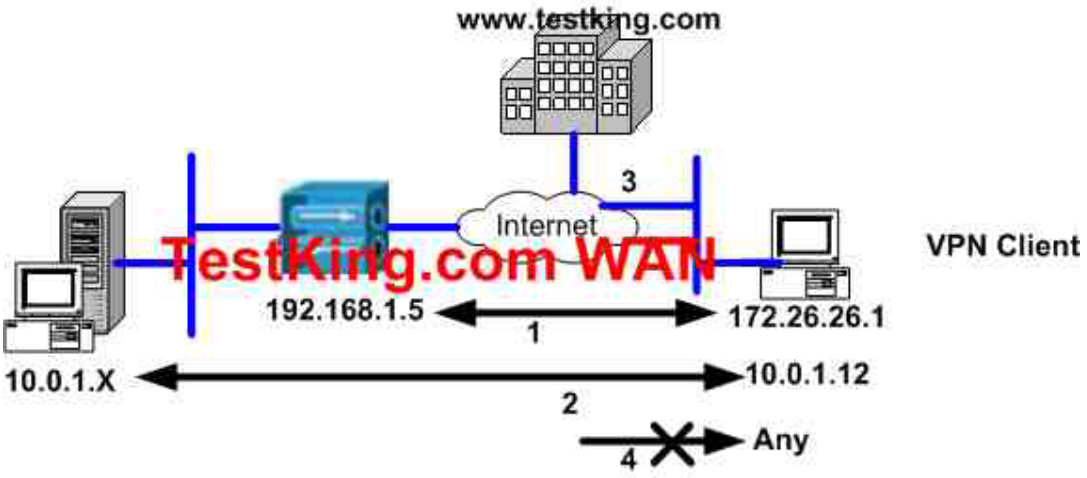
C. Action forward, source and destination address 10.0.1.10
D. Action drop, source and destination address, 10.0.1.10

Answer: B
Explanation:
A firewall rule includes the following fields:

- **Action—The action taken if the data traffic matches the rule:**
  - Drop = Discard the session.
  - Forward = Allow the session to go through.

- **Direction—The direction of traffic to be affected by the firewall:**
  - Inbound = traffic coming into the PC, also called local machine.
  - Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.
- **Source Address—The address of the traffic that this rule affects:**
  - Any = all traffic; for example, drop any inbound traffic.
  - This field can also contain a specific IP address and subnet mask.
  - Local = the local machine; if the direction is Outbound then the Source Address is local.
- **Destination Address—The packet's destination address that this rule checks (the address of the recipient).**
  - Any = all traffic; for example, forward any outbound traffic.
  - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- **Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).**
- **Source Port—Source port used by TCP or UDP.**
- **Destination Port—Destination port used by TCP or UDP.**

QUESTION NO: 3
Study the Exhibit below carefully:



Connection	Action	Direction	Source Address	Destination Address
1	10	Inbound	10	Local
	10	Outbound	Local	10
2	11	Inbound	11	Local
	11	Outbound	Local	11
3	12	Outbound	Local	12
4	13	Inbound	13	Local
	13	Outbound	Local	13

According to the diagram, the firewall feature was enabled on the VPN Client. You can view the VPN Client's firewall policy for the four connection types, labeled 1 through 4 in the diagram (Bottom half of the diagram.) by clicking on the Firewall tab of the VPN Client connection status windows.

Connection 4 displays the default policy that is applied to traffic from source address X; and any local outbound traffic returning to its destination address X will have action Y applied to this traffic.

Which of the following would be the correct action, source and destination address for this policy?

A. action forward, source and destination address, any
B. action forward, source and destination address, www.testking.com
C. action drop, source and destination address, any
D. action drop, source and destination address, www.testking.com

Answer: C
A firewall rule includes the following fields:

- **Action—The action taken if the data traffic matches the rule:**
  - Drop = Discard the session.
  - Forward = Allow the session to go through.

- **Direction—The direction of traffic to be affected by the firewall:**
  - Inbound = traffic coming into the PC, also called local machine.
  - Outbound = traffic going out from the PC to all networks while the VPN Client is connected to a secure gateway.
- **Source Address—The address of the traffic that this rule affects:**
  - Any = all traffic; for example, drop any inbound traffic.
  - This field can also contain a specific IP address and subnet mask.
  - Local = the local machine; if the direction is Outbound then the Source Address is local.

- **Destination Address—The packet's destination address that this rule checks (the address of the recipient).**
    - Any = all traffic; for example, forward any outbound traffic.
    - Local = The local machine; if the direction is Inbound, the Destination Address is local.
- **Protocol—The Internet Assigned Number Authority (IANA) number of the protocol that this rule concerns (6 for TCP; 17 for UDP and so on).**
- **Source Port—Source port used by TCP or UDP.**
- **Destination Port—Destination port used by TCP or UDP.**

QUESTION NO: 4
What three configuration steps must be completed to create a custom firewall policy when configuring a custom firewall policy in the VPN Concentrator? Choose three.

A. Assign the new rule to Cisco CCP.

B. Associate the new rule with the new policy.

C. Assign the new policy to Cisco CCP

D. Define a rule to restrict traffic.

E. Associate the new policy with a rule.

F. Define a new policy.

Answer: B, C, D
Explanation: Building custom CPP policies is a four step process on the concentrator.
Step 1: Define rules to restrict traffic
Step 2: Add a new policy (called a filter on the VPN concentrator)
Step 3: Associate the new rules with the newly created policy
Step 4: Assign the new policy to the CPP

This is a tricky one. Both F and D can be correct; however, as we can only choose a total of 3, one must go.
Because Cisco writes "Add" and not "Define" in step 2, i would go with answer D instead of F
Reference: Ciscopress CCSP Self Study, CSVPN Second edition Page: 200

Topic 6, Configure the Cisco Virtual Private Network Client Auto-Initiation Feature (10 questions)

Section 1: Overview of the Cisco VPN Software Client auto-initiation (6 questions)

QUESTION NO: 1
What is the function of the auto-initiate retry time?

A. It will specify the waiting period (in minutes) before retrying a failed connection
B. It will specify the number of retries before auto-initiate Are You Thee polling commences
C. It will specify the waiting period (in seconds) before retrying a failed connection
D. It will specify the number of retries before auto-initiate is suspended

Answer: A
AutoInitiationRetryInterval—specifies the number of minutes to wait before retrying an auto initiation connection. The range is one to ten minutes. If you don't include this parameter in the file, the default retry interval is one minute.

QUESTION NO: 2
Which of the following statements regarding VPN client auto-imitate feature is valid?

A. The auto-initiation features is automatically configured in the VPN clinet.ini file but disabled by default.
B. The auto-initiation feature is automatically configured in the VPNclient.pcf file but disabled by default.
C. The auto-initiation feature is not resident In the VPNclient.ini file y default, it must be added.
D. The auto-initiation feature is not resident in the VPNclient

Answer: C
Explanation:
When your network administrator has configured your VPN Client for auto initiation (by including it in the vpnclient.ini file), the Options menu includes the option Automatic VPN Initiation. When you select this option, the VPN Dialer displays a dialog box that lets you

enable/disable auto initiation and change the setting of the retry interval. Disabling auto initiation in this way does not remove it from your configuration. If you need to enable auto initiation after you have disabled it, you can return to this dialog box and enable it again. The only way you can remove auto initiation from your configuration is through editing the vpnclient.ini file.

QUESTION NO: 3
What does the Auto-Initiation List parameter define under the auto-initiate parameters?

A. list of auto-initiation supported Concentrator addresses
B. list of auto-initiation supported network addresses
C. list of auto-initiation section names within the VPNclient.ini file
D. list of auto-imitation supported host addresses

Answer: C

Explanation: Explanation:
To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

- AutoInitiationEnable—enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.
- AutoInitiationRetryInterval—specifies the number of minutes to wait before retrying an auto initiation connection. The range is 1 to 10 minutes or 5 to 600 seconds. If you do not include this parameter in the file, the default retry interval is one minute.
- AutoInitiationRetryIntervalType—specifies whether the retry AutoInitiationRetryInterval parameter is displayed in minutes or seconds. The default is minutes.
- AutoInitiationList—provides a series of section names, each of which contains a network address, a subnet mask, a connection entry name, and optionally, a connect flag. You can include a maximum of 64 section (network) entries.
  -
    - The section name is the name of an entry in the auto initiation list (within brackets)
    - The network and subnet mask identify a subnet
    - The connection entry specifies a connection profile (.pcf file) configured for auto initiation.
    - The connect flag, if present, indicates the action to take if there is a match. If the Connect parameter is set to 1, the VPN Client should auto initiate; if 0, the VPN Client should not auto initiate. The default setting is 1. This parameter is optional. You can use it to exclude certain network ranges from auto initiation. For example, you might want to address a situation where Mobile IP and VPN

software clients co-exist on client PCs and you want the VPN Client to auto initiate when not on a corporate subnet.

QUESTION NO: 4
What color is the padlock icon in system tray for the VPN software client, when the client is attempting to Auto Initiate a connection?

A. black
B. yellow
C. red
D. green

Answer: D
Explanation:
The system tray icon is an open green lock when the client is attempting Auto Initiation.

QUESTION NO: 5
If your VPN software client is Auto-Initiating a connection to a Concentrator, but is cancelled, how long will the client wait before trying to connect again?

A. 5 seconds
B. 30 seconds
C. 2 minutes
D. 5 minutes
E. 10 minutes

Answer: C
Explanation:
When Auto-Initiation is cancelled, the client will attempt a new connection to the Concentrator every 2 minutes.

QUESTION NO: 6
The TestKing CEO is curious as to what the function of the auto-initiate retry timer is. What can you tell her?

A. specifies the time (in minutes) to wait before retrying to wait before retrying a failed connection
B. specifies the number of retries before auto-initiate is suspended
C. specifies the number of retries before auto-initiate Are You There polling commences

Answer: A

Explanation:
To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

- AutoInitiationEnable—enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.
- AutoInitiationRetryInterval—specifies the number of minutes to wait before retrying an auto initiation connection. The range is 1 to 10 minutes or 5 to 600 seconds. If you do not include this parameter in the file, the default retry interval is one minute.
- AutoInitiationRetryIntervalType—specifies whether the retry AutoInitiationRetryInterval parameter is displayed in minutes or seconds. The default is minutes.
- AutoInitiationList—provides a series of section names, each of which contains a network address, a subnet mask, a connection entry name, and optionally, a connect flag. You can include a maximum of 64 section (network) entries.
    -
    - The section name is the name of an entry in the auto initiation list (within brackets)
    - The network and subnet mask identify a subnet
    - The connection entry specifies a connection profile (.pcf file) configured for auto initiation.
    - The connect flag, if present, indicates the action to take if there is a match. If the Connect parameter is set to 1, the VPN Client should auto initiate; if 0, the VPN Client should not auto initiate. The default setting is 1. This parameter is optional. You can use it to exclude certain network ranges from auto initiation. For example, you might want to address a situation where Mobile IP and VPN software clients co-exist on client PCs and you want the VPN Client to auto initiate when not on a corporate subnet.

Section 2: Configure the Cisco VPN Software Client auto-initiation (4 questions)

QUESTION NO: 1
At what stage is the auto VPN initiation menu item available from the VPN client GUI?

A. It is available by default.
B. after auto-initiate dll is added to the Cisco Systems VPN Client folder
C. after AutoInitiateEnable=1 line is added to VPNclient.ini file
D. after AutoInitiateEnable=1 line is added to VPNclient.pcf file

Answer: C
Explanation: To configure auto initiation for users on the network, you add parameters to the VPN Client's global profile (vpnclient.ini). For information on how to create or use a global profile, see "Creating a Global Profile."

The only configurable features available to the user through the VPN Client GUI application are the ability to disable auto initiation and the ability to change the retry interval. These features are available through the Options menu when auto initiation has been configured through the global profile. If auto initiation is not configured, these options do not appear in the Options menu. When auto initiation is configured, some VPN Client status displays and dialog boxes differ slightly from standard connection dialog boxes to indicate to the user that auto initiation is occurring. For a complete explanation of how auto initiation appears to the VPN Client user, see Cisco VPN Client User Guide for Windows, "Using Automatic VPN Initiation."

To configure auto initiation, you must add the following keywords and values in the [Main] section of the vpnclient.ini global profile file:

AutoInitiationEnable—enables or disables auto initiation. To enable auto initiation, enter 1. To disable it, enter 0.

QUESTION NO: 2
Which of the following is specified by the AutoInitiationList parameter?

A. Section names

Answer: A
AutoInitiationList – A list of auto-initiation related **section names** within the INI file.

QUESTION NO: 3
Which of the following files will you advice the new TestKing trainee technician to modify to enable the Cisco VPN Software Client Auto-Initiation feature?

A. The main.ini file

B. The user.ini file

C. The client.ini file

D. The vpclinet.ini file

Answer: D
Explanation:
When your network administrator has configured your VPN Client for auto initiation (by including it in the vpnclient.ini file), the Options menu includes the option Automatic VPN Initiation When you select this option, the VPN Dialer displays a dialog box that lets you enable/disable auto initiation and change the setting of the retry interval. Disabling auto initiation in this way does not remove it from your configuration. If you need to enable auto initiation after you have disabled it, you can return to this dialog box and enable it again. The only way you can remove auto initiation from your configuration is through editing the vpnclient.ini file.

QUESTION NO: 4
On your VPN software client, how do you change the Auto-Initiate retry interval?

A. options, settings, auto initiate
B. options, automatic vpn initiation
C. options, auto initiate setup
D. options, initiation timer interval

Answer: B
Explanation:
You can change the timer of the Auto-Initiation timer on your VPN software client from options, automatic vpn initiation.

Topic 7, Monitor and Administer Cisco VPN 3000 Remote Access Networks (22 questions)

Section 1: Monitoring (6 questions)

QUESTION NO: 1
John the I.T administrator at Testking Inc. is working on the Monitoring Sessions screen. He needs to know which data is shown on the Monitor Sessions screen. (Choose three)

A. The screen shows Tunnel summary
B. The screen shows Session summary
C. The screen shows LAN-to-LAN sessions
D. The screen shows Client tunnels
E. The screen shows Remote access sessions
F. The screen shows Site-to-site tunnels

Answer: B C E
Explanation:
Session Summary Table
This table shows summary totals for LAN-to-LAN, remote access, and management sessions. A session is a VPN tunnel established with a specific peer. In most cases, one user connection = one tunnel = one session. However, one IPSec LAN-to-LAN tunnel counts as one session, but it allows many host-to-host connections through the tunnel.

- **Active LAN-to-LAN Sessions** - The number of IPSec LAN-to-LAN sessions that are currently active.
- **Active Remote Access Sessions -** The number of PPTP, L2TP, IPSec remote-access user, L2TP over IPSec, and IPSec through NAT sessions that are currently active.
- **Active Management Sessions -** The number of administrator management sessions that are currently active.
- **Total Active Sessions -** The total number of sessions of all types that are currently active.
- **Peak Concurrent Sessions -** The highest number of sessions of all types that were concurrently active since the VPN Concentrator was last booted or reset.
- **Concurrent Sessions Limit -** The maximum number of concurrently active sessions permitted on this VPN Concentrator. This number is model-dependent, for example, model 3060 = 5000 sessions.
- **Total Cumulative Sessions** - The total cumulative number of sessions of all types since the VPN Concentrator was last booted or reset.

QUESTION NO: 2
The administrator would like to verify that the proper *orgid* was entered in the configuration. However, the Cisco IOS IDS is not communicating with its Postoffice

group.

What command should he be running to see the *orgid* on the router?

A. show ip audit statistics
B. show ip audit interface
C. show ip audit detail
D. show ip audit configuration

Answer: D
Explanation: Use the show ip audit configuration EXEC command to display additional configuration information, including default values that may not be displayed using the show run command.

The following example displays the output of the **show ip audit** configuration command:

Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)
Audit Rule Configuration
Audit name AUDIT.1
info actions alarm

QUESTION NO: 3
Study the Exhibit below carefully:

TestKing2(config)#**ip audit po protected 10.10.10.1 to 10.10.10.254**
TestKing 2(config)#**ip audit po protected 10.10.20.1 to 10.10.20.254**

Will the IOS IDS Firewall still offer IDS functionality to each network after the commands shown above are entered when all the interfaces of TestKing 2 has IDS rules applied to it?

A. No, the **ip audit po protected** command can only be entered once. The range should be *10.10.0.0 to 10.10.20.255*.
B. No, the 10.10.10.0 network must be entered with the **ip audit po protected** command to be protected.
C. Yes, the **ip audit po protected** command affects logging records only, not IDS security functionality.
D. Yes, entering the mandatory **ip audit po protected** command for any network enables protection for all networks on the router.

Answer: C
The commands only affect the logging behavior.

QUESTION NO: 4
If a user has a session established through a 3002 Hardware Client, when will the session be dropped after a period of inactivity?

A. 5 minutes
B. 20 minutes
C. 30 minutes
D. 1 hour

Answer: C
Explanation:
A users session will be dropped after 30 minutes of inactivity on the 3002 Hardware Client.

QUESTION NO: 5
On a 3000 series Concentrator, where do you view the IP routing table?

A. configuration, system, ip routing, routing table
B. configuration, system, routing table
C. monitoring, routing table
D. monitoring, protocols

Answer: C
Explanation:
The 3000 series Concentrator IP routing table is located on the monitoring, routing table screen.

QUESTION NO: 6
Which of the following are main tabs under the Concentrator monitoring screen? Choose all that apply.

A. routing table

B. protocols
C. certificate management
D. software update
E. statistics

Answer: A,E
Explanation:
There are five tabs under the Concentrators monitoring screen: Routing Table, Filterable Event Log, System Status, Sessions, and Statistics.

Section 2: Administration (13 questions)

QUESTION NO: 1
The security team at Testking Inc. is working on the Cisco VPN Concentrator. There are times when there are multiple concurrent Cisco VPN Concentrator administration sessions at Testking Inc. What configuration privileges does each additional administrator have?

A. The additional administrators have read and write privileges
B. The additional administrators have read only
C. The administrators all have the same privileges
D. The additional administrators have monitor only

Answer: D
Explanation:
This is a hard question, the administrators all have the same rights until the first administrator locks the configuration. The key word in the question is **additional, so the answer would have to be monitoring.**

The lock icon indicates the administrator who has the configuration lock, that is, the person who has the right to make changes to the active system configuration.

Configuration locked by
The administrator (IP address or Console) who has the right to make changes to the active system configuration. The configuration is locked by the administrator who first makes a change to the active (running) configuration. That administrator holds the lock until logout, or until the Session Idle Timeout period expires (see the Administration | Access Rights | Access Settings screen). For example, an administrator who is just viewing and refreshing statistics on a Monitoring screen for longer than the timeout period, loses the lock.

Reference: VPN 3000 Concentrator Ref Volume 2. Configuration 4.0.pdf

QUESTION NO: 2
Peter the security administrator at Testking Inc. is working on the Cisco VPN Concentrator. After he made some changes to the Cisco VPN Concentrator, he rebooted the system but forgot to save the changes he made.
In the GUI, what happens if you reboot without saving the configuration changes?

A. The Cisco VPN Concentrator configuration changes remain.
B. The Cisco VPN Concentrator system does not allow you to reboot without saving.
C. The Cisco VPN Concentrator system warns you that the configuration changes will be lost, do you still want to proceed.
D. The Cisco VPN Concentrator configuration changes are lost.

Answer: D
Explanation:

Reboot without saving the active configuration = Reboot using the existing CONFIG file and without saving the active configuration. (This is the default selection.)

Reference: VPN 3000 Concentrator Ref Volume 2. Config 4.0.pdf

QUESTION NO: 3
Robert the security administrator for Testking Inc. is working LAN-to-LAN tunnel. Where can Robert the administrator, verify that the LAN-to-LAN tunnel was established?

A. View | IPSec Tunnels
B. Monitor | Tunnels
C. Monitor | Systems
D. Administration | Sessions

Answer: D
Explanation:
Administration | Administer Sessions
This screen shows comprehensive statistics for all active sessions on the VPN Concentrator. You can also click the name of a session to see detailed parameters and statistics for that session. See Administration | Sessions | Detail.
Group

Choose a group from the menu to monitor statistics for that group only. The default is --All-- which displays statistics for all groups.

Logout All: PPTP User | L2TP User | IPSec User | L2TP/IPSec User | IPSec/NAT User | IPSec/LAN-to-LAN
These active labels let you log out *all* active sessions of a given tunnel type at once:
- PPTP User = PPTP remote-access users
- L2TP User = L2TP remote-access users
- IPSec User = IPSec remote-access users
- L2TP/IPSec User = L2TP over IPSec users
- IPSec/NAT User = IPSec through NAT users
- IPSec/LAN-to-LAN = IPSec LAN-to-LAN

QUESTION NO: 4
The security team at Testking Inc., wants to know what can you do in the images tab of AUS?

A. You can add and delete PIX OS images
B. You can add and delete PDM images
C. You can delete but not add configuration files
D. You can add but not delete PDM images
E. You can add but not delete configuration files

Answer: E
Explanation: There is no way to accurately answer this question, since Cisco makes it clear in their documentation that you can neither add nor delete configuration files in AUS. You have to do this in PIX MC.

QUESTION NO: 5
In which way would you load the boot configuration file and make it the active configuration when you need to perform swap configuration?

A. write to the config file
B. save the Config.bak file and reboot the system
C. reboot the system
D. update the Cisco VPN executable system software

Answer: C
To reload the boot configuration file and make it the active configuration, you must reboot the system. When you click OK, the system automatically goes to the Administration | System Reboot screen, where you can reboot the system. You can also click the highlighted link to go to that screen.

OK / Cancel
To swap CONFIG and CONFIG.BAK files, click OK. The Manager goes to the Administration | System Reboot screen.

To leave the files unchanged, click Cancel. The Manager returns to the Administration | File Management screen.

QUESTION NO: 6
Refer to the commands illustrated, if there is a reference to a *4050 UDP Bomb (Attack, Atomic)* in the logs, all of the following occurred EXCEPT:

```
router(config)#ip audit name NIDS info action alarm
router(config)#ip audit name NIDS attack action alarm drop reset
router(config-if)#ip audit NIDS in
```

A. The attack triggered an alarm
B. The packet was dropped
C. The IOS IDS detected the attack attempt
D. The attack forced a reset packet to be sent

Answer: D
Only TCP sessions can be reset!
UDP is not session-orientated, and so there is no session that could be reset.

QUESTION NO: 7
How can you schedule a reboot time for you 3000 series Concentrator?

A. administration, general
B. administration, system reboot
C. administration, administer sessions
D. administration, access settings

Answer: B
Explanation:
Schedule a reboot or a shutdown of your Concentrator from the administration, system reboot screen.

QUESTION NO: 8
Which of the following are valid preconfigured accounts on a Concentrator? Choose all that apply.

A. user
B. mis
C. admin
D. isp
E. config

Answer: A,B,C,D,E
Explanation:
These are the five predefined user accounts on a Concentrator.

QUESTION NO: 9
By default, what period of inactivity will cause a Concentrator to log out an administrative session?

A. 2 minutes
B. 5 minutes
C. 8 minutes
D. 10 minutes

Answer: D
Explanation:
If you are administratively logged into a Concentrator, by default you will be logged out after ten minutes of inactivity.

QUESTION NO: 10
What do you press from your management console to reset the administrative password on a Concentrator?

A. Control + Z
B. Control + C
C. Alt + Y
D. Alt + H

Answer: B
Explanation:
You can reset the administrative password on a Concentrator, by pressing the control key plus the letter c, right after seeing the three periods (?) appear on the screen after a reboot.

QUESTION NO: 11
How do you encrypt your Concentrator configuration file?

A. configuration, system, tunneling protocols, encryption
B. configuration, system, management protocols, backup
C. administration, access rights, access settings
D. administration, file management, swap config file

Answer: C
Explanation:
If you need your configuration file stored in encrypted form, go to the Concentrator administration, access rights, access settings screen.

QUESTION NO: 12
On a Concentrator, where can you configure a required software version a remote client must have before connecting to the Concentrator?

A. configuration, system, management protocols, software update
B. configuration, system, events, auto update
C. administration, software update, clients
D. administration, access rights, access settings

Answer: C
Explanation:
To require that remote clients connecting to a Concentrator have a specific software version (or higher) go to administration, software update, clients.

QUESTION NO: 13
How do you upgrade your Concentrator's software image?

A. administration, file management, system update
B. administration, software update, concentrator
C. administration, system reboot, system update
D. administration, access rights, software update

Answer: B
Explanation:
From your Concentrator, select administration, software update, then concentrator to upgrade your Concentrator software version.

Section 3: Bandwidth Management (3 questions)

QUESTION NO: 1
Kathy and Jason the security department heads are in charge of configuring a bandwidth policy. They know that configuring a bandwidth policing policy is a two-step process: configuring, then applying the policy.
Where is the configured bandwidth policies applied on the VPN Concentrator? (Choose three)

A. It must be applied to an interface.
B. It can optionally be applied to an interface.
C. The bandwidth policy must be applied to a group.
D. It can be optionally applied to a group.
E. It must be applied to a LAN-to-LAN tunnel.
F. It can be optionally applied to a LAN-to-LAN tunnel.

Answer: A, D, F
Explanation:
A: MUST be defined and applied to an interface before applying group reservation policies
D: If not applied, the default defined on the interface is used
F: SUGGESTED to apply, otherwise there is no guarantee that the tunnel will come up again, if all bandwidth is needed by users.
… If not applied, the default defined on the interface is used.

QUESTION NO: 2
The Testking Inc. I.T administrative team can not figure out what the two bandwidth management features available on the VPN Concentrator are. (Choose two)

A. Create Traffic shaping
B. Create a Bandwidth Management Policy
C. Weighted fair queuing
D. Create custom queuing
E. Use bandwidth Reservation
F. Use bandwidth shaping

Answer: B E
Explanation:

Task	Use this Screen...	Do this...
Create a Bandwidth Management Policy	Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add	Name the policy, then apply reservation and/or policing and set the corresponding parameters.
Enable Bandwidth Management on the Public	Configuration | Interfaces | Ethernet	Check the Bandwidth Management

Interface	2, Bandwidth tab	check box. Set the link rate. Apply a bandwidth management policy.
Use Bandwidth Policing	Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify	Create a policing policy: Check the Policing check box and enter the policing rate and burst size.
Use Bandwidth Reservation	Configuration | Policy Management | Traffic Management | Bandwidth Policies | Add or Modify	Create a reservation policy: Check the Bandwidth Reservation check box and enter the minimum bandwidth.
Use Bandwidth Aggregation	Configuration | User Management | Groups | Bandwidth Policy | Interfaces	Set Aggregate Bandwidth to a value greater than zero.
Assign Bandwidth Policy(ies) to:		
• Interface	Configuration | Interfaces | Ethernet 2, Bandwidth tab	Choose a policy from the Bandwidth Policy drop-down menu.
• Group	Configuration | User Management | Groups | Bandwidth Policy | Interfaces	Choose a policy from the Policy drop-down menu.
• LAN-to-LAN	Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN | Add or Modify	Choose a policy from the Bandwidth Policy drop-down menu.

Reference: VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring

QUESTION NO: 3
What is the purpose of the bandwidth policing feature?

A. Provision of a minimum and maximum data transfer rate to a remote user.
B. Provision of a maximum data transfer rate to a remote user.
C. Provision of a minimum and maximum data transfer rate with an excess burst size to a remote user.
D. Provision of a maximum data transfer rate with a maximum burst size to a remote user.

Answer: D
Explanation:
The policing rate is the maximum limit on the rate of sustained tunneled traffic.
The burst size indicates the maximum size of an instantaneous burst of bytes allowed before traffic is capped back to the policing rate.
-> Both, Policing Rate (= maximum data transfer rate) AND maximum Burst Size are Bandwidth Policing entities.

Topic 8, Configure the Cisco VPN 3002 Hardware Client for Remote Access (13 questions)

Section 1: Cisco VPN 3002 Hardware client remote access with pre-shared keys (13 questions)

QUESTION NO: 1
James the security administrator at Testking Inc. is working on configuring the network extension mode. His first job is to know what the two steps in configuring network extension mode are. (Choose two)

A. You must enable network extension mode on the Cisco VPN Concentrator and push it down to the Cisco VPN 3002 during tunnel establishment.
B. You must answer No when the Cisco VPN 3002 prompts you to use PAT mode.
C. You must change the default address on the Cisco VPN 3002 private interface.
D. You must change the default address on the Cisco 3002 public interface.
E. You must enable network extension mode on the private interface.
F. You must enable network extension mode on the public interface.

Answer: B C
Explanation:

4. In the Main window, select **Quick Configuration** from the menu. Follow the online instructions for all subsequent screens. Note that to configure Network Extension mode, you must change the private interface IP address and disable PAT.

QUESTION NO: 2
John the security administrator at Testking Inc. is working on configuring the Cisco VPN 3002. John wants to know what is the default configuration of the Cisco VPN 3002 public interface.

A. The public interface has DHCP server enabled.
B. The public interface has Static IP address of 92.168.10.1
C. The public interface has No configuration
D. The public interface has DHCP client enabled.

Answer: D
Explanation:
Configure the VPN 3002 public interface, using DHCP, PPPoE, or static address assignment. Note that the DHCP client is enabled by default on the public interface.

QUESTION NO: 3
The TestKing CEO wants to know which of the following is the default configuration of the Cisco VPN 3002 private interface. What will your reply be?

A. DHCP server is enabled
B. DHCP client is enabled
C. static IP address of 192.168.10.1
D. enabled with an IP address of 0.0.0.0

Answer: C
Explanation: The default configuration for the VPN 3002 clients private interface is a static IP address with the value of 192.168.10.1

QUESTION NO: 4
What is the default status of the VPN tunnel when the Cisco VPN 3002 is fully configured in client mode?

A. The tunnel is up automatically.
B. The manual and automatic modes are defined on the Cisco VPN Concentrator and then pushed to the Cisco VPN 3002 during tunnel establishment.
C. The tunnel must be manually initiated via the Monitoring-tunnel status screen.
D. The tunnel must be manually initiated via the Monitoring-system status screen.

Answer: B
Explanation:

When the VPN 3002 Hardware Client brings up a tunnel, the headend concentrator sends its Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers information. The VPN 3002 Hardware Client stores the information, and then passes it to the local PCs, using Dynamic Host Configuration Protocol (DHCP). This information enables the local PCs to send DNS and WINS packets to the correct enterprise DNS/WINS servers. When a PC is configured with a short lease period, it forces the PC to request its DHCP options every five minutes from the VPN 3002 Hardware Client until the tunnel is established.
WINS and DNS in the VPN 3002 Hardware Client
When the VPN 3002 Hardware Client brings up a tunnel, the headend concentrator sends its Domain Name System (DNS) and Windows Internet Naming Service (WINS) servers information. The VPN 3002 Hardware Client stores the information, and then passes it to the local PCs, using Dynamic Host Configuration Protocol (DHCP). This information enables the local PCs to send DNS and WINS packets to the correct enterprise DNS/WINS servers. When

a PC is configured with a short lease period, it forces the PC to request its DHCP options every five minutes from the VPN 3002 Hardware Client until the tunnel is established.

Note: If the VPN 3002 Hardware Client is initially configured at the remote site, the PC used to configure it does not get the WINS/DNS server information because a tunnel was not established at the time of the configuration. You have to reboot the PC and obtain the DNS/WINS servers information by renewing the DHCP lease or by acquiring it manually.

Configure the VPN 3000 Concentrator
Use this procedure to configure the VPN 3000 Concentrator.

Select Configuration > Interfaces, and make sure that the IP addresses are configured on the public and private interfaces.

Also make sure that you are able to get to the Internet from your VPN 3000 Concentrator.

Create a group to be used for a VPN 3002 Hardware Client IP Security (IPSec) connection by selecting Configuration > User Management > Groups > Add.

In this example, the group name is "3002group" and the password is "cisco123."

Under the General tab, specify your local DNS and WINS servers, and check IPSec under Tunneling Protocols.

If your VPN 3002 Hardware Client is behind a Port Address Translation (PAT) device, enable the IPSec through Network Address Translation (NAT) option under the IPSec tab.

If this option is disabled, then the VPN 3002 Hardware Client and the VPN 3000 Concentrator are not able to communicate with each other. IPSec through NAT uses User Datagram Protocol (UDP) port 10000 by default. You can select any port between 4001 and 49151. Make sure that this UDP port is not blocked anywhere in your topology. Once done, click the Add button to add the group.

Create a user for the VPN 3002 Hardware Client IPSec connection.

Tunnel Initiation

The VPN 3002 always initiates the tunnel to the central-site Concentrator. The central-site Concentrator cannot initiate a tunnel to a VPN 3002. The VPN 3002 creates only one IPSec tunnel to the central-site Concentrator, in either PAT or Network Extension mode. With split tunneling enabled, it can support multiple unencrypted data streams.

After the tunnel is established between the VPN 3002 and the central-site Concentrator, the central-site Concentrator can initiate data exchange only in Network Extension mode with all traffic traveling through the tunnel. If you want the tunnel to remain up indefin1itely, you should configure the VPN 3002 for Network Extension mode and not use split tunneling.

QUESTION NO: 5
Which mode of operation will you advice the TestKing trainee technician to use when she needs to view the devices behind the Hardware Client?

A. main extension mode
B. aggressive extension mode
C. discovery extension mode
D. network extension mode
E. client extension mode

Answer: D
Explanation:
You can configure two different modes for the VPN 3002 Hardware Client to use. Client mode, also called Port Address Translation (PAT) mode, and LAN Extension mode (also called Network Extension mode) are useful depending upon what you are attempting to accomplish.
PAT mode, the default, is used to isolate all the clients behid the VPN 3002 Hardware Client (on the private side) from the corporate network. Enabling PAT mode disables LAN Extension mode. Disabling PAT mode enables LAN Extension mode. The mechanism used to select either of the two modes ensures that only one mode is enabled at any given time. Hence to view the devices behind the Hardware Client you would need to coose the network extension mode

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.371

QUESTION NO: 6
What is the default IP address of the 3002 Hardware Client?

A. 10.1.1.1
B. 172.16.10.1
C. 192.168.10.1
D. 224.1.1.1

Answer: C
Explanation:
The default IP address of the 3002 Hardware Client is 192.168.10.1. This must be changed to any other IP address if you choose to use LAN Extension mode.

QUESTION NO: 7
What would you enable if you want certain remote client traffic to be encrypted to the Head End Concentrator, but all general web surfing traffic to be routed by the remote users' local ISP?

A. Auto Initiate
B. Interactive Hardware Authentication
C. Dynamic DNS
D. Split Tunneling

Answer: D
Explanation:
Allowing the local ISP to route general traffic instead of encrypting all traffic to the Head End Concentrator, then forcing the Concentrator to **web surfing traffic** is a process called Split Tunneling.

QUESTION NO: 8
What is the maximum number of tunnels that can be simultaneously active between a 3002 Hardware Client and a Concentrator?

A. 1
B. 4
C. 30
D. 1000

Answer: A
Explanation:
There can only be one active tunnel at a time from a 3002 Hardware Client to a Concentrator.

QUESTION NO: 9
How many different VPN user sessions can a 3002 Hardware Client support at one time to a Concentrator?

A. 1
B. 50
C. 127
D. 253
E. 10000

Answer: D
Explanation:

The 3002 Hardware Client will allow up to 253 different user sessions over the tunnel to the Head End Concentrator.

QUESTION NO: 10
Which of the following are modes the 3002 Hardware Client operates in when connected to a Concentrator? Choose all that apply.

A. negotiated
B. rotating
C. client
D. server
E. LAN negotiated
F. LAN Extension

Answer: C,F
Explanation:
The 3002 Hardware Client operates in two different modes, Client (default), and LAN Extension.

Q UESTION NO: 11
Where are 3002 Hardware Client preshared keys configured at?

A. configuration, system, ip routing, authentication
B. configuration, system, tunneling protocols, ipsec
C. configuration, system, management protocols, keys
D. configuration, system, general, authentication

Answer: B
Explanation:
To use preshared keys for authentication to your Concentrator, go to configuration, system, tunneling protocols, ipsec

QUESTION NO: 12
What is the minimum number of key characters needed to create a preshared key?

A. 4
B. 6
C. 8
D. 12

Answer: A

Explanation:
A preshared key needs to be at least 4 characters long, not more that 32.

QUESTION NO: 13
On your 3002 Hardware Client, where do you specify to be in Client mode or LAN Extension mode while connected to a Concentrator?

A. configuration, system, tunneling protocols, mode
B. configuration, system, ip routing, mode
C. configuration, policy management, traffic management, nat
D. configuration, policy management, traffic management, connections

Answer: C
Explanation:
For your 3002 Hardware Client to be configured in Client mode or LAN Extension mode, go to the 3002 Hardware Client screen configuration, policy management, traffic management, nat.

Topic 9, Configure the Cisco Virtual Private Network 3002 Hardware Client (8 questions)

Section 1: Overview of the Hardware Client interactive unit and user authentication features (3 questions)

QUESTION NO: 1
John and Kathy are the security administrators for Testking Inc. They are currently working on the Cisco VPN 3002. Kathy is not sure how the interactive unit authentication is enabled on the Cisco VPN 3002. How is interactive unit authentication enabled on the Cisco VPN 3002?

A. Make sure the unit authentication is unchecked on the Cisco VPN Concentrator and pushed down to the Cisco VPN 3002.
B. Make sure the interactive unit authentication is checked on the Cisco VPN 3002.
C. Make sure that the interactive unit authentication is checked on the Cisco VPN Concentrator and pushed down to the Cisco VPN 3002.
D. Make sure the interactive unit authentication is unchecked on the Cisco VPN 3002.

Answer: C
Explanation:
You configure interactive hardware client authentication in Hardware Client tab of the Configuration | User Management | Groups screen on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

Reference: VPN 3000 Series Concentrator Reference Volume I: Configuration

QUESTION NO: 2
John the security administrator for Testking Inc. is working on the Cisco VPN 3002. When John is using the default Cisco VPN 3002 unit authentication, what happens to the unit password?

A. The unit password is pushed down to the Cisco VPN 3002 the first time the tunnel is established.
B. The unit password is authenticated via TACAS+ server.
C. The unit password is stored permanently in Cisco VPN 3002 memory.
D. The unit password is authenticated via NT Domain server.

Answer: C
Explanation:
The DEFAULT is unit authentication, which uses a stored password (set and stored in the

hardware client's configuration).
Other methods (to improve security):
- Interactive authentication (once for the tunnel establishment, by the first user who establishes the tunnel)
- User authentication (each user must authenticate)

Note: The question is in regards to unit authentication, NOT interactive unit authentication.

QUESTION: 3
When you bring up your VPN client, how do you configure whether to authenticate to the Concentrator via a group name and password or a digital certificate?

A. options, authenticate
B. options, properties
C. options, properties, authentication
D. options, application launcher

Answer: C
Explanation:
Authenticate to a Concentrator via a group name and password, or choose to use a digital certificate from the VPN software from options, then properties, then authentication.

Section 2: Configuring the Hardware Client interactive unit authentication feature (0 questions)

Section 3: Configuring the Hardware Client user authentication feature (3 questions)

QUESTION NO: 1
Kathy the security administrator at Testking Inc. wants to know more about authentication. One of the first things she has to do is know how user authentication is enabled on the Cisco VPN 3002? (Choose two)

A. Pushed down to the Cisco VPN 3002.
B. Pushed down to the Cisco VPN Concentrator.
C. Checked on the Cisco VPN Concentrator
D. Unchecked on the Cisco VPN 3002.

Answer: A C
Explanation:
You configure individual user authentication on the VPN Concentrator, which pushes the policy to the VPN 3002.

QUESTION NO: 2
John the security administrator for Testking Inc. is not sure which is true about the Cisco VPN 3002 unit authentication option. Which of these answers is true?

A. The true statement is the username and password is pushed down to the Cisco VPN 3002 during tunnel establishment.
B. The true statement is the Cisco VPN 3002 prompts the user for a unit password before a tunnel is established.
C. The true statement is the Cisco VPN 3002 prompts the user for the username and password before a tunnel is established.
D. The true statement is the tunnel is established without user intervention.

Answer: D
Explanation:
Unit authentication uses a stored password (set and stored in the hardware client's configuration).
Other methods (to improve security):
- Interactive authentication (once for the tunnel establishment, by the first user who establishes the tunnel)
- User authentication (each user must authenticate)

Note: The question regards unit authentication, NOT interactive unit authentication.

QUESTION NO: 3
Jason the security administrator for Testking Inc. is working on authentication types. Which three are supported user authentication types? (Choose three)

A. AES for authenticating users
B. SDI for authenticating users
C. TACACS+ for authenticating users
D. Entrust for authenticating users
E. NT Domain for authenticating users
F. Radius for authenticating users

Answer: B E F
Explanation:
This screen lets you add, modify, delete, or change the priority order of authentication servers for a group. You can add external RADIUS, NT Domain and SDI servers for authenticating users. To add an internal server, go to the Configuration | System | Servers | Authentication screen. For further information about internal servers, see "Configuration | System | Servers | Authentication".

Reference: VPN 3000 Configuration Reference 3.6.pdf

Section 4: Monitoring the Hardware Client user statistics (2 questions)

QUESTION NO: 1
Where can you see how much a 3000 series Concentrator CPU is being utilized?

A. monitoring, general
B. monitoring, system status
C. monitoring, statistics
D. monitoring, hardware
E. monitoring, sessions

Answer: B
Explanation:
View many statistics such as CPU utilization, software version, etc. of a 3000 series Concentrator from the monitoring, system status screen.

QUESTION NO: 2
What 3002 Hardware Client screen shows if your tunnel is established to the Head End Concentrator?

A. monitoring, setup
B. monitoring, system status
C. monitoring, sessions
D. monitoring, statistics

Answer: B
Explanation:
You can view the status of the tunnel to the Head End Concentrator from your 3002 Hardware Client by selecting monitoring, system status. This is also where the software version is located.

Topic 10, Configure the Cisco Virtual Private Network Client Backup Server and Load Balancing (28 questions)

Section 1: Configuring the Cisco VPN Client backup server feature (8 questions)

QUESTION NO: 1
Kathy the security administrator at Testking Inc. is working on the Cisco VPN concentrator and needs to know the capabilities of the hardware.
What are the two RRI features supported by the Cisco VPN Concentrator? (Choose two)

A. Client RRI
B. Tunnel mode RRI
C. Transport mode RRI
D. LAN extension RR1
E. Network extension RRI
F. Cisco VPN Concentrator RRI

Answer: A E
Explanation:
Client Mode and Network Extension Mode

The VPN 3002 works in either of two modes: Client mode or Network Extension mode. Client mode is the default.

Reference: VPN 3002 Hardware Client Getting Started 4.0.pdf

QUESTION NO: 2
The security team at Testking Inc. is working on the Cisco VPN series. There are a few questions that come up when configuring the network.
If the Cisco VPN Concentrator sends the Cisco VPN 3002 a backup server list, what does the Cisco VPN 3002 do with any existing backup server addresses in its configuration?

A. The Cisco VPN 3002 adds the new list to the bottom of its existing list.
B. The Cisco VPN 3002 merges the two lists and deletes duplicate IP addresses.
C. The Cisco VPN 3002 deletes its configuration list and goes with the Cisco VPN Concentrator-downloadable list.
D. The Cisco VPN 3002 ignores the downloaded list and keep the configured list.

Answer: C
Explanation:
About Backup Servers
About Backup Servers
IPSec backup servers let a VPN 3002 connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002, or on a group basis at the central-site VPN Concentrator. If you configure backup servers on the primary central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group.
Not asked:
By default, the policy is to use the backup server list configured on the VPN 3002.
Asked question:
Alternatively, the VPN Concentrator can push a policy that supplies a list of backup servers in order of priority, replacing the backup server list on the VPN 3002 if one is configured.
(-> Replacing means deleting all client configuration. – Also see Page 12-5)
It can also disable the feature and clear the backup server list on the VPN 3002 if one is configured.

QUESTION NO: 3
The TestKing trainee technician wants to know what the backup server feature will enable the Cisco VPN 3002 to access. What will your reply be?

A. backup DHCP server
B. backup Cisco VPN Concentrator
C. backup authentication server
D. backup certificate server

Answer: B
Explanation:
IPSec backup servers let a VPN 3002 hardware client connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002, or on a group basis at the central-site VPN Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server policy to the VPN 3002 hardware clients in the group.
You can configure the backup server feature from the primary VPN Concentrator or the VPN 3002. From the VPN Concentrator configure backup servers on either of the Configuration | User Management | Base Group or Groups | Mode Configuration screens. On the VPN 3002, configure backup servers on the Configuration | System | Tunneling Protocols | IPSec screen

QUESTION NO: 4
Of the following operating systems, which is capable of supporting the Cisco VPN Client Virtual Adapter? (Select two options.)

A. Windows 98
B. Windows NT 4.0
C. Windows 2000
D. Windows XP
E. Mac OS X version 10.1.0 or higher
F. Solaris 2.6 or higher

Answer: C, D

QUESTION NO: 5
How many different Concentrators can the 3002 Hardware Client be configured to try and connect to if the primary Concentrator fails?

A. 5
B. 10
C. 15
D. 20

Answer: B
Explanation:
The 3002 Hardware Client can be configured to connect to 10 different Concentrators if its primary has failed.

QUESTION NO: 6
If a 3002 Hardware Client cannot connect to a Head End Concentrator, by default how long will it wait until it attempts to connect to a backup Concentrator?

A. 2 seconds
B. 8 seconds
C. 15 seconds
D. 35 seconds

Answer: B
Explanation:
By default the 3002 Hardware Client is in Client mode, which means it will try to connect to a backup Concentrator after 8 seconds of initially attempting contact with the main Concentrator. If the 3002 Hardware Client is in LAN Extension mode, it will attempt every 4 seconds.

QUESTION NO: 7
Which of the following protocols allows a backup Concentrator to become active if the main Concentrator fails?

A. CDP
B. AYT
C. ADDL
D. VRRP

Answer: D
Explanation:
If you have two or more Concentrators in parallel, you can configure one to be in standby mode to take over as the active Concentrator if the main one fails via Virtual Router Redundancy Protocol (VRRP).

QUESTION NO: 8
What is the rated time a backup Concentrator will fully take over as the active Concentrator in a VRRP configuration?

A. 1-2 seconds
B. 2-4 seconds
C. 3-10 seconds
D. 9-20 seconds

Answer: C
Explanation:
For a backup VRRP Concentrator to fully take over and become the active Concentrator, the process is rated by Cisco as taking 3-10 seconds to complete.

Section 2: Configuring the Cisco VPN Client load balancing feature (8 questions)

QUESTION NO: 1
Jason the security administrator is currently working on Cisco VPN.
When a VPN 3002 is configured to establish a tunnel to a load balancing cluster, what IP address should Jason put in the VPN 3002 remote server field?

A. Cluster's virtual IP address.
B. Master the Cisco VPN Concentrator's private interface IP address.
C. Master the Cisco VPN Concentrator's public interface IP address.
D. Load balancing server's virtual IP address.

Answer: A
Explanation:
When configuring the VPN3002 hardware client, or using the EASYVPN software client and connecting to a remote site for clustering, the Virtual IP address is used in the VPN3002 server field.

All clients other than the Cisco VPN Client or the Cisco 3002 Hardware Client connect directly to the VPN Concentrator as usual;they do not use the virtual cluster IP address.

Step 1 Configure the cluster: establish a common *virtual cluster IP address*, UDP port (if necessary), and IPSec shared secret for the cluster. These values are identical for every device in the cluster. VPN Virtual Cluster IP Address

Enter the single IP address that represents the entire virtual cluster. Choose an IP address that is within the public subnet address range shared by all the VPN Concentrators in the virtual cluster.

Step 2 Configure the device: enable load balancing on the device and define device-specific properties. These values vary from device to device.

QUESTION NO: 2
John the security administrator at Testking Inc. needs to know which statement is true when two adjacent Cisco VPN Concentrators are configured for VRRP and the master Cisco VPN Concentrator fails.

A. The true statement is "all sessions are lost."
B. The true statement is "no sessions are lost."
C. The true statement is "only site-to-site users need to re-establish their tunnels."
D. The true statement is "only remote access users need to re-establish their tunnels."

Answer: D
Explanation:
These functions apply only to installations where two or more VPN Concentrators are in parallel. One VPN Concentrator is the master system, and the other(s) are backup systems. A backup system acts as a virtual master system when a switchover occurs.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
Which of the following statements regarding Cisco VPN Concentrator load balancing feature is valid?

A. Cisco VPN Concentrators load balance both site-to-site and remote access tunnels.
B. Cisco VPN Concentrators load balance site-to-site tunnels only.
C. Cisco VPN Concentrators load balance remote access tunnels only.
D. Cisco VPN Concentrators load balances administration sessions.

Answer: C
Note Load balancing is effective only on remote sessions initiated with the Cisco VPN Client (Release 3.0 and later) or the Cisco VPN 3002 Hardware Client (Release 3.5). All other clients, including LAN-to-LAN connections, can connect to a VPN Concentrator on which load balancing is enabled, but they cannot participate in load balancing.

QUESTION NO: 4
The TestKing trainee technician wants to know which IP address is used for the VPN virtual cluster IP address. What will your reply be?

A. IP address within the Cisco VPN Concentrator's public subnet address range
B. single IP address that represents the master Cisco VPN Concentrator
C. IP address within the Cisco VPN Concentrator's private subnet address range
D. single IP address for the master Cisco VPN Concentrator with a separate IP address for all the secondary Cisco VPN Concentrators

Answer: A
Explanation:

VPN Virtual Cluster IP Address – A single IP address from the public subnet that will be used to represent the load-balancing cluster to potential clients.

Reference: CCSP Cisco Secure VPN certification guide p.416

QUESTION NO: 5
What is the minimum software version needed on a 3002 Hardware Client to be able to have the Head End Concentrators load balance its tunnel connection?

A. 2.4
B. 3.0
C. 3.2
D. 3.5

Answer: D
Explanation:
For the Head End Concentrators to load balance 3002 Hardware Client tunnels, the Hardware Client must be running at least software version 3.5.

QUESTION NO: 6
What is the default priority on a 3030 Concentrator when determining a Cluster Master for load balancing?

A. 5
B. 8
C. 15
D. 35

Answer: A

Explanation:
Cluster Master load balancing default priorities: 3005 = 1, 3015 = 3, 3030 = 5, 3060 = 7, 3080 = 9.

QUESTION NO: 7
On a Concentrator, where can you configure the Cluster Master load balancing priority?

A. configuration, system, general, priority
B. configuration, system, general, identification
C. configuration, system, load balancing
D. configuration, system, events, load balancing

Answer: C
Explanation:
If you need to change the default Cluster Master priority on your Concentrator, go to configuration, system, load balancing.

QUESTION NO: 8
What protocol and port do Concentrators use when communicating virtual router information?

A. UDP 4500
B. UDP 9023
C. TCP 4500
D. TCP 9023

Answer: B
Explanation:
Multiple Concentrators running load balancing communicate information about the virtual router over UDP 9023.

Section 3: Overview of the Cisco VPN Client Reverse Route Injection feature (12 questions)

QUESTION NO: 1
Kathy the security administrator for Testking Inc. needs to know which IP address does the Cisco VPN Concentrator advertise, for network extension RRI.

A. IP address on the Cisco VPN Client NIC
B. Assigned IP address on the Cisco VPN 3002
C. Public interface IP address on the Cisco VPN 3002
D. Private interface network address on the Cisco VPN 3002

Answer: B
Explanation:
Just as with client mode, Network extention RRI advertises the assigned IP address of the VPN client
Reference: Ciscopress CCSP Self Study, CSVPN Second edition Page: 276

QUESTION NO: 2
John the security administrator is assigned to find out which client RRI statement is true when troubleshooting the network.

A. The true statement is the "host route can be advertised with both OSPF and RIP."
B. The true statement is the "host route is deleted when the client RRI is disabled."
C. The true statement is the "host route is added when the option is enabled."
D. The true statement is the "host route is advertised out the public interface."

Answer: A
Explanation:
To add routes to the routing table of the VPN Concentrator without advertising them to the private network, disable routing on the private interface.
To advertise the routes, enable OSPF or RIP on the VPN Concentrator's private interface.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
Peter the security administrator at Testking Inc. is working on the Cisco VPN Concentrator. The network auto-discovery feature enables the Cisco VPN Concentrator to learn automatically which networks are reachable at both ends of a LAN-to-LAN tunnel. Peter needs to know from which routing protocols can the Cisco VPN Concentrator learn these networks.

A. Routing protocol RIP
B. Routing protocol EIGRP
C. Routing protocol OSPF

D. Routing protocols RIP and OSPF

Answer: A
Explanation:
The Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and Inbound RIP must be enabled on that interface.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 4
Jane the security administrator for Testking Inc. is working on the RRI.
For client RRI, which IP address does the Cisco VPN Concentrator advertise?

A. It advertises the Cisco VPN 3002 private interface IP address
B. It advertises the Cisco VPN 3002 assigned IP address
C. It advertises the Cisco VPN Client NIC IP address
D. It advertises the Cisco VPN 3002 public interface IP address

Answer: B
Explanation:
You can configure the VPN Concentrator to add routes to its routing table for remote hardware or software clients. The VPN Concentrator can then advertise these routes to its private network via RIP or OSPF. This feature is called reverse route injection (RRI).
When the tunnel is launched, the Concentrator assigns the hardware client a virtual IPAddress.
It's true, it assigns it to the hardware client private interface (A is also true).
But as Cisco refers to the term "assigned" IP address on Page 12-21 in the Cisco Secure Virtual Private Networks Training documents (Version 4.0), B seems to be the best choice.
Note: As the question refers to IP addresses, not network addresses it's clear that PAT is performed on the hardware client. So it does Client Mode RRI (single IP host route entry), not Network Extension Mode RRI (network).

QUESTION NO: 5
Which of the following routing protocols is supported by the Hardware Client?

A. OSPF
B. RIP
C. EIGRP
D. all of the above
E. none of the above

Answer: A, B
Source: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.407

Explanation:

There is no configuration requirement, other than being in Network Extension mode (NEM), on the VPN 3002 Hardware Client for RRI to occur. Therefore, this section will cover the configurations necessary on the VPN concentrator.

RRI will work only with RIP and OSPF. Using Virtual Routing Redundancy Protocol (VRRP) with RRI will probably cause routing loops because both the primary and the backup servers will advertise the same routes.

QUESTION NO: 6
The Cisco VPN Concentrator is capable of supporting routing updates based on what protocol?

A. IS-IS
B. EIGRP
C. BGP
D. RIP

Answer: D
Explanation:

There is no configuration requirement, other than being in Network Extension mode (NEM), on the VPN 3002 Hardware Client for RRI to occur. Therefore, this section will cover the configurations necessary on the VPN concentrator.

RRI will work only with RIP and OSPF. Using Virtual Routing Redundancy Protocol (VRRP) with RRI will probably catuse routing loops because both the primary and the backup servers will advertise the same routes.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.407

QUESTION NO: 7
On a Concentrator, how do you configure RRI hold down routes?

A. configuration, system, servers, rri
B. configuration, system, ip routing, rri
C. configuration, system, tunneling protocols, rri
D. configuration, system, general, rri

Answer: B
Explanation:
On a Concentrator, enter RRI parameters from configuration, system, ip routing, reverse route injection. This enables you to advertise to neighbor routers that your VPN tunnels are always

up, even if they go down, preventing your neighbor from being forced to recalculate their routing tables.

QUESTION NO: 8
Where do you set RIP processing on your 3000 series Concentrator?

A. configuration, system, ip routing, rip
B. configuration, system, ip routing, interfaces
C. configuration, system, interfaces, ip routing
D. configuration, interfaces

Answer: D
Explanation:
Rip and Rip2 can be defined on the configuration, interfaces Concentrator tab.

QUESTION NO: 9
Which of the following routing protocols can be used to distributed routes via RRI? Choose all that apply.

A. RIP
B. EIGRP
C. OSPF
D. ISIS

Answer: A,C
Explanation:
You can inject routes to the Head End Concentrator from a 3002 Hardware Client via RRI if you use RIP or OSPF.

QUESTION NO: 10
Which of the following protocols might cause a routing loop when used with RRI?

A. NAT
B. OSPF
C. VRRP
D. ESP

Answer: C
Explanation:
When a 3000 series Concentrator is redistributing routes via RRI, a routing loop may occur with VRRP because the standby Concentrator will advertise the RRI routes as well.

QUESTION NO: 11
Which routing protocols can a 3000 series Concentrator run? Choose all that apply.

A. RIP
B. IGRP
C. EIGRP
D. ISIS
E. OSPF

Answer: A,E
Explanation:
A 3000 series Concentrator has support for RIP, RIPv2, and OSPF.

QUESTION NO: 12
On a 3000 series Concentrator, where do you configure Reverse Route Injection (RRI)?

A. configuration, system, ip routing, rri
B. configuration, system, tunneling protocols, ipsec, rri
C. configuration, system, general, rri
D. configuration, system, events, routing, rri

Answer: A
Explanation:
Remote Client RRI can be configured from the Concentrator, on the configuration, system, ip routing, rri screen. You also configure RRI hold down routes here

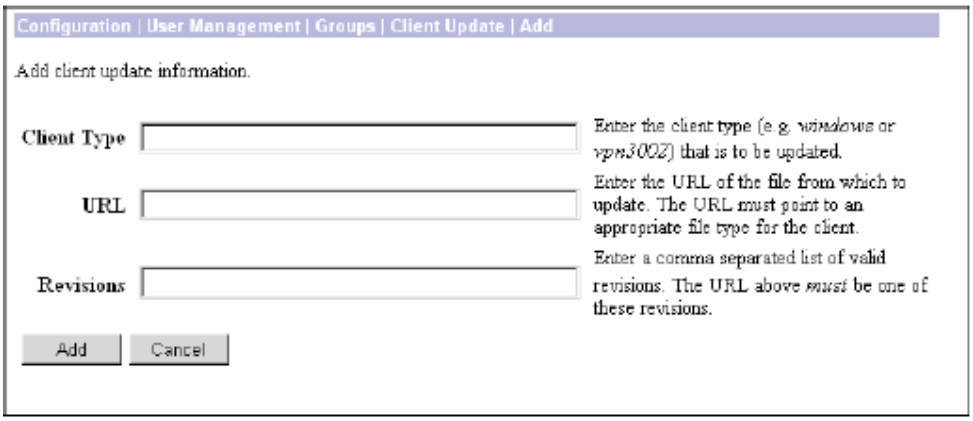
Topic 11, Configure the Virtual Private Network 3002 Hardware Client for Software Auto-Update (11 questions)

Section 1: Overview and configuration of the VPN 3002 Hardware Client software auto-update feature (8 questions)

QUESTION NO: 1
John the security administrator for Testking Inc. is working on the Cisco VPN concentrator. He needs to know what are the three group-auto-update parameters? (Choose three)

A. Client type
B. URL
C. TFTP server
D. TFTP file
E. Revision
F. Action required

Answer: A B E
Explanation:



Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 2
Jane the security administrator for Testking Inc. is working on the Cisco VPN concentrator. Jane needs to know what the three steps in the auto-update configuration process are. (Choose three)

A. Enable the client update functionality in the Cisco VPN Concentrator.
B. Modify the group-client, auto-update parameter.
C. Enable the client update functionality in the Cisco VPN 3002.
D. Configure the IKE auto-update message parameters.
E. Configure the IPSec auto-update message parameters.
F. Send an update message.

Answer: A B F
Explanation:
This process uploads the executable system software to the VPN Concentrator, which then verifies the integrity of the software image. The new image file must be accessible by the workstation you are using to manage the VPN Concentrator. Software image files ship on the Cisco VPN 3000 Concentrator CD-ROM. Updated or patched versions are available from the Cisco website, www.cisco.com, under Service & Support > Software Center. It takes a few minutes to upload and verify the software, and the system displays the progress. Please wait for the operation to finish. To run the new software image, you must reboot the VPN Concentrator. The system prompts you to reboot when the update is finished.

Reference: VPN 3000 Concentrator Ref Vol 2. Config 4.0.pdf

QUESTION NO: 3
Which of the following operating systems will have the Virtual Adapter available for use? (Choose two).

A. Windows 98
B. Windows XP
C. MacOs
D. Windows 2000
E. Windows ME
F. Solaris

Answer: B, D
It is available on Windows 2000 and XP only

QUESTION NO: 4
Which of the following is the proper way to enter an auto-update URL?

A. http://10.0.1.10/vpn3002-3.5.rel-k9.bin
B. tftp://10.0.1.10/vpn3002-3.5.Rel-k9.bin
C. http://10.0.1.10/vpn3002-3.5.Rel-k9.bin
D. ftp://10.0.1.10/vpn3002-3.5.Rel-k9.bin

Answer: B
Explanation:

Setting up the head-end VPN 3000 Series Concentrator for automatically updating CSVPN simple through the GUP. Configuring the concentrator for Automatic Client Update consists of the following steps:

1) Navigate to Configuration | User Management | Groups, and select the group.
2) Choose Modify Client Update
3) Choose Add from the Client Update screen to add a new client package.
4) On the next screen, enter Windows as the client type, enter *tftp://IP address of server/filename* as the URL, and enter the revision number.
5) Select Apply to finish the setup at the head-end.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.283

QUESTION NO: 5
Which of the following features allows a Concentrator to mandate that any remote clients trying to establish a tunnel must be running a certain client software version?

A. software selection
B. auto-update
C. tunnel setup
D. client termination

Answer: B
Explanation:
A Concentrator can mandate that remote clients be running a specific software version before they are allowed to connect. If they are not, the Concentrator will provide a link where the current version is available for download.

QUESTION NO: 6
Which of the following operating systems have vpn client software support for Auto Update? Choose all that apply.

A. linux
B. mac
C. solaris
D. windows

Answer: D
Explanation:
The Auto Update feature is only supported on the Microsoft Windows software VPN client.

QUESTION NO: 7

How often are Auto Update messages sent from a Concentrator to the 3002 Hardware Client?

A. every 10 seconds
B. every 45 seconds
C. every 2 minutes
D. every 5 minutes

Answer: D
Explanation:
A Concentrator will send Auto Update messages to all 3002 Hardware Clients informing them of a required software version to run before a connection will be allowed. If the 3002 Hardware Client is already running the correct version, it will just drop the Auto Update messages.

QUESTION NO: 8
How many times will a 3002 Hardware Client try to download an Auto Update software version before stopping?

A. 5
B. 10
C. 20
D. 30

Answer: C
Explanation:
When a Head End Concentrator is mandating an Auto Update software upgrade, the 3002 Hardware Client will try to download and run a file integrity check on the new version up to 20 consecutive times before quitting.

Section 2: Monitoring the Cisco VPN 3002 Hardware Client software auto-update feature (3 questions)

QUESTION NO: 1
John is the security administrator at Testking Inc. and his job is to view event logs. Which statement about the live event log is true?

A. With the event log, the administrator can pause, and then filter the live event log.
B. The live event log can filter events by various criteria.
C. As events occur, the live event log automatically updates.
D. The live event log automatically updates the display every six seconds.

Answer: C
Explanation:
Monitoring | Live Event Log

Pause Display/Resume Display

To pause the display, click **Pause Display**. While paused, the screen does not display new events, the button changes to Resume Display, and the timer counts down to 0 and stops. You can still scroll through the event log. Click the button to resume the display of new events and restart the timer.

Clear Display

To clear the event display, click **Clear Display**. This action does *not* clear the event log, only the display of events on this screen.

Restart

To clear the event display and reload the entire event log in the display, click **Restart**.

Timer

The timer counts 5 - 4 - 3 - 2 - 1 to show where it is in the 5-second refresh cycle. A momentary Rx indicates receipt of new events. A steady 0 indicates the display has been paused.

The screen always displays the most recent event at the bottom. Use the scroll bar to view earlier events. To filter and display events by various criteria, see the Monitoring | Filterable Event Log section above.

QUESTION NO: 2
By viewing which event class will an administrator be able to monitor an update process?

A. AUTOUPDATE
B. IPSec
C. UPDATE

D. IKE

Answer: A
Explanation: To view only the update-specific information, scroll down in the Event Class section and select AUTOUPDATE
Reference: Ciscopress CCSP Self Study, CSVPN Second edition Page: 239

QUESTION NO: 3
Which of the following represents the default configuration of the Cisco VPN 3002 public interface?

A. DHCP server is enabled
B. DHCP client is enabled
C. static IP address of 192.168.10.1
D. no configuration

Answer: B

Topic 12: Configure the Cisco Virtual Private Network 3000 Series Concentrator for the IPSec Over UDP and IPSec Over TCP (16 questions)

Section 1: Overview of Port Address Translation (3 questions)

QUESTION NO: 1
John the Jr. Security administrator at Testking Inc. does not understand how Cisco solved the PAT translation issue.

A. They wrap a standard IKE packet with a UDP port number.
B. They changed the IKE TCP port number from a well known to a dynamically assigned port number.
C. They changed the IPSec TCP port number from a well known to a dynamically assigned port number.
D. They wrap a standard IPSec packet with a UDP port number.

Answer: D
Explantion:
NAT-T (NAT Traversal) lets IPSec peers establish a LAN-to-LAN connection through a NAT device. It does this by encapsulating IPSec traffic in UDP datagrams, using port 4500, thereby providing NAT devices with port information. NAT-T auto-detects any NAT devices, and only encapsulates IPSec traffic when necessary.

Reference: VPN 3000 Series Concentrator Reference Volume I: Configuration

QUESTION NO: 2
Jane the security administrator at Testking Inc. is working on the Cisco VPN 3002. Which statement is true of the Cisco VPN 3002 port address translation?

A. PAT is always enabled on the Cisco VPN 3002 pubic interface.
B. PAT status is configured on the Cisco VPN Concentrator and then pushed to the Cisco VPN 3002 during tunnel establishment.
C. The administrator can disable PAT when the default private interface address is changed.
D. The Cisco VPN 3002 does not support PAT.

Answer: C
Explanation:
Using a Browser to Configure the VPN 3002

1. Use a LAN cable to attach a PC to the private interface (3002) or switch port (3002-8E) .

2. Enter the default IP address (192.168.10.1) in the browser Location or Address field.

3. At the VPN 3002 Login prompt, enter the login name **admin** and the default password **admin**. Click **Login**.

4. In the Main window, select **Quick Configuration** from the menu. Follow the online instructions for all subsequent screens. Note that to configure Network Extension mode, you must change the private interface IP address and disable PAT.

QUESTION NO: 3
What is the process called when a network devices changes many IP addresses to a different single IP address, so anybody exterior to the network does not know the real IP addresses?

A. VRRP
B. NAT
C. CDP
D. PAT

Answer: D
Explanation:
NAT is a one to one translation. PAT is a many to one translation.

Section 2: Configuring IPSec over UDP (5 questions)

QUESTION NO: 1
John the security administrator for Testking Inc. is working on troubleshooting IPSec. He needs to know which encapsulation method takes precedence, in a remote access NAT environment with multiple encapsulation schemes enabled?

A. The answer is NAT-transparency takes precedence over IPSec over TCP.
B. The answer is IPSec over UDP takes precedence over IPSec over TCP.
C. The answer is NAT-transparency takes precedence over IPSec over UDP.
D. The answer is IPSec over UDP takes precedence over NAT-transparency.

Answer: C
Explanation:
If both, IPSec over UDP and NAT-T are enabled, NAT-T takes precedence.
Additional note: IPSec over TCP would take precedence over all others, because if enabled, no further negotiations are performed

QUESTION NO: 2
John the security administrator at Testking Inc. is working on configuring the Cisco VPN Concentrator. When John is configuring the Cisco VPN Concentrator for IPSec over UDP, which statement is true?

A. When configuring the Cisco VPN Concentrator, in the Mode Config | IPSec over UDP port number field, enter a value between 1000 and 4000.
B. When configuring the Cisco VPN Concentrator, in the IPSec-IPSec over UDP port number field, enter a value between 1 and 4000.
C. When configuring the Cisco VPN Concentrator, go to configuration | User Management | Groups | Mode Config tan and select **IPSec over UDP**.
D. When configuring the Cisco VPN Concentrator, go to Configuration | System | Tunneling Protocols | IPSec and select **IPSec over UDP**.

Answer: C
Explanation:
Configuration | User Management | Groups | Add or Modify (Internal)
These screens let you:
• Mode Config Parameters: Banner, password storage, split-tunneling policy, default domain name, IPSec over UDP, backup servers.

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

QUESTION NO: 3
Your boss at TestKing.com is curios about UDP. What should you tell her?

A. IPSec over UDP is a non-negotiable, system-wide parameter.
B. IKE over UDP is negotiated on a group basis.
C. IPSec over UDP is negotiated on a group basis
D. IKE over UDP is a non-negotiable, system-wide parameter.

Answer: C
Explanation:

There are three requirements for running UDP NAT Transparent IPSec (or IPSec over UDP):
1) Run version 3.0.3 or later software.
2) The concentrator and the VPN 3002 Hardware Client must use the same port
3) You must configure IPSec over UDP for the group on the VPN concentrator through the Configuration | User Management | Groups | Modify screen. Clicking the IPSec over UDP box causes the VPN concentrator to expect IPSec over UDP (UDP NAT Transparent IPSec) instead of IPSec over TCP.

Reference: CSVPN student guide, Ciscopress p.420

QUESTION NO: 4
When running IPSEC over UDP, what is the valid configurable port range you can use?

A. 1024-65535
B. 4001-49151
C. 8000-12000
D. 22000- 42880

Answer: B
Explanation:
With IPSEC over UDP you cannot use any port, it must be within the range of 4001-49151.

QUESTION NO: 5
Where is IPSEC over UDP enabled on a Concentrator?

A. configuration, system, tunneling protocols, ipsec
B. configuration, system, ip routing, ipsec
C. configuration, user management, groups, mode config
D. configuration, policy management, tunnels

Answer: C
Explanation:

IPSEC over UDP is configured on your Concentrator from the mode config tab on the configuration, user management, groups screen.

Section 3: Configuring NAT-Transversal (2 questions)

QUESTION NO: 1
What will be the consequence of enabling both NAT-T and IPSec over UDP on the Concentrator and Client?

A. IPSec over UDP takes precedence.
B. The user choice of protocol takes precedence
C. NAT-T takes precedence
D. An election process between the negotiating peers for which protocol takes precedence will occur

Answer: C

QUESTION NO:2
NAT Traversal uses which UDP port?

A. 3745
B. 4290
C. 4500
D. 4780

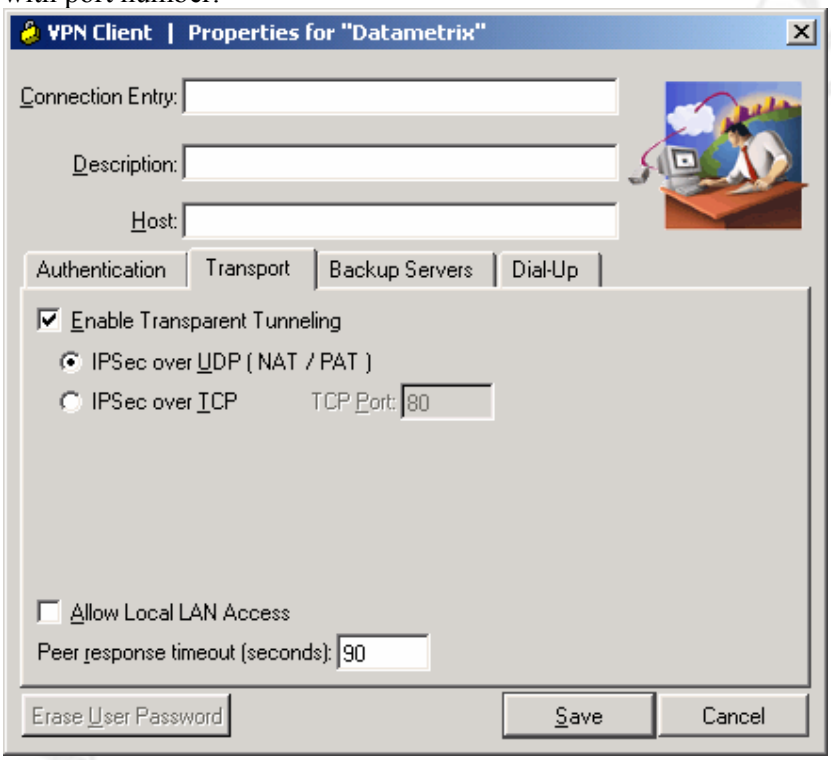
Answer: C
Explanation:
NAT Traversal uses UDP port 4500 to communicate between a Concentrator and a 3002 Hardware Client. NAT Traversal has replaced IPSEC over UDP as the default on 3002 Hardware Clients.

Section 4: Configuring IPSec over TCP (6 questions)

QUESTION NO: 1
Which of the following statements is valid when configuring the Cisco VPN Client for IPSec over TCP?

A. There is no configuration because the information is pushed down to the Cisco VPN Client.
B. There is no configuration needed because the feature is enabled by default.
C. IPSec over TCP must be enabled on the Cisco VPN Client.
D. IPSec over TCP and a TCP port number must be configured on the Cisco VPN Client.

Answer: D
Explanation:
See figure below, the default for IPSec is over UDP and TCP must be manually configured with port number.



QUESTION NO: 2
Which of the following statement regarding the configuration of the Cisco VPN Concentrator for IPSec over TCP is valid?

A. In the IPSec | IPSec over TCP port number field, enter a value between 1 and 4000.
B. Go to Configuration | System | Tunneling Protocols | IPSec and Select **IPSec over TCP**.

C. Go to Configuration | User Management | Groups | Mode Config tab and select **IPSec over TCP.**
D. in the Mode Config | IPSec over TCP port number field, enter a value between 1000 and 4000

Answer: B
Explanation:

To enable IPSec over TCP/IP, you must make configuration changes on both the VPN concentrator and the VPN 3002 Hardware Client. IPSec over TCP/IP is configured on the VPN 3002 Hardware Client under the Configuration | System | Tunneling Protocols | IPSec screen. On the VPN concentrator, configuration settings for IPSec over TCP/IP are made on the Configuration |System | Tunneling Protocols | IPSec | IPSec over TCP.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.418

QUESTION NO: 3
What port is used for IPSEC over TCP?

A. 8000
B. 10000
C. 12000
D. 47383

Answer: B
Explanation:
When a 3002 Hardware Client and a Concentrator are communicating with IPSEC over TCP, they will use the default configured port of 10,000.

QUESTION NO: 4
How many different ports can your Concentrator be configured to communicate IPSEC over TCP?

A. 1
B. 10
C. 20
D. 100

Answer: B
Explanation:
A Concentrator can be configured to communicate on up to 10 different defined ports for IPSEC over TCP. This allows different 3002 Hardware Client's access with their own port. The 3002 Hardware Client can only be configured for 1 port.

QUESTION NO: 5
How is IPSEC over TCP enabled on a Concentrator?

A. configuration, system, general, ipsec
B. configuration, system, general, tcp
C. configuration, system, tunneling protocols, ipsec
D. configuration, system, tunneling protocols, tcp

Answer: C
Explanation:
Use the check box to enable or disable IPSEC over TCP communications from the Concentrators configuration, system, tunneling protocols, ipsec screen.

QUESTION NO: 6
What minimum software version must a 3002 Hardware Client be running to communicate to a Concentrator via IPSEC over TCP?

A. 3.2
B. 3.5
C. 3.6
D. 3.7

Answer: B
Explanation:
To communicate with IPSEC over TCP between a 3002 Hardware Client and a Concentrator, both devices must be running at least version 3.5.

Topic 13, Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN with Pre-Shared Keys (6 questions)

Section 1: Cisco VPN 3000 Series Concentrator IPSec LAN-to-LAN (1 question)

QUESTION NO: 1
Which two products is the result of a LAN-to-LAN VPN application?

A. Cisco VPN Client a Cisco VPN 3002
B. Cisco VPN Concentrator to Cisco VPN Concentrator
C. Cisco VPN 3002 to a Cisco VPN Concentrator
D. Cisco VPN Client to a Cisco VPN Concentrator

Answer: B
LAN-to-LAN communication are established with other VPN 3000 concentrators, PIX firewalls, 7100/4000 series routers and other IPSec-complaint security gateways. The only answer is then B.

Section 2: LAN-to-LAN configuration (5 questions)

QUESTION NO: 1
Greg the security administrator at Testking Inc. must edit the reachable subnets at both ends of the LAN-to-LAN tunnel. Which feature allows Greg to edit the reachable subnets at both ends of the LAN-to-LAN tunnel?

A. You can edit the "Network lists"
B. You can edit the "Network auto-discovery"
C. You can edit the "Cisco VPN configuration tool"
D. You can edit the "LAN-to-LAN wizard"

Answer: A
Explanation:
Configuration | Policy Management | Traffic Management | Network Lists
This section of the Manager lets you configure network lists, which are lists of networks that are grouped as single objects. Network lists make configuration easier: for example, you can use a network list to configure one filter rule for a set of networks rather than configuring separate rules for each network.

You can use network lists in configuring filter rules (see Configuration | Policy Management | Traffic Management | Rules). You can also use them to configure split tunneling for groups and users (see Configuration | User Management), and to configure IPSec LAN-to-LAN connections (see Configuration | System | Tunneling Protocols | IPSec LAN-to-LAN).

The Manager can automatically generate a network list containing the private networks reachable from the Ethernet 1 (Private) interface. It generates this list by reading the routing table, and Inbound RIP must be enabled on that interface.

QUESTION NO: 2
Peter is the Security administrator at Testking Inc. and he is working on the Cisco VPN Concentrator configurations. In the local network section of the IPSec LAN-to-LAN screen, he needs to know what IP address is entered in the IP address field.

A. In the IP address field, the network, subnet, and host IP address of the remote Cisco VPN Concentrator's private interface is entered.
B. In the IP address field, the network, and subnet IP address of the remote private LAN is entered.
C. In the IP address field, the network, subnet, and host IP address of the local Cisco VPN Concentrator's private interface is entered.
D. In the IP address field, the network, and subnet IP address of the local private LAN is entered.

Answer: D
Explanation:
D is the best choice, although the term "subnet IP address" is used to name the "wildcard mask", specifying the subnet portion of the network address:
Page 15-18:
Step 1: Set the local network IP address, i.e. 10.0.1.0
Step 2: Set the wildcard mask, i.e. 0.0.0.255. The wildcard mask is the reverse of the subnet mask.

QUESTION NO: 3
Which enrollment request field will you tell the TestKing trainee technician must match a group name configured in the remote Cisco VPN Concentrator when that trainee has been instructed to complete an enrollment request form?

A. common name
B. organization
C. subject alternative name
D. organizational unit

Answer: D
Explanation:

The OU should match the IPSec group name. Using a different name thatn the IPSec group will mean that the IPSec group used will not have any access.

Reference: Cisco Press CCSP Cisco Secure VPN (Roland, Newcomb) p.460

QUESTION NO: 4
Which of the following is the correct way to enter a network and wildcard for a Concentrator network list? (x = network, y = wildcard)

A. x.x.x.x\y.y.y.y
B. x.x.x.x./y.y.y.y
C. x.x.x.x>y.y.y.y
D. x.x.x.x.<y.y.y.y

Answer: B
Explanation:
A Network List network and wildcard mask are entered with a forward slash (/) separating them without any spaces between them.

QUESTION NO: 5
On a Concentrator, how is a LAN To LAN connection created?

A. configuration, system, tunneling protocols, ipsec, lan to lan
B. configuration, system, ip routing, ipsec, lan to lan
C. configuration, general, tunneling protocols, ipsec, lan to lan
D. configuration, general, ip routing, ipsec, lan to lan

Answer: A
Explanation:
LAN to LAN connections are created on a Concentrator from the configuration, system, tunneling protocols, ipsec, lan to lan screen.

Topic 14, Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN with NAT (5 questions)

Section 1: LAN-to-LAN overview (1 question)

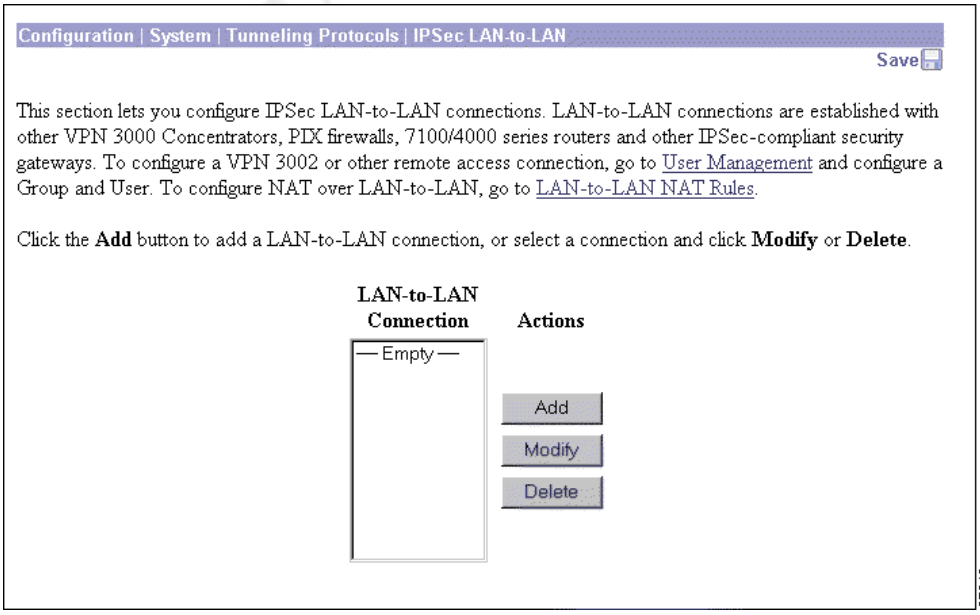
QUESTION NO: 1
James the security administrator for Testking Inc. is configuring LAN-to-LAN connections. One of the problems he needs to solve is what two products does the LAN-to-LAN VPN applications consists of.

A. The Cisco VPN Client to a Cisco VPN 3002
B. The Cisco VPN Client to a Cisco VPN Concentrator
C. The Cisco VPN Concentrator to a Cisco VPN Concentrator
D. The Cisco VPN 3002 to a Cisco VPN Concentrator

Answer: C
Explanation:

While the VPN Concentrator can establish LAN-to-LAN connections with other protocol-compliant VPN secure gateways, these instructions assume VPN Concentrators on both sides. And here, the "peer" is the other VPN Concentrator or secure gateway.

In a LAN-to-LAN connection, IPSec creates a tunnel between the public interfaces of two VPN Concentrators, which correspondingly route secure traffic to and from many hosts on their private LANs. There is no user configuration or authentication in a LAN-to-LAN connection; all hosts configured on the private networks can access hosts on the other side of the connection, at any time.



Section 2: Configuring the Concentrator LAN-LAN NAT feature (4 questions)

QUESTION NO: 1
James is the security administrator for Testking Inc. and is working on configuring the Cisco VPN Concentrator. When configuring Concentrator LAN-to-LAN NAT rule types, which rule type defines a one-to-one address mapping between networks?

A. NAT
B. PAT
C. Dynamic
D. Static

Answer: D
Explanation:
Mapping rules that you configure determine how LAN-to-LAN NAT translates network addresses. There are three types of mapping rules:

- *Static* LAN-to-LAN NAT rules map source IP addresses to Translated IP addresses on a one-to-one basis. Static rules apply both to
  - *inbound* traffic, which is traffic received over a LAN-to-LAN tunnel.
  - *outbound* traffic, which is traffic bound for a LAN-to-LAN tunnel.

  Static rules are restricted to networks in which the local network and mapped network are of the same size. Port mappings are unnecessary, and are not performed.
- *Dynamic* LAN-to-LAN NAT rules map source IP addresses to one of a pool of available translated IP addresses, or to a single address. Dynamic mappings apply only to outbound traffic.
- *PAT* LAN-to-LAN NAT rules are dynamic rules with Port Address Translation. PAT rules apply to outbound traffic only

Reference: VPN 3000 Concentrator Ref Volume 1. Configuration 4.0.pdf

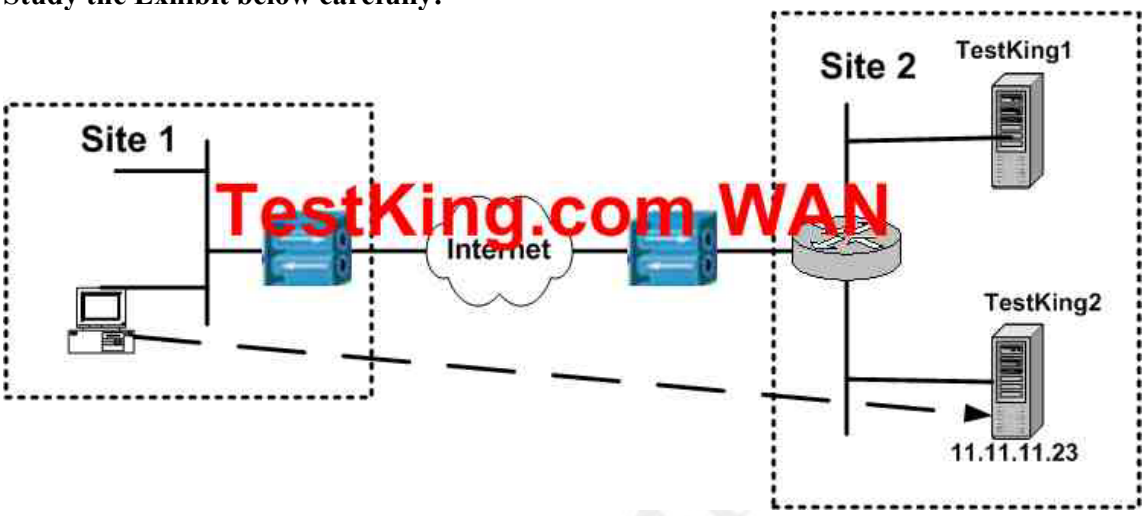
QUESTION NO: 2
In LAN-to-LAN NAT, the NAT rule type is selected; NAT source and translated network addresses are defined and LAN-to-LAN tunnel NAT rules are enabled. The final step is to tie the translated IP addresses to the Concentrator so the Concentrator knows how to route the translated IP addresses.

In which way are the translated addresses tied to the Concentrator?

A. by configuring custom private interface filters
B. by configuring static routes in the LAN-to-LAN wizard
C. by defining the local and remote networks in the LAN-to-LAN wizard
D. by enabling network auto-discovery in the LAN-to-LAN wizard

Answer: C

QUESTION NO: 3
Study the Exhibit below carefully:

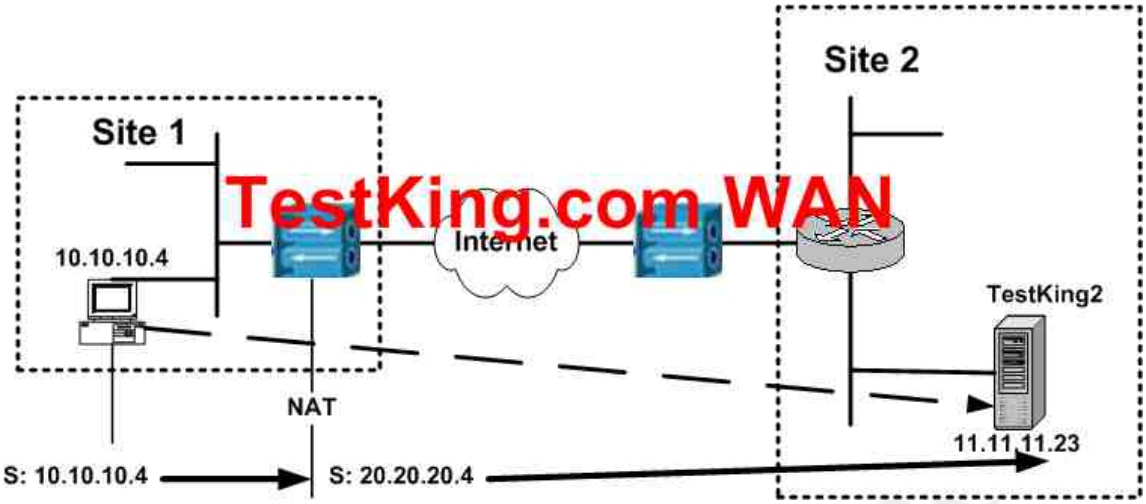


A PC at site 1 wants to access server TestKing2 through a LAN-to-LAN tunnel. Which of the following statements is valid?

A. LAN-to-LAN NAT should be performed at site 2 Concentrator only.
B. LAN-to-LAN NAT should be performed at both site 1 and 2 Concentrator.
C. LAN-to-LAN NAT should be performed at site 1 Concentrator only.
D. LAN-to-LAN NAT is not required for this application.

Answer: B
There is no exact example to verify that B, is the only correct answer, but typical NAT configurations are set on both sites.

QUESTION NO: 4
Study the Exhibit below carefully:



According to this exhibit, if any PC at site 1 wants to access server TestKing2, the PC IP address is translated to 20.20.20.X/24(X=PC host address) in this particular network. How is the source network IP address and wildcard mask configured on the Concentrator at site 1 to enable the Concentrator to perform the translation?

A. IP address – 20.20.20.0 Wildcard Mask – 0.0.0.0
B. IP address – 20.20.20.0 Wildcard Mask – 0.0.0.255
C. IP address – 10.10.10.0 Wildcard Mask – 0.0.0.0
D. IP address – 10.10.10.0 Wildcard Mask – 0.0.0.255

Answer: D

Topic 15, Cisco Virtual Private Network 3000 Series Concentrator LAN-to-LAN using Digital Certificates (5 questions)

Section 1: Root certificate installation (4 questions)

QUESTION NO: 1
Kathy the security administrator at Testking Inc. is troubleshooting SCEP enrollment. To troubleshoot SCEP enrollment, Kathy should scrutinize what event class in the event log?

A. IKE
B. IPSec
C. SCEP
D. Cert
E. RRI

Answer: D
Explanation:

The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible. The protocol supports the following operations:

- CA and RA public key distribution
- Certificate enrollment
- Certificate revocation
- Certificate query
- CRL query

QUESTION NO: 2
What is the minimum version of the PIX Firewall to enable the Cisco VPN Client to interoperate with a PIX firewall?

A. 5.1
B. 5.2
C. 5.3
D. 6.0
E. 6.1
F. 6.2

Answer: D
Explanation:

The Cisco VPN Client version 3.6 is a software product that enables the use of secure tunnels from workstations to any Cisco Easy VPN Server. Currently, these servers include the Cisco PIX Firewall (version 6.0 and later), the Cisco IOS Software-based platforms (versions 12.2(8)T and later), and the Cisco VPN 3000 Series Concentrators (version 3.0 and later).

Reference: CCSP VPN Ciscopress p. 265

QUESTION NO: 3
Which of the following represents the types of certificates found in a central CA environment? (Select two options.)

A. public key certificate
B. root certificate
C. private key certificate
D. certificate of authority
E. identity certificate
F. signature certificate

Answer: B, E
Reference: Ciscopress CCSP Self Study, CSVPN Second edition Page: 143

Explanation:

A CA certificate is used to sign other certificates. A certificate signed by itself is called a self-signing or root certificate. When one certificate issues another, the issued certificate is referred to as a subordinate certificate.
A CA might also issue an identity certificate. Identity certificates are used on specific systems or hosts. An identity certificate authenticates that the device referred to by the certificate is actually a member of the specified group. VPN Concentrators require that at least one identity certificate and its associated root certificate is present before certificate is present before certificates are employed.

Reference: CCSP VPN student guide Ciscopress p.454

QUESTION NO: 4
How many CA root certificates can the 3030 support?

A. 5
B. 8
C. 14
D. 20

Answer: D
Explanation:
The 3015, 3030, 3060, and 3080 Concentrators can support up to 20 root certificates.

Section 2: Identify certificate installation (1 questions)

QUESTION NO: 1
James is the security administrator for Testking Inc. and has upgraded the VPN Concentrator software to release 3.6. In VPN Concentrator release 3.6, certificate group matching is based on fields in which type of certificate?

A. Identity certificate
B. RA certificate
C. SSL certificate
D. CA certificate

Answer: A
Explanation:
This section of the Manager allows you to define rules to match a user's certificate to a permission group based on fields in the distinguished name (DN). In releases previous to 3.6, the VPN Concentrator used the OU field from a user's certificate to assign that user to a permission group. For example, if the OU field of a user's certificate was "Sales, " the VPN Concentrator assigned that user to the "Sales" permission group. The certificate group matching feature allows you identify members of a permission group on the basis of other criteria: you can use other fields of the certificate or you can have all certificate users share a permission group. To match users' permission groups based on other fields of the certificate, you must define rules that specify which fields to match for a group and then enable each rule for that selected group. A group must already exist in the configuration before you can create a rule for it. You can assign multiple rules to the same group. When multiple rules are assigned to the same group, a match results for the first rule that tests true. Once you have defined rules, you must configure a certificate group matching policy to define the method you want to use to identify the permission groups of certificate users: match the group from the rules, match the group from the OU field, or use a default group for all certificate users. You can use any or all of these methods.

Reference: VPN 3000 Configuration Reference 3.6.pdf