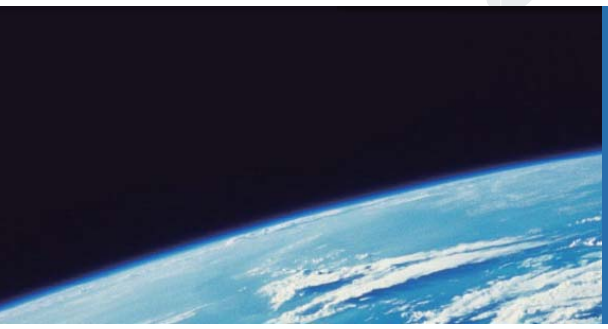
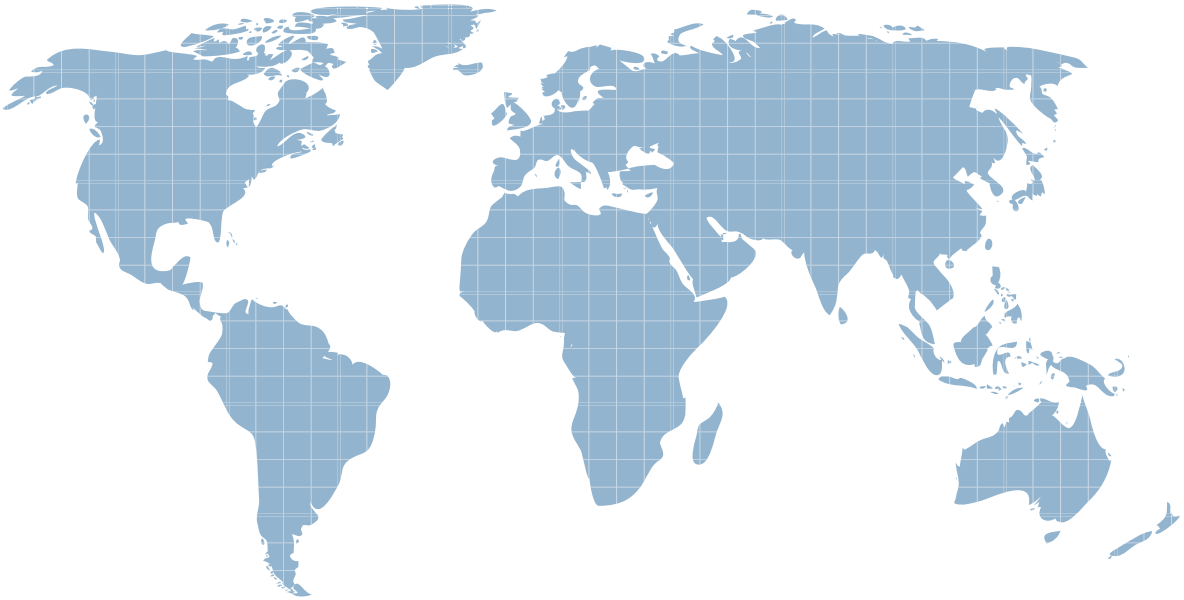


# ITTEST

## QUESTION & ANSWER

Guías de estudio precisos, Alta tasa de paso!



Ittest ofrece información actualizada de forma gratuita en un año!

http://www.ittest.es/

**Exam** : **SC0-502**

**Title** : Security Certified Program (SCP)

**Version** : Demo

1.Now that you have Certkiller somewhat under control, you are getting ready to go home for the night. You have made good progress on the network recently, and things seem to be going smoothly. On your way out, you stop by the CEO's office and say good night. You are told that you will be meeting in the morning, so try to get in a few minutes early.
The next morning, you get to the office 20 minutes earlier than normal, and the CEO stops by your office, "Thanks for coming in a bit early. No problem really, I just wanted to discuss with you a current need we have with the network."
"OK, go right ahead." You know the network pretty well by now, and are ready for whatever is thrown your way.
"We are hiring 5 new salespeople, and they will all be working from home or on the road. I want to be sure that the network stays safe, and that they can get access no matter where they are."
"Not a problem," you reply. "I'll get the plan for this done right away."
"Thanks a lot, if you have any questions for me, just let me know."
You are relieved that there was not a major problem and do some background work for integrating the new remote users. After talking with the CEO more, you find out that the users will be working from there home nearly all the time, with very little access from on the road locations.
The remote users are all using Windows 2000 Professional, and will be part of the domain. The CEO has purchased all the remote users brand new Compaq laptops, just like the one used in the CEO's office, and which the CEO takes home each night; complete with DVD\CD-burner drives, built-in WNICs, 17" LCD widescreen displays, oversized hard drives, a gig of memory, and fast processing. 'I wish I was on the road to get one of those,' you think.
You start planning and decide that you will implement a new VPN Server next to the Web and FTP Server. You are going to assign the remote users IP Addresses: 10.10.60.100~10.10.60.105, and will configure the systems to run Windows 2000 Professional.
Based on this information, and your knowledge of the Certkiller network up to this point, choose the best solution for the secure remote user needs:}

A. You begin with configuring the VPN server, which is running Windows 2000 Server. You create five new accounts on that system, granting each of them the Allow Virtual Private Connections right in Active Directory Users and Computers. You then configure the range of IP Addresses to provide to the clients as: 10.10.60.100 through 10.10.60.105. Next, you configure five IPSec Tunnel endpoints on the server, each to use L2TP as the protocol.
Then, you configure the clients. On each system, you configure a shortcut on the desktop to use to connect to the VPN. The shortcut is configured to create an L2TP IPSec tunnel to the VPN server. The connection itself is configured to exchange keys with the user's ISP to create a tunnel between the user's ISP endpoint and the Certkiller VPN Server.
B. To start the project, you first work on the laptops you have been given. On each laptop, you configure the system to make a single Internet connection to the user's ISP.

Next, you configure a shortcut on the desktop for the VPN connection. You design the connection to use L2TP, with port filtering on outbound UDP 500 and UDP 1701. When a user double-clicks the desktop icon you have it configured to make an automatic tunnel to the VPN server.
On the VPN server, you configure the system to use L2TP with port filtering on inbound UDP 500 and UDP 1701. You create a static pool of assigned IP Address reservations for the five remote clients. You configure automatic redirection on the VPN server in the routing and remote access MMC, so once the client has connected to the VPN server, he or she will automatically be redirected to the inside network, with all resources available in his or her Network Neighborhood.
C. You configure the VPN clients first, by installing the VPN High Encryption Service Pack. With this installed, you configure the clients to use RSA, with 1024-bit keys. You configure a shortcut on the desktop that automatically uses the private\public key pair to communicate with the VPN Server, regardless of where the user is locally connected.
On the VPN Server, you also install the VPN High Encryption Service Pack, and configure 1024-bit RSA encryption. You create five new user accounts, and grant them all remote access rights, using Active Directory Sites and Services. You configure the VPN service to send the server's public key to the remote users upon the request to configure the tunnel. Once the request is made, the VPN server will build the tunnel, from the server side, to the client.
D. You decide to start the configuration on the VPN clients. You create a shortcut on the desktop to connect to the VPN Server. Your design is such that the user will simply double-click the shortcut and the client will make the VPN connection to the server, using PPTP. You do not configure any filters on the VPN client systems.
On the VPN Server, you first configure routing and remote access for the new accounts and allow them to have Dial-In access. You then configure a static IP Address pool for the five remote users. Next, you configure the remote access policy to grant remote access, and you implement the following PPTP filtering:
¨´Inbound Protocol 47 (GRE) allowed
¨´Inbound TCP source port 0, detination port 1723 allowed
¨´Inbound TCP source port 520, destination port 520 allowed
¨´Outbound Protocol 47 (GRE) allowed
¨´Outbound TCP source port 1723, destination port 0 allowed
¨´Outbound TCP source port 520, destination port 520 allowed
E. You choose to configure the VPN server first, by installing the VPN High Encryption Service Pack and the HISECVPN.INF built-in security template through the Security Configuration and Analysis Snap-In. Once the Service pack and template are installed, you configure five user accounts and a static pool of IP Addresses for each account.
You then configure the PPTP service on the VPN server, without using inbound or outbound filters - due to the protection of the Service Pack. You grant each user the right to dial into the server remotely, and move on to the laptops.
On each laptop, you install the VPN High Encryption Service Pack, to bring the security level of the laptops up to the same level as the VPN server. You then configure a shortcut on each desktop that controls the direct transport VPN connection from the client to the

server.

Answer: D

2.For three years you have worked with Certkiller doing occasional network and security consulting. Certkiller is a small business that provides real estate listings and data to realtors in several of the surrounding states. The company is open for business Monday through Friday from 9 am to 6 pm, closed all evenings and weekends. Your work there has largely consisted of advice and planning, and you have been frequently disappointed by the lack of execution and follow through from the full time staff.
On Tuesday, you received a call from Certkiller 's HR director, "Hello, I'd like to inform you that Red (the full time senior network administrator) is no longer with us, and we would like to know if you are interested in working with us full time."
You currently have no other main clients, so you reply, "Sure, when do you need me to get going?"
"Today," comes the fast and direct response. Too fast, you think.
"What is the urgency, why can't this wait until tomorrow?"
"Red was let go, and he was not happy about it. We are worried that he might have done something to our network on the way out."
"OK, let me get some things ready, and I'll be over there shortly."
You knew this would be messy when you came in, but you did have some advantage in that you already knew the network. You had recommended many changes in the past, none of which would be implemented by Red. While pulling together your laptop and other tools, you grab your notes which have an overview of the network:
Certkiller network notes: Single Internet access point, T1, connected to Certkiller Cisco router. Router has E1 to a private web and ftp server and E0 to the LAN switch. LAN switch has four servers, four printers, and 100 client machines. All the machines are running Windows 2000. Currently, they are having their primary web site and email hosted by an ISP in Illinois.
When you get to Certkiller , the HR Director and the CEO, both of whom you already know, greet you. The CEO informs you that Red was let go due to difficult personality conflicts, among other reasons, and the termination was not cordial.
You are to sign the proper employment papers, and get right on the job. You are given the rest of the day to get setup and running, but the company is quite concerned about the security of their network. Rightly so, you think, 'If these guys had implemented even half of my recommendations this would sure be easier.' You get your equipment setup in your new oversized office space, and get started. For the time you are working here, your IP Address is 10.10.50.23 with a mask of \16.
One of your first tasks is to examine the router's configuration. You console into the router, issue a show running-config command, and get the following output:
MegaOne#show running-config
Building configuration...
Current configuration:

```
!
version 12.1
service udp-small-servers
service tcp-small-servers
!
hostname MegaOne
!
enable secret 5 $1$7BSK3$H394yewhJ45JAFEWU73747.
enable password clever
!
no ip name-server
no ip domain-lookup
ip routing
!
interface Ethernet0
no shutdown
ip address 2.3.57.50 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
no shutdown
ip 10.10.40.101 255.255.0.0
no ip directed-broadcast
!
interface Serial0
no shutdown
ip 1.20.30.23 255.255.255.0
no ip directed-broadcast
clockrate 1024000
bandwidth 1024
encapsulation hdlc
!
ip route 0.0.0.0 0.0.0.0 1.20.30.45
!
line console 0
exec-timeout 0 0
transport input all
line vty 0 4
password remote
login
!
end
```

After analysis of the network, you recommend that the router have a new configuration. Your goal is to make the router become part of your layered defense,

and to be a system configured to help secure the network.
You talk to the CEO to get an idea of what the goals of the router should be in the new configuration. All your conversations are to go through the CEO; this is whom you also are to report to.
"OK, I suggest that the employees be strictly restricted to only the services that they must access on the Internet." You begin.
"I can understand that, but we have always had an open policy. I like the employees to feel comfortable, and not feel like we are watching over them all the time. Please leave the connection open so they can get to whatever they need to get to. We can always reevaluate this in an ongoing basis."
"OK, if you insist, but for the record I am opposed to that policy."
"Noted," responds the CEO, somewhat bluntly.
"All right, let's see, the private web and ftp server have to be accessed by the Internet, restricted to the accounts on the server. We will continue to use the Illinois ISP to host our main web site and to host our email. What else, is there anything else that needs to be accessed from the Internet?"
"No, I think that's it. We have a pretty simple network, we do everything in house."
"All right, we need to get a plan in place as well right away for a security policy. Can we set something up for tomorrow?" you ask.
"Let me see, I'll get back to you later." With that the CEO leaves and you get to work.
Based on the information you have from Certkiller ; knowing that the router must be an integral part of the security of the organization, select the best solution to the organization's router problem:}

A. You backup the current router config to a temp location on your laptop. Friday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

```
MegaOne#configure terminal
MegaOne(config)#no cdp run
MegaOne(config)#no ip source-route
MegaOne(config)#no ip finger
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 deny ip 0.0.0.0 255.255.255.255 any
MegaOne(config)#access-list 175 deny ip 10.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 127.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 deny ip 192.168.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
```

MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface serial 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no ip directed broadcast
MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z
MegaOne#

B. You backup the current router config to a temp location on your laptop. Sunday night, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Ethernet 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no cdp enable
MegaOne(config)#interface Ethernet 1
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no cdp enable
MegaOne(config-if)#Z
MegaOne#

C. You backup the current router config to a temp location on your laptop. Early Monday morning, you come in to build the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:

MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Serial 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no cdp enable
MegaOne(config-if)#no ip directed broadcast

MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z
MegaOne#
D. As soon as the office closes Friday, you get to work on the new router configuration. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#interface Ethernet 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config)#interface Ethernet 1
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#Z
MegaOne#
E. With the office closed, you decide to build the new router configuration on Saturday. Using your knowledge of the network, and your conversation with the CEO, you build and implement the following router configuration:
MegaOne#configure terminal
MegaOne(config)#no cdp run
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 80
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 20
MegaOne(config)#access-list 175 permit tcp any 2.3.57.60 0.0.0.0 eq 21
MegaOne(config)#access-list 175 permit tcp any 10.10.0.0 0.0.255.255 established
MegaOne(config)#access-list 175 permit ip any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit udp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 permit icmp any 10.10.0.0 0.0.255.255
MegaOne(config)#access-list 175 deny ip 0.0.0.0 255.255.255.255 any
MegaOne(config)#access-list 175 deny ip 10.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 127.0.0.0 0.255.255.255 any
MegaOne(config)#access-list 175 deny ip 172.16.0.0 0.0.255.255 any
MegaOne(config)#access-list 175 deny ip 192.168.0.0 0.0.255.255 any
MegaOne(config)#no ip source-route
MegaOne(config)#no ip finger
MegaOne(config)#interface serial 0
MegaOne(config-if)#ip access-group 175 in
MegaOne(config-if)#no ip directed broadcast
MegaOne(config-if)#no ip unreachables
MegaOne(config-if)#Z

MegaOne#
Answer: A

3.It has been quite some time since you were called in to address the network and security needs of Certkiller . You feel good in what you have accomplished so far. You have been able to get Certkiller to deal with their Security Policy issue, you have secured the router, added a firewall, added intrusion detection, hardened the Operating Systems, and more.
One thing you have not done however, is run active testing against the network from the outside. This next level of testing is the final step, you decide, in wrapping up this first stage of the new Certkiller network and security system. You setup a meeting with the CEO to discuss.
"We have only one significant issue left to deal with here at Certkiller ," you begin. "We need some really solid testing of our network and our security systems."
"Sounds fine to me, don't you do that all the time anyway? I mean, why meet about this?"
"Well, in this case, I'd like to ask to bring in outside help. Folks who specialize in this sort of thing. I can do some of it, but it is not my specialty, and the outside look in will be better and more independent from an outside team."
"What does that kind of thing cost, how long will it take?"
"It will cost a bit of money, it won't be free, and with a network of our size, I think it can be done pretty quick. Once this is done and wrapped up, I will be resigning as the full time security and network pro here. I need to get back to my consulting company full time. Remember, this was not to be a permanent deal. I can help you with the interview, and this is the perfect time to wrap up that transition."
"All right, fair enough. Get me your initial project estimates, and then I can make a more complete decision. And, I'll get HR on hiring a new person right away."
Later that afternoon you talk to the CEO and determine a budget for the testing. Once you get back to your office, you are calling different firms and consultants, and eventually you find a consulting group that you will work with.
A few days later you meet with the group in their office, and you describe what you are looking for, and that their contact and person to report to is you. They ask what is off limits, and your response is only that they cannot do anything illegal, to which they agree and point out is written in their agreement as well.
With this outside consulting group and your knowledge of the network and company, review and select the solution that will best provide for a complete test of the security of Certkiller .}

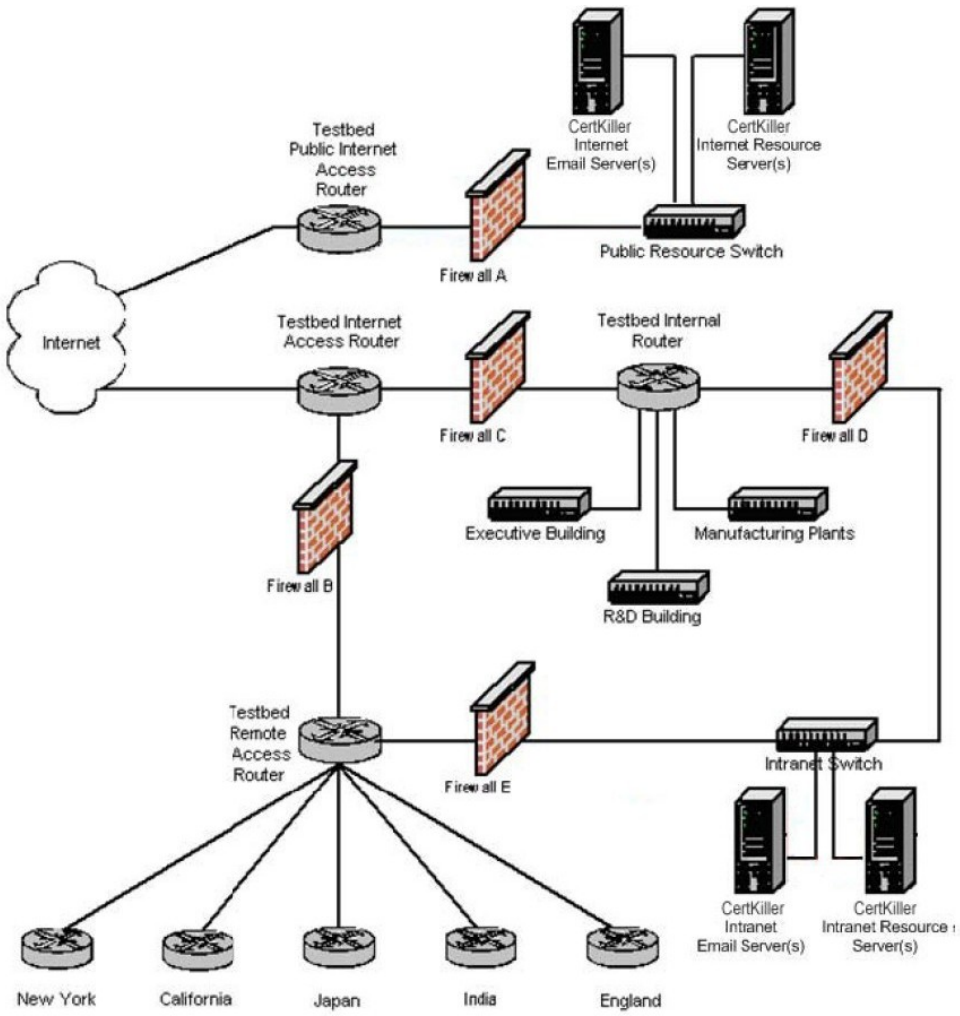
A. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.
The first thing the consultants will do is dumpster diving and physical surveillance, looking for clues as to user information and other secret data that should not be outside of the network. Once they have identified several targets through the dumpster diving, they

will run scans to match up and identify the workstations for those users.
After identifying the user workstations, they will run vulnerability checks on the systems, to find holes, and if a hole is found they have been given permission to exploit the hole and gain access of the system.
They will attempt to gain access to the firewall and router remotely, via password guessing, and will test the response of the network to Denial of Service attacks. Finally, they will call into Certkiller to see what information they can learn via social engineering.
B. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.
The consultants will first run remote network surveillance to identify hosts, followed by port scans and both passive and active fingerprinting. They will then run vulnerability scanners on the identified systems, and attempt to exploit any found vulnerabilities. They will next scan and test the router and firewall, followed by testing of the IDS rules.
They will then perform physical surveillance and dumpster diving to learn additional information. This will be followed by password sniffing and cracking. Finally, they will call into Certkiller to see what information they can learn via social engineering.
C. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.
The consultants surprise you with their initial strategy. They intend to spend nearly 100% of their efforts over the first week on social engineering and other physical techniques, using little to no technology. They have gained access to the building as a maintenance crew, and will be coming into the office every night when employees are wrapping up for the day.
All of their testing will be done through physical contact and informal questioning of the employees. Once they finish that stage, they will run short and direct vulnerability scanners on the systems that they feel will present weakness.
D. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.
The consultants have decided on a direct strategy. They will work inside the Certkiller office, with the group introducing themselves to the employees. They will directly interview each employee, and perform extensive physical security checks of the network. They will review and provide analysis on the security policy, and follow that with electronic testing. They will run a single very robust vulnerability scanner on every single client and server in the network, and document the findings of the scan.
E. The consulting group has identified the steps it will follow in testing the network. You have asked to be kept up to date, and given an approximate schedule of events. You intend to follow along with the test, with weekly reports.
The consultants will start the process with remote network surveillance, checking to see what systems and services are available remotely. They will run both passive and active fingerprinting on any identified system. They will run customized vulnerability scanners on the identified systems, and follow that through with exploits, including new zero-day

exploits they have written themselves.
They will next run scans on the router, firewall, and intrusion detection, looking to identify operating systems and configurations of these devices. Once identified, they will run customized scripts to gain access to these devices. Once they complete the testing on the systems, they will dumpster dive to identify any leaked information.
Answer: B

4.Certkiller is a company that makes state of the art aircraft for commercial and government use. Recently Certkiller has been working on the next generation of low orbit space vehicles, again for both commercial and governmental markets.
Certkiller has corporate headquarters in Testbed, Nevada, US

A. Testbed is a small
town, with a population of less than 50,000 people. Certkiller is the largest company in town, where most families have at least one family member working there.
The corporate office in Testbed has 4,000 total employees, on a 40-acre campus environment. The largest buildings are the manufacturing plants, which are right next to the Research and Development labs. The manufacturing plants employee approximately 1,000 people and the R&D labs employ 500 people. There is one executive building, where approximately 500 people work. The rest of the employees work in Marketing, Accounting, Press and Investor Relations, and so on. The entire complex has a vast underground complex of tunnels that connect each building.
All critical functions are run from the Testbed office, with remote offices around the world. The remote offices are involved in marketing and sales of Certkiller products. These offices also perform maintenance on the Certkiller aircraft and will occasionally perform R&D and on-site manufacturing.
There are 5 remote offices, located in: New York, California, Japan, India, and England. Each of the remote offices has a dedicated T3 line to the Certkiller HQ, and all network traffic is routed through the Testbed office - the remote offices do not have direct Internet connections.
You had been working for two years in the New York office, and have been interviewing for the lead security architect position in Testbed. The lead security architect reports directly to the Chief Security Officer (CSO), who calls you to let you know that you got the job. You are to report to Testbed in one month, just in time for the annual meeting, and in the meantime you review the overview of the Certkiller network.




Your first day in Certkiller Testbed, you get your office setup, move your things in place, and about the time you turn on your laptop, there is a knock on your door. It is Blue, the Chief Security Officer, who informs you that there is a meeting that you need to attend in a half an hour.

With your laptop in hand, you come to the meeting, and are introduced to everyone. Blue begins the meeting with a discussion on the current state of security in Certkiller .

"For several years now, we have constantly been spending more and more money on our network defense, and I feel confident that we are currently well defended." Blue, puts a picture on the wall projecting the image of the network, and then continues, "We have firewalls at each critical point, we have separate Internet access for our public systems, and all traffic is routed through our controlled access points. So, with all this, you might be wondering why I have concern."

At this point a few people seem to nod in agreement. For years, Certkiller has been at the forefront of perimeter defense and security. Most in the meeting are not aware that there is much else that could be done.

Blue continues, "Some of you know this, for the rest it is new news: MassiveCorp is moving their offices to the town right next to us here. Now, as you all know, MassiveCorp has been trying to build their orbital systems up to our standards for

years and have never been able to do so. So, from a security point of view, I am concerned."
This is news to most people, Green, the Vice President of Research asks, "We have the best in firewalls, we have the best in you and your systems, what are you suggesting?"
Blue responds, "I suggest trust. Not with MassiveCorp, but in our own systems. We must build trusted networks. We must migrate our network from one that is well-defended to one that is well-defended and one that allows us to trust all the network traffic."
The meeting continues for some time, with Blue leading the discussion on a whole new set of technologies currently not used in the network. After some time, it is agreed upon that Certkiller will migrate to a trusted networking environment.
The following week, Blue informs you that you will be working directly together on the development of the planning and design of the trusted network. The network is going to run a full PKI, with all clients and servers in the network using digital certificates. You are grateful that in the past two years, Blue has had all the systems changed to be running only Windows 2000, both server and professional systems, running Active Directory. You think the consistent platform will make the PKI roll out easier.
The entire Certkiller network is running Active Directory, with the domain structure as in the following list:
Testbed. Certkiller .org
Newyork. Certkiller .org
California. Certkiller .org
Japan. Certkiller .org
India. Certkiller .org
England. Certkiller .org
Although you will be working in the Testbed office, the plan you develop will need to include the entire Certkiller organization.
Based on this information, select the solution that describes the best plan for the new trusted network of Certkiller :}

A. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a CPF based on your own guidelines, including physical and technology controls.
3. Design the system to be a full hierarchy, with the Root CA located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.
4. Design the hierarchy with each remote office and building having it's own enrollment CA.

5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
7. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.
B. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a CPF based on your own guidelines, including physical and technology controls.
3. Design the system, outside of the executive office, to be a full hierarchy, with the Root CA for the hierarchy located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.
4. In the executive building, you design the system to be a mesh CA structure, with one CA per floor of the building.
5. Design the hierarchy with each remote office and building having it's own enrollment CA.
6. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
7. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
8. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.
9. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.
10. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
11. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.
C. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
1. Draft a Certificate Policy (CP) document to define what users will be allowed to do with their certificates, and a Certification Practice Statement (CPS) document to define the technology used to ensure the users are able to use their certificates as per the CPS.

2. Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component.
3. Design the system to be a full hierarchy, with the Root CA located in the executive building. Every remote office will have a subordinate CA, and every other building on the campus in Testbed will have a subordinate CA.
4. Design the hierarchy with each remote office and building having it's own enrollment CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
7. Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.
D. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
1. Draft a Certificate Policy (CP) document to define what users will be allowed to do with their certificates, and a Certification Practice Statement (CPS) document to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component.
3. Design the system to be a full mesh, with the Root CA located in the executive building.
4. Design the mesh with each remote office and building having it's own Root CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA mesh in the executive office, and get all users acclimated to the system.
7. Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.
E. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
1. Draft a Certification Practice Statement (CPS) to define what users will be allowed to

do with their certificates, and a Certificate Policy (CP) to define the technology used to ensure the users are able to use their certificates as per the CPS.
2. Draft a CPF based on your own guidelines, including physical and technology controls.
3. Design the system to be a full mesh, with the Root CA located in the executive building.
4. Design the mesh with each remote office and building having it's own Root CA.
5. Build a small test pilot program, to test the hierarchy, and integration with the existing network.
6. Implement the CA mesh in the executive office, and get all users acclimated to the system.
7. Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
8. One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the system.
9. Test the team in each location on proper use and understanding of the overall PKI and their portion of the trusted network.
10. Evaluate the rollout, test, and modify as needed to improve the overall security of the Certkiller trusted network.
Answer: C

5.Blue thanks you for your plan and design and took it into consideration. You are then informed that Blue has gone ahead and made a new plan, which will incorporate some of your suggestions, but is going to build the network a bit differently. In Testbed and in each remote office there will be a single self-sufficient CA hierarchy, one that is designed to directly integrate with the existing network. Blue mentions that the hierarchy is only to go two-levels deep, you are not to make an extensive hierarchy in any location. This means a distinct CA hierarchy in six locations, inclusive of the Testbed headquarters.
Using this information, choose the solution that will provide for the proper rollout of the Certificate Authorities in the network.}

A. In each location, you recommend the following steps:
1. Harden a system to function as the Root CA
2. Harden a system to function as the Registration Authority
3. Configure CATool on the Root CA
4. Configure CATool on the Registration Authority, as a subordinate to the Root CA
5. Once the Subordinate CA is active, take the Root CA offline
6. Configure users for the CAs
7. Configure each Root CA to trust each other Root CA via cross certification
8. Test the CA hierarchy
9. Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate
B. In each location, you recommend the following steps:

1. Harden a system to function as the Root CA
2. Harden a system to function as a Registration Authority
3. Configure a Windows Enterprise Root CA
4. Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification
5. Configure a Windows Stand-Alone Subordinate Enrollment Authority to function as the Registration Authority
6. Once the Stand-Alone Subordinate is installed, take the Enterprise Root CA offline
7. Test the CA hierarchy
8. Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

C. In each location, you recommend the following steps:
1. Harden a system to function as the Root CA
2. Harden a system to function as the Registration Authority
3. Configure a Windows Enterprise Root CA
4. Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification
5. Configure a Windows Enterprise Registration Authority, as a subordinate to the Enterprise Root CA
6. Once the Subordinate CA is active, take the Enterprise Root CA offline
7. Test the CA hierarchy
8. Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

D. In each location, you recommend the following steps:
1. Harden a system to function as the Root CA
2. Harden a system to function as the Registration Authority
3. Configure CATool on the Root CA
4. Configure CATool on the Registration Authority, as a subordinate to the Root CA
5. Configure users for the CAs
6. Configure each Root CA to trust each other Root CA via cross certification
7. Test the CA hierarchy
8. Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

E. In each location, you recommend the following steps:
1. Harden a system to function as the Root CA
2. Harden a system to function as the Registration Authority
3. Configure a Windows Enterprise Root CA
4. Configure each Enterprise Root CA to trust each other Enterprise Root CA via cross certification
5. Configure a Windows Registration Authority, as a subordinate to the Enterprise Root CA
6. Test the CA hierarchy
7. Have the local administrative staff inform and train each user how to connect to the Registration Authority through their browser and request a certificate

Answer: E

6.Now that you have a fully functioning CA hierarchy in each location, and that the trusted network is well underway, you are called in to meet with Blue. Blue comes into the room, and you talk to one another for a while. It seems that now with the CA hierarchy in place, you need to plan the certificate rollout for the individual users and computers in the network.
Since this is the executive building, Blue places higher security requirements here than on the other buildings. Certificates need to be issued to all the entities, computers and users, in the network. Blue has decided that for all senior level management, the process for certificate issuance should be even more secure than the rest of the deployment.
Based on this information, and you understanding of the Certkiller environment, choose the best solution to assigning certificates to the computers and users of the trusted network in the Executive building:}

A. You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network, followed by assigning certificates to the users in the network. For this task, you divide the other administrators into four teams, one per floor of the building. Each team will be responsible for the assigning of certificates to the computers and users on the corresponding floor. To make the process faster, you have decided to install a new CA for each floor. The team leader on each floor will install and configure the CA, and you will oversee the process.
With the new CAs installed, one administrator from each team goes to each desk on the floor and makes a request for a certificate for the computer using Internet Explorer. Once the machine certificate is installed, the administrator has each user log on to their machine and the administrator walks the user through the process of connecting to the CA_SERVER\certsrv on their floor to request a user certificate.
To ensure the security of the senior level management, you lead the team on the fourth floor. You install the new CA yourself, and oversee the configuration of the certificates for every machine and user on the floor.
B. You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1. You open Active Directory Users and Computers
2. You use Group Policy to edit the domain policy that is controlling the executive building.
3. You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4. In the template list, you select computer, and define CA as the location to send the request.

5. You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart.
Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:
1. Log on to your computer as your normal user account
2. Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3. Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request.
4. When the certificate is issued, click the Install This Certificate hyperlink on screen.
Finally, you address the senior level management. For these people, you want the security to be higher, so you select a stronger algorithm for their certificates. With all the other certificates, you used the default key strength and algorithms. However, the senior level management needs higher security. Therefore, you personally walk each person through the process of requesting a certificate; only you ensure that they select 1024-bit AES as their encryption algorithm.
C. You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:
1. You open Active Directory Users and Computers
2. You use Group Policy to edit the domain policy that is controlling the executive building.
3. You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4. In the template list, you select computer, and define CA as the location to send the request.
5. You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart.
Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:
1. Log on to your computer as your normal user account
2. Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3. Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request.
4. When the certificate is issued, click the Install This Certificate hyperlink on screen.
Finally, you address the senior level management. For these people, you want the security to be higher, so you select a different certificate scheme. By using a different

scheme, you ensure that there will be no possibility of other people in the building gaining access to the senior level management accounts. For these accounts you utilize licensed PGP digital certificates that can be used for both authentication and secure email. You personally show each manager how to create and use their key ring, providing for very secure communication.

D. You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this you perform the following steps:

1. You open Active Directory Users and Computers
2. You use Group Policy to edit the domain policy that is controlling the executive building.
3. You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4. In the template list, you select computer, and define CA as the location to send the request.
5. You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart.

Once you finishing setting up the computers to be assigned certificates, you shift your focus to the users, except for the senior management, in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:

1. Log on to your computer as your normal user account
2. Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3. Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request.
4. When the certificate is issued, click the Install This Certificate hyperlink on screen.

Finally, you address the senior level management in the building. For these people, you personally go into their office and walk through the steps with each person.

1. The user logs on to the computer with their normal user account
2. You open the MMC and add the personal certificates snap-in
3. You right-click certificates and Request A New Certificate
4. The user fills in the requested information, and you verify this information.
5. You put the certificate request onto a USB drive, and take the request back to the CA.
6. You put the USB drive into the CA, manually process the request, and put the issued certificate onto the USB drive.
7. You bring the USB drive back to each person, and manually import their new certificate

E. You meet with the other administrators of the executive building and let them know what you are working on, and how they can help. You will first assign certificates to the computers in the network. To make the process easier, you have decided to configure the network so that the computers will request certificates automatically. In order to do this

you perform the following steps:
1. You open Active Directory Users and Computers
2. You use Group Policy to edit the domain policy that is controlling the executive building.
3. You expand Computer Configuration to Public Key Policies, and you click the Automatic Certificate request option.
4. In the template list, you select computer, and define CA as the location to send the request.
5. You restart the computers that you can, and wait for the policy to refresh on the systems you cannot restart.
Once you finishing setting up the computers to be assigned certificates, you shift your focus to all the users in the executive building. In order to have each user obtain a certificate you issue a memo (the actual memo goes into extreme detail on each step, even listing common questions and answers) to all users that instructs them to perform the following steps:
1. Log on to your computer as your normal user account
2. Open Internet Explorer, and to connect to the CA_SERVER\certsrv.
3. Select the option to Request A Certificate, and to choose a User Certificate Request type, then submit the request.
4. When the certificate is issued, click the Install This Certificate hyperlink on screen.
Answer: D

7.Now that the network is moving towards a trusted network, you are preparing for the specific new implementations in Certkiller . Just as you wrap up some paperwork for the morning, Blue calls you and lets you know that you are going to be needed in a meeting this afternoon.
You get to Blue's office and sit down at the desk. Blue begins the conversation, "You know we have some solid fundamental issues addressed in our new trusted network, but I have yet to feel that we have addressed any serious concerns."
"I've been thinking about some similar issues," you reply.
"Good, then I'm sure you have been thinking about our email. Right now, I cannot guarantee the integrity of any email, and I cannot guarantee the confidentiality of any email. We have reasonable controls towards guaranteeing the availability of our email, but what's the point if there is no confidentiality or integrity?"
"I agree. I think that addressing this issue should be an immediate priority."
"One concern is that whatever the system is that we put in place, it must be very user-friendly. As we roll out these new systems, anything that will significantly increase the calls into the help desk is something we need to minimize. A second concern is that it not be too costly. We already have this new investment in the trusted network, we need to be sure that we utilize what are building to the fullest extent possible."
"I think we should be able to do that without much difficulty. I already have some solid ideas," you reply.
"OK, take a few days on this. For the moment, just concern yourself with the

executive building; the others can follow the plan in their own buildings. Let's meet again this coming Monday and you can describe your suggestion then."
Based on this conversation, and your knowledge of Certkiller , select the best solution to the email problems in the network.}
A. After careful consideration you decide that you will implement secure email in a test group using PGP. You will use a full licensed version of PGP. You will go to each computer and you will install the full PGP on each system.
Once installed, you will show each user how to create a PGP certificate by requesting the certificate from the CATool CA server you installed specifically for secure email. After the user has received a certificate, you associate that PGP certificate with their Windows domain user account.
With the PGP certificate associated with the user account, you show each user how to manage their key ring. You show them how to generate their key, and you configure all user's key strength to be 2048 bits. Now that the user has a strong key and a PGP certificate, you configure the email client of each user.
You explain that each user will have to install the public key of each other user in the network. You test this by sending an email from your laptop with your PGP certificate attached, and you have the user save the attachment to their Outlook folder. With the certificate saved, you show them how to send secure email to you. You receive the email on your laptop, and double-click the lock to show the user that the secure email message was successfully sent and received.
B. After careful consideration you decide that you will implement secure email in a test group using X.509v3 digital certificates. You choose this since every user received their certificate during an earlier phase, and those certificates included the ability to be used for secure email.
Using the X.509v3 certificates, you will configure each machine to use S\MIME. You go to each computer and open Outlook Express, which is the default client email program in the test group. You go to the Tools and Account option, selecting the Mail tab, and the properties for the email account.
You select he Security Tab and in the submenu for the Signing Certificate you configure the certificate for the user's account. You select 3DES as the algorithm to use. You then check the Encrypt Contents And Attachments For All Outgoing Messages check box and the Digitally Sign All Outgoing Messages check box. You accept the default of including the digital id when sending signed messages and the default to add sender's certificates to the user's address book, and close the properties the email account.
You show the user how to send and receive email, showing the red ribbon that indicates a signed message and the blue lock that indicates an encrypted message.
C. After careful consideration you decide that you will implement secure email in a test group using GPG. You have decided to use GPG to avoid any licensing conflicts that might occur if any user requires secure email exchange with another individual that is in a country with different cryptography laws. You will go to each computer and you will install GPG on each system.
Once installed, you will show each user how to create the required directory structure, by typing the command: gpg --gen-key Once the directory structure is created, you will

show each user how to generate the required files, by typing the command: gpg --gen-key Since you want very secure email, you configure each system to use 2048 bit key strength and you select DSA and ElGamal encryption.
With GPG installed and configured, you show each user how to use their new secure email. You have them open Outlook and create a new message to you. Once the message is created, you have them select the Security drop-down list and choose both GPG Sign and GPG Encrypt, and then press send.
You show them on your laptop that you receive the message. You press Reply, and on your laptop also select the Security drop-down menu, where you choose both GPG Sign and GPG Encrypt. The user receives the message, and you show that secure email was successfully sent and received.
D. After careful consideration you decide that you will implement secure email in a test group using PGP. You will use a full licensed version of PGP. You will go to each computer and you will install the full PGP on each system.
Once installed, you will show each user how to create a PGP certificate by requesting the certificate from the MS Enterprise Root CA server you installed, and configured specifically for secure email certificates. After the user has received a certificate, you associate that PGP certificate with their Windows domain user account.
With the PGP certificate associated with the user account, you show each user how to manage their key ring. You show them how to generate their key, and you configure all user's key strength to be 2048 bits. Now that the user has a strong key and a PGP certificate, you configure the email client of each user.
You explain that each user will have to install the public key of each other user in the network. You test this by sending an email from your laptop with your PGP certificate attached, and you have the user save the attachment to their Outlook folder. With the certificate saved, you show them how to send secure email to you. You receive the email on your laptop, and double-click the lock to show the user that the secure email message was successfully sent and received.
E. After careful consideration you decide that you will implement secure email in a test group using X.509v3 digital certificates. You choose this since every user received their certificate during an earlier phase, and those certificates included the ability to be used for secure email.
You will configure each machine to use PGP, with the X.509v3 certificates option. You go to each computer and open Outlook Express, which is the default client email program in the test group. You go to the Tools and Account option, selecting the Mail tab, and the properties for the email account.
You select he Security Tab and in the submenu for the Signing Certificate you configure the certificate for the user's account. You select DSA and ElGamal as the cryptosystem to use. You then check the Encrypt Contents And Attachments For All Outgoing Messages check box and the Digitally Sign All Outgoing Messages check box. You accept the default of including the digital id when sending signed messages and the default to add sender's certificates to the user's address book, and close the properties the email account.
You show the user how to send and receive email, showing the red ribbon that indicates a signed message and the blue lock that indicates an encrypted message.

Answer: B

8.You have now been involved in several major changes in the security of Certkiller , and specifically the Testbed campus. You have worked on the planning and design of the trusted network, you have worked on the initial rollout of the CA hierarchy, you have worked on assigning certificates to the end users and computers in the Executive building of the Testbed campus, and you have managed the implementation of secure email - a critical service for Certkiller .
Blue has asked you to meet with the other administrative staff of the Testbed campus and discuss how the certificates will impact the organization. There are a total of about 40 people in the meeting, and you have decided that your primary focus during this meeting will be on encryption\cryptography.
Choose the best solution for providing the correct information to your administrative staff on how encryption\cryptography and digital certificates will be properly used in the network:}

A. You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the Certkiller network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA has a pair of keys and UserB has a pair of keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB.
"We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserB will use the public key that UserA has made available to encrypt the message. Once encrypted, UserB will send the message over the network to User
A. UserA will then use the other key of the pair, the private key to decrypt the message," you explain to the group.
You further explain some of the common algorithms used in the network. You tell them that Diffie-Hellman was the first widely used private key algorithm, and that Diffie-Hellman itself is not used to secure messages, rather to exchange a symmetric key. You explain that RSA was another breakthrough in that it was a private key algorithm that was able to secure messages.
You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.
B. You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the Certkiller network.

You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA has a pair of keys and UserB has a pair of keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB.
"We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the public key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, called the private key, to decrypt the message," you explain to the group.
You further explain some of the common algorithms used in the network. You tell them that Diffie-Hellman was the first widely used public key algorithm, and that Diffie-Hellman itself is not used to secure messages, rather to exchange a symmetric key. You explain that RSA was another breakthrough in that it was a public key algorithm that was able to secure messages.
You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.

C. You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the Certkiller network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA and UserB have a set of mathematically linked keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB.
"We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the public key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the private key to decrypt the message," you explain to the group.
You further explain some of the common algorithms used in the network. You tell them that RSA was the first widely used private key algorithm, and that RSA itself is not used to secure messages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough in that it was a private key algorithm that was able to secure messages.
You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject

Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.
D. You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the Certkiller network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA and UserB have a set of mathematically linked keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB.
"We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the private key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the public key to decrypt the message," you explain to the group.
You further explain some of the common algorithms used in the network. You tell them that RSA was the first widely used private key algorithm, and that RSA itself is not used to secure messages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough in that it was a private key algorithm that was able to secure messages.
You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the entity that issued the certificate, and a Subject Field that holds the distinguished name of the person who has the private key that corresponds to the public key in the certificate.
E. You gather the administrative staff together in the conference room to discuss cryptography in the network. You begin your talk with the function of cryptography, in general, and then you move towards specific implementations in the Certkiller network. You explain that public key cryptography is founded on math, and that the big picture fundamental point is that UserA and UserB have a set of mathematically linked keys. You explain that one key of each key pair is made available to the other users in the network. You illustrate this with an example of sending an encrypted message from UserA to UserB.
"We know, for example, that UserA wishes to send a message to UserB and wants that message to be secure. UserA will use the private key that UserB has made available to encrypt the message. Once encrypted, UserA will send the message over the network to UserB. UserB will then use the other key of the pair, the public key to decrypt the message," you explain to the group.
You further explain some of the common algorithms used in the network. You tell them that RSA was the first widely used private key algorithm, and that RSA itself is not used to secure messages, rather to exchange a symmetric key. You explain that Diffie-Hellman was another breakthrough in that it was a private key algorithm that was able to secure messages.

You then describe digital certificates and some of their features. You tell the group that digital certificates can be assigned to different entities, including users and computers. You state that these digital certificates include many options, for example an Issuer Field that holds the distinguished name of the person who issued the certificate, and a Subject Field that holds the full OIDs describing the use of the certificate by the holder of the certificate.
Answer: B

9.You have now seen to it that all end users and computers in the Testbed office have received their certificates. The administrative staff has been trained on their use and function in the network. The following day, you meet with Blue to discuss the progress.
"So far so good," starts Blue, "all the users have their certificates, all the computers have their certificates. I think we are moving forward at a solid pace. We have talked about the ways we will use our certificates, and we need to move towards securing our network traffic."
"I agree," you reply, "last week I ran a scheduled scan, and we still have vulnerability in our network traffic. The folks from MassiveCorp would love to have a sniffer running in here, I'm sure of that."
"That's exactly the point. We need a system in place that will ensure that our network traffic is not so vulnerable to sniffing. We have to get some protection for our packets. I'd like you to design the system and then we can review it together."
The meeting ends a few minutes later, and you are back in your office working on the design.
Choose the best solution for protecting the network traffic in the executive office of the Testbed campus:}

A. After further analysis on the situation, you decide that you will need to block traffic in a more complete way at the border firewalls. You have decided that by implementing stricter border control, you will be able to manage the security risk of the packets that enter and leave the network better.
You implement a new firewall at each border crossing point. You will configure half of the firewalls with Checkpoint FW-1 NG and the other half with Microsoft IS
A. By using
two different firewalls, you are confident that you will be minimizing any mass vulnerability.
At each firewall you implement a new digital certificate for server authentication, and you configure the firewall to require every user to authenticate all user connections. You block all unauthorized traffic and run remote test scans to ensure that no information is leaking through.
Once the test scans are complete, you verify that all users are required to authenticate with the new firewall before their traffic is allowed to pass, and everything works as you planned.
B. You spend time analyzing the network and decide that the best solution is to take

advantage of VPN technology. You will create one VPN endpoint in each building. Your plan is to create a unique tunnel between each building.
You first install a new Microsoft machine, and configure it to perform the functions of Routing and Remote Access. You then create a tunnel endpoint, and configure each machine to use L2TP to create the tunnel.
To increase security, you will implement full 256-bit encryption on each tunnel, and you will use 3DES on one half of the tunnels and AES on the other half of the tunnels. You will be sure that each tunnel uses the same algorithm on both ends, but by using two algorithms you are sure that you have increased the security of the network in a significant way.
C. You decide that you will implement an IPSec solution, using the built-in functionality of Windows. You decide that you wish for there to be maximum strength, and therefore you choose to implement IPSec using both AH and ESP.
First, you configure each server in the network with a new IPSec policy. You choose to implement the default Server IPSec Policy. Using this policy you are sure that all communication both to and from the server will utilize IPSec. You reboot the servers that you can and use secedit to force the others to refresh their policy.
Next, with the help of the administrative staff, you will configure each client in the network. For the clients, you use the default Client IPSec Policy. You reboot the client machines that you can and use secedit to force the others to refresh their policy.
D. You decide that you will implement an IPSec solution, using custom IPSec settings. You wish to utilize the digital certificates that are available in the network. You decide that you wish for there to be maximum strength, and therefore you choose to implement IPSec using both AH and ESP.
First, you configure a custom policy for the servers in the network. You verify that none of the default policies are currently implemented, and you create a new policy. Your new policy will use SHA for AH and SHA+3DES for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the servers that you can and use secedit to force the others to refresh their policy.
Next, with the help of the administrative staff, you will configure each client in the network. For the clients, you verify that no default policy is enabled, and you create a policy that uses SHA for AH and SHA+3DES for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the client machines that you can and use secedit to force the others to refresh their policy.
E. You decide that you will implement an IPSec solution, using custom IPSec settings. You wish to utilize the digital certificates that are available in the network. You decide that you wish for there to be maximum strength, and therefore you choose to implement IPSec using both AH and ESP.
First, you configure a custom policy for the servers in the network. To increase strength, you will implement your custom policy on top of the default Server IPSec Policy. You verify that the policy is running, and then you create a new policy. Your new policy will use SHA+3DES for AH and SHA for ESP. You make sure that the policy is to include all

IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the servers that you can and use secedit to force the others to refresh the two policies.
Next, with the help of the administrative staff, you will configure each client in the network. For the clients you also need the highest in security, so you will use a custom policy on the default policy. You verify that the default Client IPSec policy is enabled, and then you create a policy that uses SHA+3DES for AH and SHA for ESP. You make sure that the policy is to include all IP traffic, and for Authentication Method, you use the certificate that is assigned to each server. You reboot the client machines that you can and use secedit to force the others to refresh the two policies.
Answer: D

10.You had been taking a short vacation, and when you come into work on Monday morning, Blue is already at your door, waiting to talk to you.
"We've got a problem," Blue says, "It seems that the password used by our Vice President of Engineering has been compromised. Over the weekend, we found this account had logged into the network 25 times. The Vice President was not even in the office over the weekend."
"Did we get the source of the compromise yet?"
"No, but it won't surprise me if it is our new neighbors at MassiveCorp. I need to you to come up with a realistic plan and bring it to me tomorrow afternoon. This problem must be resolved, and like everything else we do not have unlimited funds - so keep that in mind."
Based on this information, choose the best solution to the password local authentication problem in the Executive building.}

A. Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Blue that includes the following points:
1. For all executives you recommend no longer using passwords, and instead migrating to a token-based authentication system.
2. You will install the RSA SecurID time-based token system.
3. You will create SecurID user records for each user to match their domain accounts.
4. You will assign each user record a unique token.
5. You will hand deliver the tokens to the correct executive.
6. Users will be allowed to create their own PIN, which will be 4 characters long.
7. The tokens will replace all passwords for authentication into each user's Windows system.
B. Since you are aware of the significance of the password problems, and since you do not have unlimited funds, you plan to address this problem through education and through awareness. You write up a plan for Blue that includes the following points:
1. All end users are to be trained on the methods of making strong passwords
2. All end users are instructed that they are to change their password at a minimum of every 30 days.

3. The administrative staff is to run password-checking utilities on all passwords every 30 days.
4. All end users are to be trained on the importance of never disclosing their password to any other individual.
5. All end users are to be trained on the importance of never writing down their passwords where they are clearly visible.
C. Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Blue that includes the following points:
1. You will reconfigure the Testbed. Certkiller .org domain to control the password problem.
2. You will configure AD in this domain so that complex password policies are required.
3. The complex password policies will include:
a. Password length of at least 8 characters
b. Passwords must be alphanumeric
c. Passwords must meet Gold Standard of complexity
d. Passwords must be changed every 30 days
e. Passwords cannot be reused
D. Since you are aware of the significance of the password problems, you plan to address the problem using technology. You write up a plan for Blue that includes the following points:
1. For all executives you recommend no longer using passwords, and instead migrating to a token-based authentication system.
2. You will install the RSA SecurID challenge-response token system.
3. You will create SecurID user records for each user to match their domain accounts.
4. You will assign each user record a unique token.
5. You will hand deliver the tokens to the correct executive.
6. Users will be required to use tokencodes from the One-Time tokencode list. The tokencodes will be alphanumeric and will be 4 characters long.
7. The tokens will replace all passwords for authentication into each user's Windows system.
E. Since you are aware of the significance of the password problems, plan to address the problem using technology. You write up a plan for Blue that includes the following points:
1. For all executives you recommend no longer using passwords, and instead migrating to a biometric solution.
2. You will install retinal scanners at every user's desktop in the executive building.
3. You will personally enroll each user at each desktop.
4. You will instruct each user on the proper positioning and use of the scanner.
5. The biometric system will replace all passwords for authentication into each user's Windows system.
Answer: A