Latest Version: 6

Question: 1

GlobalCorp is a company that makes state of the art aircraft for commercial and government use. Recently GlobalCorp has been working on the next generation of low orbit space vehicles, again for both commercial and governmental markets. GlobalCorphas corporate headquarters in Testbed, Nevada,
US
A. Testbed is a small town, with a population of less than 50,000 people. GlobalCorp 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 RD 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 GlobalCorp products. These offices also perform maintenance on the GlobalCorp aircraft and will
occasionally perform RD 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 GlobalCorp 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 intime for the annual meeting, and in the meantime you review the overview of the GlobalCorp network. Your first day in GlobalCorpTestbed, 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
anhour.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 GlobalCorp. "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, GlobalCorp 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." Blue responds, "I suggest trust. Not

withMassiveCorp, but in our own systems. We must build trusted networks. We must migrate our network from one that is well-defended to one that iswell-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 thenetwork. After some time, it is agreed upon that GlobalCorp will migrate to a trusted networking environment. The following week, Blue informs you that you will be workingdirectly together on the development of the planning and design of the trustednetwork. 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 GlobalCorp network is running Active Directory,with the domain structure as in the following list:

Testbed.globalcorp.org Newyork.globalcorp.org California.globalcorp.org Japan.globalcorp.org India.globalcorp.org England.globalcorp.org Although you will be working in the Testbed office, the plan you develop will need to include the entire GlobalCorp organization. Based on this information, select the solution that describes the best plan for the new trusted network of GlobalCorp:}

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.

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.

Design the hierarchy with each remote office and building having it's own enrollment CA.

Build a small test pilot program, to test the hierarchy, and integration with the existing network.

Implement the CA hierarchy in the executive office, and get all users acclimated to the system.

Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the

system. One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.

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 GlobalCorp trusted network.

B. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:

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.

Draft a CPF based on your own guidelines, including physical and technology controls.

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 C A, and every other building on the campus in Testbed will have a subordinate CA.

In the executive building, you design the system to be a mesh CA structure, with one CA per floor of the building.

Design the hierarchy with each remote office and building having it own enrollment CA.

Build a small test pilot program, to test the hierarchy, and integration with the existing network.
Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the
system.
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 GlobalCorp trusted network.
C. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
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.
Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component. 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.
Design the hierarchy with each remote office and building having it own enrollment CA.
Build a small test pilot program, to test the hierarchy, and integration with the existing network.
Implement the CA hierarchy in the executive office, and get all users acclimated to the system.
Implement the CA hierarchy in each other campus building in Testbed, and get all users acclimated to the
system.
One at a time, implement the CA hierarchy in each remote office; again getting all users acclimated to the system.
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 GlobalCorp trusted network.
D. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
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.
Draft a Certificate Practices Framework (CPF) document based on RFC 2527, including every primary component.
Design the system to be a full mesh, with the Root CA located in the executive building. 3.Design the system to be a full mesh, with the Root CA located in the executive building.
Design the mesh with each remote office and building having it own Root CA.
Build a small test pilot program, to test the hierarchy, and integration with the existing network.
Implement the CA mesh in the executive office, and get all users acclimated to the system.
Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the

system.
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 GlobalCorp trusted network.
E. You design the plan for two weeks, and then you present it to Blue. Your plan follows these critical steps:
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.
Draft a CPF based on your own guidelines, including physical and technology controls.
Design the system to be a full mesh, with the Root CA located in the executive building.
Design the mesh with each remote office and building having it own Root CA.
Build a small test pilot program, to test the hierarchy, and integration with the existing network.
Implement the CA mesh in the executive office, and get all users acclimated to the system.
Implement the CA mesh in each other campus building in Testbed, and get all users acclimated to the system.
One at a time, implement the CA mesh in each remote office; again getting all users acclimated to the system.
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 GlobalCorp trusted network.

Answer: C

Question: 2

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 otherbuildings. 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 GlobalCorp 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 thecomputer using Internet Explorer. Once themachine certificate is installed, the administrator has each user log on to their machine and the administrator walks the userthrough 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 thenew 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 canhelp. 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 account1.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 managementaccounts. For these accounts you utilize licensed PGPdigital certificates thatcan be used for both authentication and secure email. You personally show each manager how to create and usetheir 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 toperform 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 workingon, 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 thisyou 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

Question: 3

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 havetheir 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 stillhave vulnerability in our network traffic. The folks from MassiveCorp would love to have a sniffer running in here, I 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 ISA. 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 oneach tunnel, and you will use 3DES on one half of the tunnels and AES on the other half of the tunnels. You will be surethat each tunnel uses the same algorithm on bothends, but by using two algorithms you are sure that you haveincreased the security ofthe 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 usesecedit to force the others to refresh their policy. Next, with the help of the administrative staff, you will configure each client in thenetwork. 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 noneof 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 forAuthentication 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 thenetwork. 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 SHAfor 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

Question: 4

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're 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 thesource of the compromise yet?" "No, but it won't surprise me if it is our new neighbors atMassiveCorp. 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 inmind." 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 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.globalcorp.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 charactersa. b.Passwords must be alphanumericb. c.Passwords must meet Gold Standard of complexityc. d.Passwords must be changed every 30 daysd. e.Passwords cannot bereusede.
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 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 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 Windows system.

Answer: A