Apple Certified Specialist
Security and Mobility

NOTEBOOK

Apple Certified Specialist - Security and Mobility v10.6

Disclaimer

This notebook is intended for personal use only, it is a collection of questions and answers regarding the subjects concerning the ACS-SaM certification v10.6.

It has never been authorized by Apple or Editors of the Apple Training Series books and is not intended to substitute any official Apple resource suggested to obtain the ACS-SaM certification.

The following content is an unofficial (my personal) guide to acquire knowledge to pass the certification exam Snow 303, it may be inaccurate and may contain mistakes, it is just the result of my studies and was intended to help myself in memorizing the main concepts learned reading the official books part of the Apple Training Series.

Marco Massari Calderone

marco at marcomc dot com

Providing Network Services: DNS

Describe security vulnerabilities associated with the DNS service including: DNS cache poisoning, server mining, DNS service profiling, Denial of Service (DoS) and service piggybacking

1. DNS Cache Poisoning is the addition of false data to the DNS server's cache, which enables hackers to:
   - Redirect real domain name queries to alternative IP addresses (to collect bank account numbers, intercept email).
   - Prevent proper domain name resolution and access to the internet (it makes a DNS server appear to be malfunctioning).
2. Server mining is the practice of retrieving a copy of a complete zone by requesting a zone transfer.
   - The hacker can see which services a domain offers and the IP address of the servers that offer them.
   - The hacker can then try specific attacks based on these services (reconnaissance before another attack).
3. DNS Service Profiling is a reconnaissance technique:
   - An hacker makes a BIND version request.
   - The server reports which version of BIND is running.
   - The hacker then compares the response to known exploits and vulnerabilities for that version of BIND.
4. Denial of Service (DoS) attack prevents legitimate use of the service by overloading it.
   An hacker sends so many service requests and queries that a server uses all of its processing power and network bandwidth trying to respond.
5. Service Piggybacking is when a common Internet user configures its computer to query another DNS server instead of it s own ISP's DNS servers.

Given a properly formatted export of a DNS configuration file, import a primary zone for a give domain.

1. Update named.conf adding the zone definition to `/etc/named.conf` wrapped in a view.
2. Copy the zone file from the original system into the `/var/named` directory giving it the same name specified in the zone definition.
3. Restart named.
4. Issue the following two commands:
   - `$ serveradmin stop dns`
   - `$ serveradmin start dns`
   - Alternatively: `$ rndc -s 127.0.0.1 -p 54`

Given a properly configured primary zone and functional DNS services on Mac OS X Server create a secondary zone for the given domain on a separate installation of Mac OS X Server to establish high availability

1. Open Server Admin and select the server where the secondary zone will be configured.
2. Select the "DNS" service.
3. Click the 'Zone' button.
4. Click the 'Add Zone' button and choose 'Add Secondary Zone (Slave)'.
5. Specify the domain name and the IP address of the Primary DNS Servers.

Configure a primary zone to accept zone transfer requests from a specific secondary zone (whitelist)

Edit the `/etc/named.conf` file and add the following line:

```
Allow-transfer {192.168.11.22, ....}
```

To create a whitelist of IP address that are allowed to transfer the entire zone to themselves.

Verify forward and reverse lookup for a primary zone

1. Forward lookup: $ dig primary.dns.server
2. Reverse lookup: $ host <ip_address>

Define the term "DNS zone"

1. DNS zones are the basic organizational units of the DNS.
2. DNS zones contain records and are defined by the way they acquire those records and respond to DNS requests.

Configure a primary zone to forward requests not contained within its domain to a forward zone.

1. In Server Admin select the 'DNS' service.
2. Click the 'Settings' button.
3. Specify the IP address of an external DNS server in the 'Forwarder IP address' list.

Describe the types of DNS zones, including master, slave and forward

1. Master zone, has the master copy of the zone's records and provides authoritative answers to lookup requests.
2. Slave zone, this is a copy of a master zone stored on a slave or secondary name server that uses zone transfers to get copies of the master zone data.
3. Forward zone, redirects all lookup requests for that zone to other DNS servers.
   Does NOT do zone transfer.
   Used to provide DNS services to a private network behind a firewall.

Configure a DNS server to provide caching-only name services by clients internal to a company's intranet and refuse all external queries

1. In Server Admin select the DNS service of the chosen server.
2. DO NOT configure any zone.
3. Click the 'Settings' button.
4. Define 'localnets' and 'localhost' in the list 'Accept recursive queries from the following networks'.
5. Define an IP address in the list of 'Forwarder IP addresses'.

Configure a DNS server to provide authoritative-only name service (non-recursive only)

1. In Server Admin select the DNS service of the chosen server.
2. Set up zones.
3. Remove all recursion from the 'Settings' pane including 'localnets' and 'localhost'.

Update the root zone stored in /var/named/named.ca

```
$ dig . ns > /var/named/named.ca
```

Given Server Admin and a DNS zone hosted on a Mac OS X Server computer add mail exchange records to the zone

1. Select the chosen zone.
2. Add mail exchanges for the zone by clicking the add (+) button and entering the name in the 'Mail Exchange' field.

Configure the mail exchange record's priority

1. Lowest priority number means highest priority.
2. Delivering mail servers will first attempt to deliver mail to the server with the lowest priority number.

Given a properly formatted DNS configuration and a separate configuration file of unknown origin and content, troubleshoot a broken DNS config by comparing against a known-good config

1. The `/etc/named.conf` must be:

```
include “/etc/rndc.key”;
controls{
           inet 127.0.0.1 port 54 allow {any’}
           keys {“rndc-key”;};
     };
options {
           include “/etc/dns/options.conf.apple”;
     };
logging {
           include “/etc/dns/loggingOptions.conf.apple”;
     };
include “/etc/dns/publicView.conf.apple”;
```

2. `options.conf.apple` must contain:

```
directory “/var/named”;
forwarders {};
allow-transfers {none;};
```

3. `loggingOptions.conf.apple` consists of:

```
category default {
                      apple_sys.log;
                };
channel apple_syslog {
                           file “/Library/Logs/named.log”;
                           security info;
                           print-time yes;
                      };
```

4. `publicView.conf.apple` will be like:

```
acl “com.apple.ServerAdmin.DNS.public” {localnets; localhost;};
view “com.apple.ServerAdmin.DNS.public” {
     allow-recursion {“com.apple.ServerAdmin.DNS.public”;};
     zone “pretend.com” {
          Type master;
          file “db.pretend.com”;
          allow-transfer {none;};
          allow-update {none;};
     }
}
```

Define the records types in the DNS system: A, CNAME, MX, NS, PTR, TXT, SRV, HINFO

1. Address (A), is a machine record created for each machine entry added to a zone (AAAA for IPv6).
2. Canonical name (CNAME), stores the "real name" of a server when it's given a nickname or alias.
3. Mail eXchange (MX), stores the name of a computer used for a domain's email. You can have multiple records.
4. Name Server (NS), stores the authoritative name server for a zone.
5. Pointer (PTR), created automatically, maps an IP address to a computer's DNS name.
6. Text (TXT), stores a text string as a response to a DNS query.
7. Service (SRV), stores information about various services mapped to the proper IP address and resolved to their respective domain names.
8. Hardware Info (HINFO), stores information about a computer's hardware and software.

Explain the difference between a fully qualified domain name (FQDN) and a relative domain name

A FQDN is the full location of the specific machine that has that name and is fully reversible to its specific address.

A relative domain name is typically only the name of the specific machine without any other domain information.

Given the Lookup pane in Network Utility and a Mac OS X Server computer verify that the DNS service on the server is correctly resolving domain names and IP addresses

1. Enter an internet address (name or IP) to lookup.
2. Select the information to lookup.

List the address for the official BIND documentation

www.isc.org/software/bind/documentation

Describe the underlying configuration/directory file structure for DNS services

1. Database files are created in /var/named hierarchy.
2. Server Admin writes on Apple specific files but is also able to interpret canonical files.
3. Manual changes will update the canonical files, but this will stop Server Admin to manage BIND configurations. (/etc/named.conf).

Describe the impact of pre-existing DNS on initial server setup

If a DNS entry for the server was already present on the DNS server that you entered in the Network Interface setting, your server should have automatically pulled the host name and domain name.

Describe the purpose and benefit of DNS caching

1. Speed up the resolution of queries and caches responses.
2. DNS requests that go outside the local network that can negatively impact the performance of the internet connection are diminished.

Describe how DNS associates computer host names to IP addresses on a network

1. The DNS service associates computer host names with IP address through the configuration of machine records.
2. A hostname and IP address are assigned to each machine.

Describe the purposes of a DNS server including translating between domain names and IP address and acting as a cache and relay for translations provided by other DNS servers

1. Convert easy-to-remember names into a harder-to-remember numbers that computers require.
2. Reduce the response time for name resolution queries (cache and relay).
3. Support services that rely on a functioning DNS.

Describe how a DNS server uses a hierarchy of DNS servers to resolve a domain name that is not stored locally

If a local DNS server don't have the answer to a query it performs a recursive query to fetch the answer. A recursive query sends the query up the DNS hierarchy and allows other servers to perform the query on the initial server's behalf.

The response to the query ultimately passes back to the originating DNS server which caches it and passes it on to the client.

List the four steps necessary to configure a new DNS service for an organization including registering a domain name, creating DNS zones, adding DNS records to the zones and starting the DNS service

1. Register your domain name.
2. Create your DNS zones.
3. Add DNS records to your zones.
4. Start the service.

Providing Network Services: DHCP

Describe the security implications of deploying the DHCP service on Mac OS X Server 10.6 and strategies to mitigate the risks based on those implications

1. Assigning static IP addresses eases accountability and mitigates the risks posed by a rogue DHCP server.
2. Only one system should act as the DHCP server.
3. Configure the DHCP service to NOT distribute DNS, LDAP and WINS information.

Describe the function of the DHCP service in Mac OS X Server

1. The primary function of DHCP is the dynamic configuration of IP information on a host machine.
2. DHCP can also be used to provide other host configuration information (LDAP, DNS, WINS).

Identify the DHCP log messages that indicate a lease was acquired from Mac OS X Server by a DHCP client

When viewing the DHCP log entries you can determine whether a specific host has received a DHCP lease by looking for D.O.R.A.:

- Discover (DHCP DISCOVER)
- Offer (OFFER)
- Request (DHCP REQUEST)
- Acknowledge (ACK)

Given the server administration tools and system logs, isolate and resolve DHCP issues with a DHCP client or with the DHCP server on Mac OS X Server.

Look for messages marked 'bootpd'

List the four primary steps that occur when a client computer requests an address from a DHCP server

1. A DHCP client sends a discover message to look for DHCP servers.
2. A DHCP server responds to a client's DHCP DISCOVER message.
3. A DHCP client requests DHCP configuration information from the DHCP server.
4. A DHCP server responds with DHCP configuration information for the DHCP client.

Given server Admin configure the lease and renewal times for a DHCP subrange in the DHCP service

1. Select the DHCP service pane of the server hosting the service.
2. Click the 'Subnets' button.
3. Select the subnet from the list.
4. Define the 'Lease Time' in hours, days, weeks or months.

Given Server Admin, configure the DNS information that will be provided to a given subrange by the DHCP service.

1. Select the subnet from the list.
2. Click the 'DNS' tab.
3. Specify the DNS server and the Search Domains to be provided to the DHCP clients.

Given Server Admin connected to a Mac OS X Server, configure the IP addressing information that will be provided to a given subrange by the DHCP service.

1. Select the subnet from the list.
2. Click the 'General' tab.
3. Specify:
   - Subnet Name
   - Starting IP address
   - Ending IP address
   - Subnet Mask
   - Network Interface
   - Router
   - Lease Time

Given Server Admin, display a list of the current client computes on the DHCP service on a Mac OS X Server computer.

Click the 'Clients' button of the DHCP service on the selected service.

Configure the DHCP service to assign a specific IP address to a specific computer based on the computer's hardware (MAC) address

1. Click the 'Static Maps' of the DHCP service on the selected server.
2. Click the 'Add Computer' button.
3. Specify Computer Name, Mac Address and corresponding IP Addresses.

Identify whether a network port has received an IP address from a DHCP server or is using link-local address

You can identify whether a host has a DHCP address or a link-local address by looking at its address: al link-local addresses are in the range `169.254.xxx.xxx.` If a clients' IP is not in that range, the client does not have a link-local address.

Given Server Admin, configure the logging detail level for the DHCP service

1. Click the 'Settings' button of the DHCP service on the selected server.
2. Chose the 'Log Level' among:
   - Low (errors only)
   - Medium (errors and warnings)
   - High (all events)

Providing Network Services: NAT/Gateway

Describe the security implications of deploying the NAT service on Mac OS X Server 10.6 and strategies to mitigate the risks based on those implications.

1. Communication from a public network cannot come into your private network unless it is requested.
2. Traffic that originates from the internet does not reach computers behind the NAT service unless port forwarding is enabled.
3. To mitigate the risks introduced by port forwarding is useful to properly configure the firewall application.

Describe how port forwarding is configured for and implemented by NAT service on Mac OS X Server 10.6

1. Port forwarding works by using port-to-service relationships created by editing the `/etc/nat/natd.plist`.
2. The content of natd.plist will be used to generate `/etc/nat/natd.conf` apple which is passed to the `natd` daemon when it starts.

Define the terms "static NAT" and "Port Address Translation"

1. Static NAT maps a private IP address to a public IP address (one-to-one mapping).
2. Dynamic NAT maps a private IP address to the first available address from a list of public IP addresses.
3. Port Address Translation (PAT) maps multiple private IP addresses to a single public IP address by using different ports.
   It's also known as port overloading, single-address NAT, port-level multiplexed NAT.

Given Server Admin, configure Mac OS X Server to provide multiple computers on a private LAN access to the internet using a single assigned public IP address.

1. Configure DHCP to distribute IP in the range you prefer and to distribute DNS configuration.
2. Configure DNS as a caching server.
3. Configure the Firewall service to stop all traffic coming from the internet.
4. Configure the NAT to allow machines in the internal network to share the internet connection of the server:
   - in the NAT Settings:
     1. Select "IP Forwarding and Network Address Translation (NAT)".
     2. Select the "External network interface".
     3. Enable port mapping protocol.
   - Alternatively use the Gateway Setup Assistant from the "Overview" button of the NAT service.

Describe how an outbound NAT connection works on Mac OS X 10.6

1. A computer requests a page on the internet.
   The request goes to the default router address which is the address of the internal ethernet interface of the server running NAT.
2. This outbound request is redirected to natd (the NAT daemon) by the divert rule in the firewall configuration (any-to-any on port 8668).

   In an internal table, natd notes the IP address of the computer that send this request and adds an internal port number xxxxx to identify the table entry applying to this request.

   Then the natd sends the request back to the firewall service and forward the request to the appropriate host on the internet using the address of the external interface of the server which is connected to the internet, as the new source.
   Also the natd port number is added to the external IP address.
3. The web service on the internet receives a request for a page and return the page requested.
   The service returns the page to the requesting address at port xxxxx.
4. The server receives the response page and the firewall forwards the response to natd for processing.
   Packets that are received with a target IP of the server are checked against the internal table. If an entry is found it is used to determine the correct target IP address and port of the host on the private network.

Given a Mac OS X Server computer configured to act as a gateway between two networks, configure the NAT service to port forwarding incoming IP traffic to computers based upon the IP port of the incoming traffic.

1. In the 'Settings' of the NAT service select 'Enable Port Mapping Protocol'
2. In the Terminal with a text editor edit `/etc/nat/natd.plist` to set the port forwarding.
3. Restart the NAT service:
   1. `$ sudo serveradmin stop nat`
   2. `$ sudo serveradmin start nat`

Describe the relationship between IP ports and services in an IP host

1. Each service is associated with one or more specific IP ports.
2. In a NAT/Gateway is possible to activate Port Forwarding in the way to redirect all traffic incoming to a specific port to a specific host situated in the private LAN, running the requested service.

Define the term 'Port Forwarding' as implemented in Mac OS X Server

Port Forwarding allows you to provide external users with access to services o the private LAN by using port-to-service relationship created by editing the /etc/nat/natd.plist file.

Given a Mac OS X Server computer configured as a gateway server, troubleshoot a situation where a computer on the private network is unable to access services on the public network.

1. Verify that the NAT service is running:
   ```
   $ sudo serveradmin <status | fullstatus> nat
   ```
2. Check the ethernet cabling and infrastructure.
3. Check the ethernet interface configuration.
4. Check the NAT service configuration.
5. Verify the Firewall service configuration:
   - Go to the 'Services' tab of the Firewall 'Settings'.
   - Temporarily set 'Editing services for' to 'any' and 'Allow all Traffic', verify if is the firewall preventing the computer to access the public servers.

Given a properly configured primary zone, functional DNS services and NAT services on Mac OS X Server, create name spaces behind a NAT gateway

1. Run DNS services behind the gateway assigning names to NAT IP address.
2. Names entered by users outside the gateway won't resolve the address behind it.
3. Set the DNS records outside the NAT-routed area to point to the NAT gateway and use NAT port forwarding to access computers behind the NAT gateway.

Security Systems and Services: Firewalls

Describe security considerations related to deploying the Firewall service on Mac OS X

1. The greatest number of reported data breaches come from within corporate networks.
2. Network-level firewalls will block unauthorized traffic trying to enter your network they will not block traffic that is originated inside your network.
3. Mobile computers frequently join new wired or wireless networks with different firewalls rules or no firewall protection at all.
4. To protect against unauthorized network access to your Mac (from within the LAN), you can enable the Application Firewall via System Preferences that allows connections base on application and service needs without requiring the use or administrator to know the ports used.
5. Enable sharing service only as required to limit the opened ports on the firewall.
6. Turn off sharing services, enable the Firewall's Stealth Mode when traveling to provide the additional blocking required when access insecure public networks.
7. When planning server installation refer to the planning documents provided by Apple: http://images.apple.com/server/macosx/docs/Worksheet_v10.6.pdf
8. Open firewall ports only for services provided to resources and individuals outside your local network.
9. Utilize address groups to limit allowed access to specific IP address or address ranges whenever possible.
10. Review your firewall logs on regular basis: note penetration (denied) attempts from the same or similar IP address ranges and consider blocking the entire range.
11. Be extremely wary of providing SMB access through the firewall.
    Many exploit uses SMB ports that are also a common vehicle for virus programmers.
12. Open only required ports, not ranges of ports.
13. Use tools such Nagios and Snort for threat analysis and detection.
14. Less is More: the less access you provide to the outside the more secure you make your internal network.

Explain the purpose of Stealth Mode in the Firewall service on a Mac OS X Server computer

Stealth options drop denied packets rather tan sending the requesting computer an error message, which makes the job for attackers much more difficult as probing attacks and open port discovery are thwarted.

Explain how to enable Stealth Mode for TCP or UDP packets in the firewall service on a Mac OS X Server computer

You find the stealth options in the Server Admin Settings pane under the Advanced tab.

Describe the architecture and configuration options of the Firewall service in Mac OS X Server

1. Mac OS X Server contains a host-based firewall service based on `ipfw` software that offers stateful and stateless packet firewall.
2. It also contains an Adaptive Firewall that dynamically creates and disable rules in `ipfw` firewall as needed; it is enabled by default.
3. You can create address group to handle network addresses to which you can apply rules.

Given the Server Admin application, configure firewall logs in Mac OS X Server 10.6

1. Logs are written in /var/log/ipfw.log
2. You can fine-tune logging from the Server Admin graphical user interface in the Logging tab of the Firewall Settings.
3. You can also issue tuning commands like:
   ```
   $ serveradmin settings ipfilter:log.AllAllowed:yes
   ```

Explain the function of the adaptive firewall in Mac OS X

The adaptive Firewall is really a monitor that dynamically creates and disables rules in the ipfw firewall as needed.

The adaptive firewall is called in action following ten failed login attempts. Such behavior blocks the requesting IP address for 15 minutes which makes brute-force password attacks virtually impossible.

Given a misconfigured service configuration and a valid network connection troubleshot an ipfw configuration

1. With Server Admin in the Firewall Settings, verify that the address groups reflect your network settings.
2. Use ping to verify that you are able to reach the server through it's IP address:
   $ ping <ip address>
3. Use telnet to verify that you're able to connect to a specific service at it's IP port:
   $ telnet <ip address> <ip port>
4. Examine the Firewall Log with Server Admin filtering for 'DENY' messages.
5. Use a packet sniffer such tcpdump from inside the sever to visualize which traffic is passing through the physical interface for a specific service:
   $ tcpdump -i en0 host <ip address> pro 'n' -s0 -w server_trace_pcap

In a worst-case scenario you can document and backup the current firewall rule set and then flush the current rules entirely. Then you can add half of the rules back in at a time, starting the firewall service each time that you introduce a new set of rules.

Incrementally adding back rules makes it easier to determine which rule is causing the undesired behavior.

Display the application firewall log

It's placed in /var/log/afl.log

Given Server Admin create an address group to allow a Firewall service to control network access to computers using the given address

1. Go to the Address Group tabs of the Firewall's Settings.
2. Click the 'add' button and specify a Group name and the Address (or range) in the group.

Configure the Firewall service to simply drop denied packets rather than sending a failure notification to the requesting computer

Enable the Stealth Mode for UDP and TCP packets in the Advanced pane of the Firewall's Settings with the Server Admin application.

Security Systems and Services: VPN

List the two encrypted transport protocol supported by the VPN service on Mac OS X Server

1. PPTP: Point-to-Point Tunneling Protocol.
   Uses PPP dial-up protocol and MS-CHAP for authentication.
   Supports PKI certificates via EAP-TLS (works on Transport Layer of OSI model).
   Works easily with most NAT firewall.
   Little overhead, fast and scalable.

2. L2TP: Layer 2 Tunneling Protocol.
   Uses PPP for communication and IPSec for encryption.
   Not much scalable do to intense encryption calculations.
   Works on Data Link layer of OSI model (able to traverse frame relay, ATM and the non-TCP/IP based networks).
   Provides for data integrity.

List the three authentication options available for the Mac OS X Server L2TP VPN Service

1. PPP Authentication:
   - Directory Service:
     (1) MS-CHAP
     (2) Kerberos
   - RADIUS
2. IPSec Authentication:
   - Shared Secret
   - Certificate

List the two authentication options available for Mac OS X Server PPTP VPN Service

1. PPP Authentication:
   - Directory Service:
     (1) MS-CHAP
     (2) Kerberos
   - RADIUS

Configure the server's VPN service to provide valid IP addresses and require server authentication

1. Open Server Admin and click the 'Settings' button of the VPN service.
2. Choose a transport protocol among PPTP and L2TP tabs.
3. Define the range of IP addresses to assign to VPN clients (it must be contiguous and not conflicting with the running DHCP service addresses).
4. Define the authentication method.

State the requirements for establishing IP addresses for VPN services on Mac OS X Server 10.6

DHCP service should exclude these addresses to avoid accidental issuance of VPN IP addresses to internal network client equipment.

Identify the location of the VPN service log file on a Mac OS X Server computer

`/var/log/ppp/vpn.log`

Identify the locations of the VPN log files on a Mac OS X computer

`/var/log/ppp.log`

Compare and contrast authentication mechanisms that can be used with Mac OS X Server's VPN service for both users and devices

1. Password allows users to save the user authentication password. Not recommended.
2. RSA Secure ID. RSA provides a onetime password device called Secure ID to provide two-factor authentication. Requires an RSA server at the host location to authenticate the generated onetime password on the device.
3. Certificate: PKI certificates can be issued to devices and installed into their keychains to provide machine-based authentication.
4. Kerberos: the VPN client can utilize Kerberos for secured single sign-on access to the VPN host.
5. CryptCard: provides a onetime password device offering two-factor authentication.
6. Shared Secret (L2TP and Cisco IPSec only): used for device-based authentication to the VPN. The secret is separated and distinct from the secret's password and is used for device validation, not user authentication.

State the requirements for integrating firewall services with VPN services on Mac OS X Server 10.6

Ensure that the appropriate ports are open on the firewall to allow communication from the Internet to the VPN server:

1. Ports 500, 1701 and 4500 UDP for L2TP.
2. Port 1723 TCP for PPTP.

Describe the features, architecture and options of the VPN service in Mac OS X Server 10.6

1. Mac OS X Server 10.6 can provide L2TP and PPTP VPN services simultaneously or individually.
2. Can leverage the Remote Authentication Dial-Up Service (RADIUS) on your Mac OS X Server or an external server to provide user authentication.
3. L2TP VPNs can be load-balances among multiple servers.
4. L2TP can provide client machine certificate authentication.
5. It's possible to specify DNS servers, network routers, and search domains provided to connect VPN clients.
6. Verbose logging is activable to support troubleshooting.

Describe the features and options of the VPN client in Mac OS X 10.6

1. VPN on-demand option which establish a predefines VPN connection whenever the user attempts to access resources in a specified domain.
2. Ability to disconnect on logout, switching users.
3. Ability to force all traffic across the VPN.
4. Ability to specify proxy and DNS servers on connection.

Describe the features and options of the VPN client in iPhone OS

1. iPhone OS supports VPN connections over WiFi and cellphone networks using L2TP, PPTP and Cisco IPSec connections.
2. iPhone OS supports multiple VPN connection settings, allowing users to connect to more than one VPN but NOT simultaneously.

Describe how 'ssh' tool in Mac OS X Server 10.6 can be used to tunnel unencrypted traffic over a network through an encrypted SSH channel

The SSH client will forward a specified local port to a port on the remote server. After the SSH tunnel is established, you can connect to a specified local port to access the network service.

Given two computers running Mac O S X Server 10.6 and a functional network connection between them, configure SSH tunnel between the two computers

```
$ ssh - L 2525:remote.server.com:25 username@remote.server.com
```

Security Systems and Services: Keys and Certificates

Describe how 802.1x is implemented on Mac OS X, Mac OS X Server and iPhone OS

1. Mac OS X Server provides an Open Directory integrated RADIUS server to provide 802.1x authentication to AirPort Express, Airport Extreme and other standards-based wired and wireless access points.
2. Mac OS X's supplicant provides four modes of operating:
    1. User mode
    2. System mode
    3. Login Window mode
    4. Mixed mode: System mode/Login Window mode
3. iPhone OS provides System Mode capability because no login window exists.
   It uses profile templates created with the iPhone Profile Configuration Utility (iPCU) or can be manually configured.

Describe the features and function of 802.1x as a Network access control mechanism

1. Offers means of restricting network access to authorized users and devices while leveraging existing authentication mechanism like Open directory, RADIUS, Active Directory and certificates.
2. Can be deployed on wired and wireless networks.
3. Eliminate unauthenticated access to the actual network.
4. Prevents hubbing: stops users to connect an unauthorized network hub or switch to a single authorized port to add devices to the network.
5. May provide dynamic Virtual LAN: the user is placed in a holding network.
   After being authenticated the user is assigned to a specific virtual LAN based on group membership in a directory or RADIUS server.
6. The authentication process requires that the client system have a service or software called 'supplicant' used for negotiation and authentication.

Define the term 'certificate'

A certificate is defined as an electronic document or file that identifies the owner of the certificate's PKI and organizational information.

Given a default installation of Mac OS X and Mac OS X Server and a functioning network connection between them, configure Mac OS X to connect to Mac OS X Server using 802.1x

1. In the Mac OS X computer open System Preferences.
2. Select the AirPort network device, turn it on.
3. Click the 'Advanced' button and select the 802.1x' tab.
4. From the pop-up menu choose 'System Profile'.
5. Leave 'username' and 'password' fields empty.
6. Select 'TLS' as authentication method.
7. Click 'configure Trust' and the certificate provided for the server.
8. In the Wireless Network field enter the SSID of the wireless network and choose the Security Type.
9. In the 'System Profile' pane add a 'Login Window' preference.
10. Leave 'username' and 'password' empty and in the authentication area select TTLS and PEAP check boxes.
11. In the 'Wireless Network' field enter the SSID of the wireless network.

Given a device running iPhone OS and Mac OS X Server a functioning network connection between them, configure the iPhone OS device to connect to a Mac OS X Server using 802.1x

1. Open the iPhone Configuration Utility.
2. Select 'Configuration Profiles', click 'File > New configuration Profile' from the menu.
3. Select the 'Wi-Fi' tab and click 'Configure'.
4. Specify the SSID of the wireless network.
5. Select 'WPA/WPA2 Enterprise' from the security pop-up menu.
6. Specify the EAP type supported.
7. Save the configuration and deploy it to the iPhone OS device.

Given a default installation of Mac OS X Server 10.6, a default installation of Mac OS X 10.6 with an expired key/certificate from the server and a functional network connection between the server and client, troubleshoot the source and cause of the expired key/certificate, and then generate a new key/certificate to replace the expired key/certificate.

1. Request a new certificate from the CA, or if you are your own CA, create one using your root certificate.
2. Select the server with the expired certificate in Server Admin.
3. Click the 'Certificate' button.
4. Select the expired certificate and click the action button choosing "Replace Certificate with Signed or Renewed Certificate".
5. Drag the renewed certificate to the sheet.
6. Click 'Replace Certificate'.

Describe the purpose and operation of keys and certificates as utilized in Mac OS X 10.6's implementation of the Public Key Infrastructure (PKI)

1. Within PKI public and private keys are created so that keys are mathematically linked: data encrypted with one key can be decrypted only by the other key and vice versa.
2. The public key can and should be distributed by the other communicating parties. However the private key remains private to the owner, is not for distribution, and is often encrypted by a passphrase.
3. Public key can:
   - Verify the signature on a message that originates from a private key.
   - Encrypt messages so that only the holder of the corresponding private key can decrypt them.
4. Private key can:
   - Digitally sign a message or certificate indicating authenticity.
   - Decrypt messages that were encrypted with the corresponding public key.
5. Public keys are often contained in certificates.
6. Mac OS X utilizes the x.509 certificate standard for public key certificates (identity certificates). It contains:
   - The public key half of a public-private key pair.
   - The key user's identity information (username, contact info).
   - A validity period that specifies how long the certificate can be trusted as accurate.
   - The URL of someone with the power to revoke the certificate (its revocation center).
   - The digital signature of a CA or the key user.

Configure an SSH key pair between a client and a server machines so that an SSH connection can be made between them.

Key must be generated for each user account:

1. In the Terminal application on the client computer create the '.ssh' folder in the user's home folder if it doesn't exists yet.
2. Change directory to '`~/.ssh`'.
3. Generate the public and private key by entering:
   ```
   $ ssh-keygen -b 1024 -t rsa -f id_rsa -P''
   ```
   (the null private key password allows for automated SSH connections)
4. Copy the public key into the authorized keys file:
   ```
   $ cat id_rsa.pub >> authorized_keys
   ```
5. Change the permissions of the private key so that only the owner can change the file:
   ```
   $ chmod go-rwx ~/.ssh/.id_rsa
   ```
6. Copy the public key and the authorized key list to the specified user's home folder in the remote computer (server):
   ```
   $ scp. authorized_keys user@remoteserver:~/.ssh/
   ```
7. To establish two-way communication between servers, repeat he process on the second computer.

Given an installation of Mac OS X Server 10.6 with a valid certificate from a trusted certificate authority (CA), view the certificate and determine the granting certificate authority.

1. Open Server Admin and select the server where the certificate is installed.
2. Click the 'Certificates' button.
3. Select the certificate for the list and individuate the 'Issuer Name' section of the 'Details' that determine the CA who signed the certificate.

Given a default installation of Mac OS X Server 10.6, display the built-in certificate(s)

1. Open the Keychain Access application.
2. Select the System Roots from the keychains list to visualize the list of built-in certificates.

Given an installation of Mac OS X Server 10.6 with a certificate issued by a certificate authority (CA) determine whether the computer trusts the certificate authority that issued the certificate

1. From the list of certificates select the certificate.
2. Verify the text by the certificate's name if the certificate is not trusted a small red 'x' will appear showing "this root certificate is not trusted".

Explain how trust of a certificate is granted

A user applies to the Certificate Authority for a certificate by providing identity and contact information, as well as the public key.

The CA must check an applicant's identity so users can trust that the certificates it issues actually belongs to the identified applicant.

Given a default installation of a Mac OS X Server 10.6, create a certificate signing request (CSR)

1. Open Server Admin and select the server you are requesting a certificate for.
2. Click 'Certificates' button.
3. Click the certificate you want to have signed.
   Its DNS name must match the DNS name the client applications will use to engage the service or application.
4. Click the 'Action' button and choose 'Generate Certificate Signing Request (CSR)'.
5. Save the CSR request file.
6. Follow your CA's directions for uploading and transmitting the request to be signed.

Given a default installation of Mac OS X Server 10.6 create a self-signed certificate

1. In Server Admin select the server with services that support SSL an click the 'Certificates' button.
2. Click the Add ('+') button and choose "Create a Certificate Identity" to open Certificate Assistant.
3. Choose to "Override defaults" and follow the onscreen instructions.

Certificate Assistant generates a key pair and a certificate.
It encrypts the files with a random passphrase, puts the passphrase in the system keychain and saves the resulting PEM files in `/etc/certificates/`.

List the services capable of using certificates in Mac OS X Server 10.6

1. Server administration using Server Admin and Server Preferences
2. Users and groups management using Workgroup Manager
3. Address Book service
4. iCal service
5. iChat service
6. Mail service
7. Open Directory
8. Podcast Producer
9. RADIUS service
10. SSH
11. VPN on L2TP
12. Web service

Given an installation of Mac OS X Server 10.6 with a certificate issued by a Certificate Authority, validate the certificate using the appropriate tool

1. `$ security verify-cert -c certificate.cer -p ssl -s certificate.com`
2. `$ security verify-cert -c certificate.crt`

Describe the function of the Certificate Authority as it applies to the PKI

The CA signs and issues digital identity certificates claiming trust of the identified party. It is a trusted party between two transactions.

Working with Mobile Devices: Providing iPhone Applications

Given access to the iPhone SDK and a Mac OS X system, install the SDK so that the primary development tool can be used to create iPhone apps
The SDK installs by default in the Developer directory at the root level of your boot drive.

State which iPhone SDK utilities are used to create an iPhone web application.
Dashcode

State which iPhone SDK utilities are used to create an iPhone native application

1. Xcode
2. Interface Builder

State how a developer gain access to the iPhone SDK
They must participate at the iPhone Developer Program.

State what is required by a developer in order to install a native application on an iPhone
You need to create or obtain the following digital assets:

1. Certificate Signing Request, to be submitted through the iPhone Developer Program Portal (visible only to members of the iPhone developer Program.
2. Developer Certificate, obtained from the portal, to be installed in your keychain.
3. Provisional Profile, associate one or more development certificates, devices and an iPhone application ID. To be installed on your device.

State the option for deploying a native iPhone application within an organization

1. Publish the application in the App Store (will be available to the World).
2. Distribute the application for manual installation via iTunes.

Explain what a provisioning profile is
A provisioning profile associates one or more development certificates, devices and an iPhone application ID.

Compare the benefits of deploying an iPhone web application compared to a native iPhone application

1. The benefits of a web application as opposed to a native application include ease of deployment, the use of existing knowledge and the use of existing tools (Dashcode).
2. The benefits of deploying a native application as opposed to a web application include its availability anytime and anywhere as well its potential to generate revenue from iTunes App Store distribution.

Explain how to install a provisioning profile

1. Drag the provisioning profile file into iTunes.
2. Or use the iPhone Configuration utility.

State which utility is used to distribute and manage iPhone configuration profiles

iPhone Configuration Utility

Explain how to use the iPhone Configuration Utility to create a configuration profile

A profile consists of payloads that represent individual collection of specific settings types within the configuration profile.

To create a new configuration profile:

1. Click the 'New' button in the toolbar of iPhone Configuration Utility.
2. You add payloads using the payloads list.
3. Edit the payloads by entering and selecting options that appear in the editing pane. Required fields are marked with a red arrow.

Explain how to distribute and install a configuration profile on an iPhone

1. Via email: clicking 'Share' from the iPhone Configuration Utility.
2. Via web: clicking 'Export' from the iPhone Configuration Utility and saving it in a location accessible browsing your website.
3. Installing it directly through iPhone Configuration Utility connecting the iPhone.

When sharing or exporting the configuration is possible to choose to sign and encrypt the profile file.

Explain where to get the iPhone Configuration Utility

`www.apple.com/support/iPhone/enterprise`

Working with Mobile Devices: Mobile Access Server

Explain the function of the Mobile Access Service on Mac OS X

M.A.S. Provides a secure method for sharing internal resources with external clients by enabling access to IMAP, SMTP and HTTP protocols and CalDAV, all behind a corporate firewall and without the need for VPN.

Explain the benefits of using Mobile Access Service as compared to VPN

1. There's no need to open ports in the firewall to allow connection to specific LAN servers.
2. MAS is more secure than VPN because MAS allows access only to specific services not to the entire LAN.
3. MAS does not host any sensitive data, which makes it less vulnerable to exploits.
4. MAS limit which users authenticate and which services authenticated users can access.
5. MAS utilizes Secure Socket Layer (SSL) to hide sensitive data over the Internet.

List the services to which the Mobile Access Service provides proxy access

1. Mail
2. iCal
3. Address Book
4. Web services hosted on various origin servers
5. Wikis hosted on Mac OS X Server 10.6

Explain how MAS server, start and stop the Mobile Access Service

1. `$ sudo serveradmin stop proxy`
2. `$ sudo serveradmin start proxy`

Compare and contrast the two methods for using certificates with proxied services

1. Create a separate certificate for each host name: prior to Mac OS X 10.6.2 with SNI support (Server Name Indication), if more than one web server was on the intranet, MAS did not know which server should receive that request, you'll have a conflict between the host header and the SSL certificate used to encrypt the traffic.
2. Create a single wild card certificate that all SSL-enabled services can share.

List the client OS requirements to allow a client computer to access services on a private network via the Mobile Access Service

To use MAS, the client only needs to have appropriate client software like CalDAV client, mail client, and any modern web browser.

Give Server Admin and Mobile Access Server, display the Mobile Access Service

1. Click the 'Logs' button in the 'Mobile Access' service of Server Admin.
2. Server Admin shows you the following service logs displaying the information related to the mobile Access Service only:
   - Address Book Access log
   - Calendar Access log
   - Mail Access log
   - Mail Error log
   - Web Access log
   - Web Error log

Given Server Admin and Mobile Access server, display the status of the Mobile Access Service including which proxy service are running and the number of requests made on each proxy service

The 'Overview' pane displays detailed information on the proxies currently running on the server and the internal servers with which those proxies are associated.