CHAPTER 9

Management

The primary goal of the management module is to facilitate the secure management of all devices and hosts within the enterprise network architecture. The management module is key for any network security management and reporting strategy. It provides the servers, services, and connectivity needed for the following:

- Device access and configuration
- Event collection for monitoring, analysis, and correlation
- Device and user authentication, authorization, and accounting
- Device time synchronization
- Configuration and image repository
- Network access control manager and profilers

Logging and reporting information flows from the network devices to the management hosts, while content, configurations, and new software updates flow to the devices from the management hosts.

Key devices that exist in the Management Module relevant for security include the following:

- CS-MARS—Event Monitoring, Analysis, and Correlation (EMAC) system that provides network-wide security intelligence and collaboration allowing quick identification and rapid reaction to threats. CS-MARS collects, trends, and correlates logging and event information generated by routers, switches, firewalls, intrusion prevention systems, Cisco Access Control Servers (ACS) and the management center for Cisco Security Agents (CSA-MC). CS-MARS collects network configuration and event information using protocols like syslog, SNMP, Telnet, SSH, and NetFlow. In addition, CS-MARS integrates with Cisco Security Manager (CSM) to provide a comprehensive security monitoring and management solution that addresses configuration management, security monitoring, analysis, and mitigation.
- Cisco Security Manager (CSM)—Management application used to configure firewall, VPN, and intrusion prevention services on Cisco network and security devices. CSM communicates with Cisco network and security devices using telnet, SSH, HTTP, or HTTPs.
- Network Access Control (NAC) Manager—Communicates with and manages the Cisco NAC Server. Provides a web-based interface for creating security policies, managing online users, and acts as an authentication proxy for authentication servers on the backend such as ACS.
- Access Control Server (ACS)—Provides Authentication, Authorization, and Accounting (AAA) services for routers, switches, firewalls, VPN services, and NAC clients. In addition, ACS also interfaces with external backend Active Directory and LDAP authentication services.
- System administration host—Provides configuration, software images, and content changes on devices from a central server.

- Configuration and software archive host—Provides repository for device configuration and system image backup files.
- Network Time Protocol (NTP) server—Used for time synchronization.
- Firewall/VPN—Provides granular access control for traffic flows between the management hosts and the managed devices for in-band management. Firewall also provides secure VPN access to the management module for administrators located at the campus, branches and other places in the network.

Note The best practices for enabling secure administrative access with protocols like SSH and SNMP are provided in Chapter 2, "Network Foundation Protection." Chapter 10, "Monitoring, Analysis, and Correlation" describes the best practices for the secure configuration of device access and reporting access required by CS-MARS.

Note The NAC Profiler server is typically deployed in the management module alongside the NAC Manager. However, if NAT is being performed on the firewall protecting the management module from the data network, then the NAC Profiler server needs to be located outside the management module such that there is no NAT between the NAC server (acting as the collector) and NAC Profiler. For more information, refer to the "NAC Appliance" section on page 5-33 and "NAC Profiler" section on page 5-45.

Key Threats in the Management Module

The following are some of the expected threat vectors affecting the management module:

- Unauthorized Access
- Denial-of-Service (DoS)
- Distributed DoS (DDoS)
- Man-in-the-Middle (MITM) Attacks
- Privilege escalation
- Intrusions
- Network reconnaissance
- Password attacks
- IP spoofing

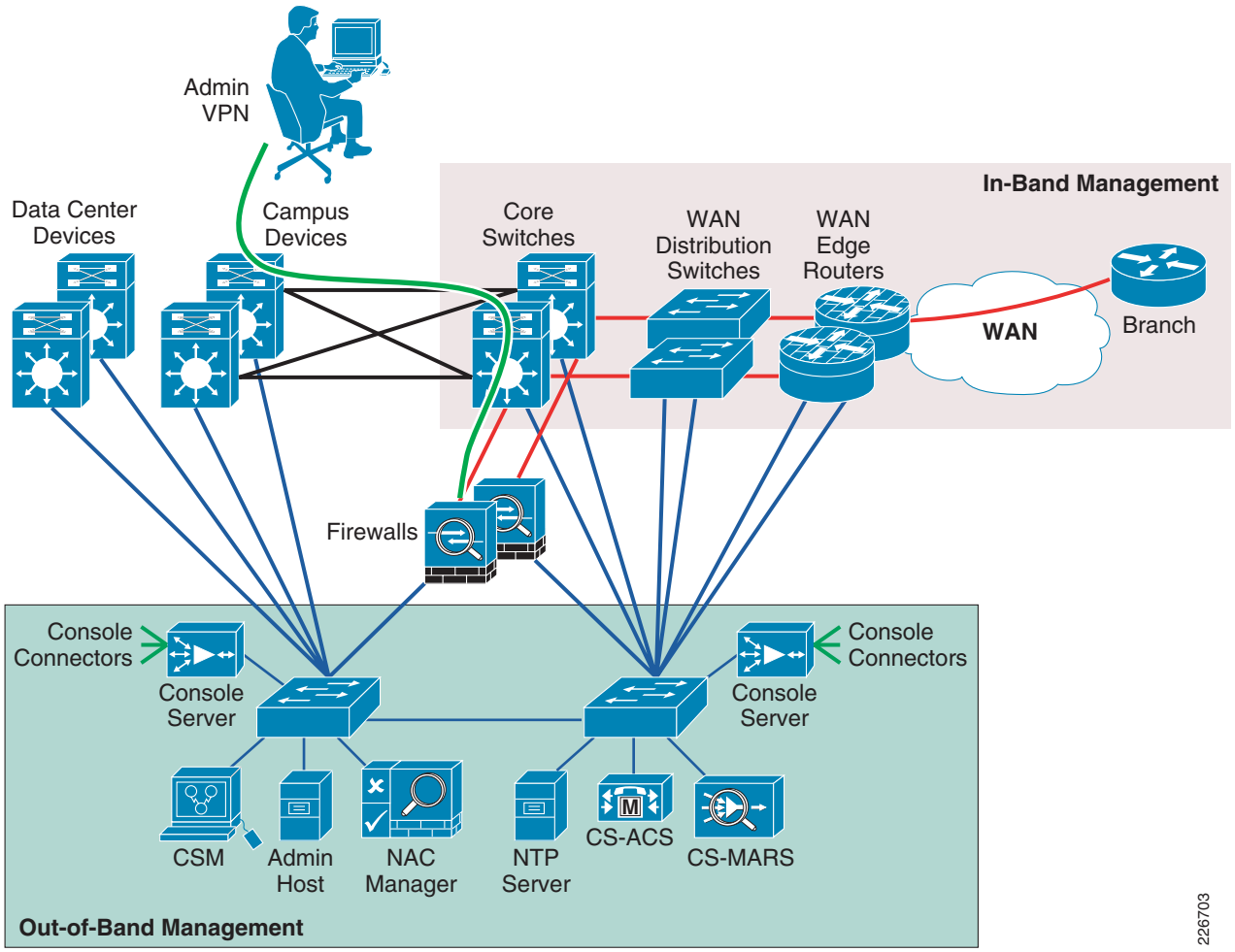
Management Module Deployment Best Practices

The SAFE architecture design includes a management network module dedicated to carrying control and management plane traffic such as NTP, SSH, SNMP, VPN, TACACS+, syslog, and NetFlow reporting. The management module provides configuration management for nearly all devices in the network through the use of two primary technologies: Cisco IOS routers acting as terminal servers and a dedicated management network segment implemented either on separated hardware or VLANs. The dedicated management network segment provides the primary method for managing network devices using secure transport protocols such as SSH and HTTPS. Hardened terminal servers provide backup console and CLI access to the network devices using the reverse-telnet function.

Because the management network has administrative access to nearly every area of the network, it can be a very attractive target to hackers. The management module is built with several technologies designed to mitigate those risks. The first primary threat is a hacker attempting to gain access to the management network itself. This threat can only be mitigated through the effective deployment of security features in the other modules in the enterprise to ensure the proper security is in place to prevent unauthorized access to services within the management module. The remaining threats assume that the primary line-of-defense has been breached. To mitigate the threat of a compromised device, access control should be implemented using a firewall, and every device should be hardened and secured using the baseline security best practices outlined in Chapter 2, “Network Foundation Protection.”

The management network combines out-of-band (OOB) management and in-band (IB) management access to manage the various devices within the different PIN modules. OOB management is used for devices at the headquarters and is accomplished by connecting dedicated management ports or spare Ethernet ports on devices directly to the dedicated OOB management network hosting the management and monitoring applications and services. The OOB management network can be either implemented as a collection of dedicated hardware or based on VLAN isolation. IB management is used for remote devices such as the branch site and access is provided through the data path using a firewalled connection to the core network module. This connectivity is depicted in Figure 9-1.

Figure 9-1 Out-of-band and In-band Management Design



When deploying a management network some of the key components of the design include the following:

- Securing the out-of-band Management network
- Securing the in-band Management access
- Providing secure remote access to the management network
- Synchronizing time using NTP
- Securing servers and other endpoint with endpoint protection software and operating system (OS) hardening best practices
- Hardening the infrastructure using Network Foundation Protection (NFP) best practices

The following section will discuss each of these components.

OOB Management Best Practices

The OOB network segment hosts console servers, network management stations, AAA servers, analysis and correlation tools, NTP, FTP, syslog servers, network compliance management, and any other management and control services. A single OOB management network may serve all the enterprise network modules located at the headquarters. An OOB management network should be deployed using the following best practices:

- Provide network isolation
- Enforce access control
- Prevent data traffic from transiting the management network

The OOB management network is implemented at the headquarters using dedicated switches that are independent and physically disparate from the data network. The OOB management may also be logically implemented with isolated and segregated VLANs. Routers, switches, firewalls, IPS, and other network devices connect to the OOB network through dedicated management interfaces. The management subnet should operate under an address space that is completely separate from the rest of the production data network. This facilitates the enforcement of controls, such as making sure the management network is not advertised by any routing protocols. This also enables the production network devices to block any traffic from the management subnets that appears on the production network links.

Devices being managed by the OOB management network at the headquarters connect to the management network using a dedicated management interface or a spare Ethernet interface configured as a management interface. The interface connecting to the management network should be a routing protocol passive-interface and the IP address assigned to the interface should not be advertised in the internal routing protocol used for the data network. Access-lists using inbound and outbound access-groups are applied to the management interface to only allow access to the management network from the IP address assigned to the management interface and, conversely, only allows access from the management network to that management interface address. In addition, only protocols that are needed for the management of these devices are permitted. These protocols could include SSH, NTP, FTP, SNMP, TACACS+, etc. Data traffic should never transit the devices using the connection to the management network.

A sample configuration demonstrating the best practices for applying access-list on the management interface of a Cisco Catalyst switch is shown below:

```
! access-list to be applied inbound on the management interface
access-list <ACL#1> permit icmp <MGMT-Subnet> <inverse-mask> host <MGMT-INT-ADDRESS>
ttl-exceeded
access-list <ACL#1> permit icmp <MGMT-Subnet> <inverse-mask> host <MGMT-INT-ADDRESS>
port-unreachable
access-list <ACL#1> permit icmp <MGMT-Subnet> <inverse-mask> host <MGMT-INT-ADDRESS>
echo-reply
access-list <ACL#1> permit icmp <MGMT-Subnet> <inverse-mask> host <MGMT-INT-ADDRESS> echo
access-list <ACL#1> permit tcp host <TACACS+-SVR-1> eq tacacs host <MGMT-INT-ADDRESS>
established
access-list <ACL#1> permit tcp host <TACACS+-SVR-2> eq tacacs host <MGMT-INT-ADDRESS>
established
access-list <ACL#1> permit tcp host < TACACS+-SVR-1> host <MGMT-INT-ADDRESS> eq tacacs
access-list <ACL#1> permit tcp host < TACACS+-SVR-2> host <MGMT-INT-ADDRESS> eq tacacs
access-list <ACL#1> permit udp host <NTP-SVR-1> host <MGMT-INT-ADDRESS> eq ntp
access-list <ACL#1> permit udp host <NTP-SVR-2> host <MGMT-INT-ADDRESS> eq ntp
access-list <ACL#1> permit tcp <MGMT-Subnet> <inverse-mask> host <MGMT-INT-ADDRESS> eq 22
access-list <ACL#1> permit tcp host <FTP-SVR-1> eq ftp host <MGMT-INT-ADDRESS> gt 1023
established
```

```
access-list <ACL#1> permit tcp host <FTP-SVR-1> eq ftp-data host <MGMT-INT-ADDRESS> gt
1023
access-list <ACL#1> permit tcp host <MGMT-Subnet> gt 1023 host <MGMT-INT-ADDRESS> gt 1023
established
access-list <ACL#1> permit udp <MGMT-Subnet> <inverse-mask> gt 1023 host
<MGMT-INT-ADDRESS> gt 1023
access-list <ACL#1> permit udp host <NAC-MGR-1> host <MGMT-INT-ADDRESS> eq snmp
access-list <ACL#1> permit udp host <NAC-MGR-2> host <MGMT-INT-ADDRESS> eq snmp
access-list <ACL#1> permit udp host <NAC-MGR-vIP> host <MGMT-INT-ADDRESS> eq snmp
access-list <ACL#1> deny   ip any any log

! access-list to be applied outbound on the management interface
access-list <ACL#2> permit ip host <MGMT-INT-ADDRESS> <MGMT-Subnet> <inverse-mask>

! Apply inbound and outbound access-lists on management interface
interface GigabitEthernet2/1
 description Connection to the OOB Management network
 no switchport
 ip address <MGMT-INT-ADDRESS> <subnet-mask>
 ip access-group <ACL#1> in
 ip access-group <ACL#2> out
```

Note An explicit deny entry with the log keyword is included at the end of the access-list applied on the inbound direction of the management interface. This triggers syslog events for traffic attempting to access the device over the management network which is not permitted. This will provide visibility into attacks and facilitate troubleshooting when needing to tune the access-list (e.g., identifying traffic which should be allowed).

IB Management Best Practices

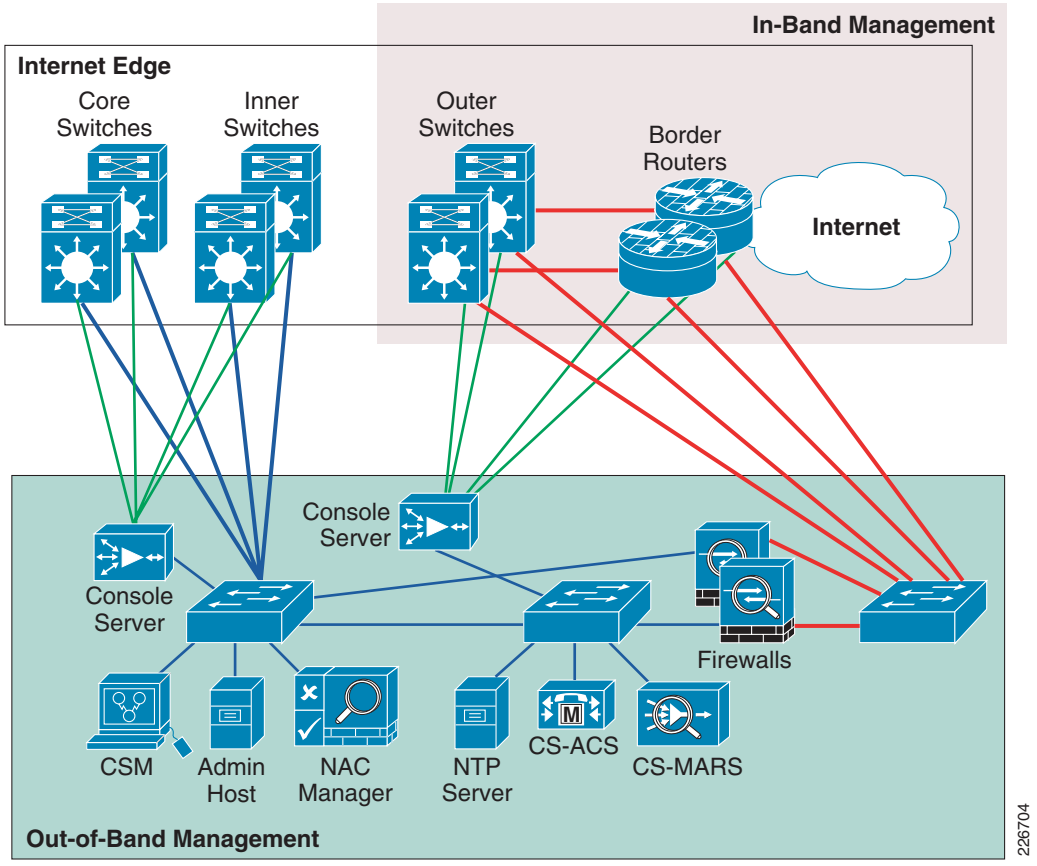
IB management provides management of devices over the same physical and logical infrastructure as the data traffic. IB management is used for devices not located at the headquarters site and devices that do not have a dedicated management interface or spare interface to be used as a management interface. IB management network access should be deployed using the following best practices:

- Enforce access control using firewalls
- Classify and prioritize management traffic using QoS at remote sites
- Provide network isolation using NAT
- Enforce the use of encrypted, secure access, and reporting protocols

Firewalls are implemented to secure the OOB management network hosting the management and monitoring servers from the rest of the network. The firewalls only allow access from the administrative IP addresses of the devices being managed IB and only for the necessary protocols and ports. The firewall is configured to allow protocols such as syslog, secure syslog, SSH, SSL, SNMP, NetFlow, IPSec and protocols needed for the NAC Server to communicate with the NAC Manager (if NAC Appliance is deployed) information into the management segment.

In addition to providing access control for managing devices located at remote sites such as the branch sites, firewalls are recommended to protect the management network from certain devices located in the Internet Edge module. In the case of the Internet edge, any devices outside the edge firewalls deployed in the Internet edge should be protected by a firewall. Despite being deployed at the headquarters, the outer switches and border routers are located outside the edge firewall; therefore, their management connections should be placed in a separate and firewalled segment. This practice is key to contain and mitigate the compromise of any devices facing the Internet. Connecting the outer switches or the border routers directly to the OOB network and without a firewall is highly discouraged, as it would facilitate the bypass of the firewall protection. Figure 9-2 illustrates the OOB and IB management connections to the devices in the Internet edge module.

Figure 9-2 Internet Edge Management Connectivity



When deploying IB management for remote sites, it is critical that QoS is employed to accurately classify and prioritize control and management traffic to and from these sites. This will ensure continuing service availability and remote management even under adverse network conditions, such as high data rates and worm outbreaks. For more information on deploying QoS in the branch, refer to the "QoS in the Branch" section on page 8-9.

Since the management subnet operates under an address space that is completely separate from the rest of the production network, all IB management access occurs through a NAT process on the firewall. Static NAT entries are used on the firewall to translate the non-routable management IP addresses to prespecified production IP ranges that are routed in the routing protocol on the data network.

The following sample ASA NAT configuration fragment illustrates the best practices for hiding the management subnet address from the production network:

```
nat-control
global (outside) 1 interface
nat (inside) 1 <MGMT-Subnet> 255.255.255.0
! create static NAT entry for MARS
static (inside,outside) 10.242.50.99 <MARS-inside-MGMT-address> netmask 255.255.255.255
! create a static NAT entry for ACS
static (inside,outside) 10.242.50.94 <ACS-inside-MGMT-address> netmask 255.255.255.255
! create a static NAT entry for CSM
static (inside,outside) 10.242.50.95 <CSM-inside-MGMT-address> netmask 255.255.255.255
! create a static NAT entry for Admin host
static (inside,outside) 10.242.50.92 <Admin-svr-inside-MGMT-address> netmask
255.255.255.255
! create a static NAT entry for FTP server
static (inside,outside) 10.242.50.96 <FTP-svr-inside-MGMT-address> netmask 255.255.255.255
! create a static NAT entry for NAC Manager
static (inside,outside) 10.242.50.110 <NAC-MGR-inside-MGMT-address> netmask
255.255.255.255
```

Note Static NAT entries are used to translate addresses assigned to management servers inside management subnet range to addresses that are in the outside address range that are routed in the data network. In the above case, management inside addresses are translated to outside addresses within the 10.242.50.0 subnet range.

The following sample inbound firewall policy fragment from the ASA firewall illustrates the best practices for only allowing needed IB access the management network through the firewall protecting OOB management network:

```
! Permit SDEE, syslog, secured syslog, NetFlow reporting, and SNMP traps to MARS
access-list OBB-inbound extended permit tcp any host 10.242.50.99 eq https
access-list OBB-inbound extended permit udp any host 10.242.50.99 eq snmptrap
access-list OBB-inbound extended permit udp any host 10.242.50.99 eq syslog
access-list OBB-inbound extended permit tcp any host 10.242.50.99 eq 1500
access-list OBB-inbound extended permit udp any host 10.242.50.99 eq 2055
! permit TACACS+ to the ACS server for device authentication
access-list OBB-inbound extended permit tcp any host 10.242.50.94 eq tacacs
! permit IPSec traffic to the firewall for remote VPN termination
access-list OBB-inbound extended permit esp any host 10.242.50.1
access-list OBB-inbound extended permit udp any eq isakmp host 10.242.50.1 eq isakmp
! permit traffic from the NAC Server to the NAC Manager
access-list OBB-inbound extended permit tcp host 10.240.10.36 host 10.242.50.110 eq https
access-list OBB-inbound extended permit tcp host 10.240.10.36 host 10.242.50.110 eq 1099
access-list OBB-inbound extended permit tcp host 10.240.10.36 host 10.242.50.110 eq 8995
access-list OBB-inbound extended permit tcp host 10.240.10.36 host 10.242.50.110 eq 8996
! permit traffic from the NAC Profiler to the NAC Manager
access-list OBB-inbound extended permit tcp host 10.240.50.10 host 10.242.50.110 eq ssh

! Apply the inbound access policy to the outside interface
access-group OBB-inbound in interface outside
```

Remote Access to the Management Network

Another recommended best practice for IB management is to configure the firewall protecting the OOB management network for client VPN termination for IB administrative access. This allows administrators at the campus and remote locations to connect to the OOB management networks to access the management servers over a secure VPN tunnel.

The following are best practices for enabling VPN termination for remote management network connectivity:

- Create a VPN address pool within the management segment subnet range
- Create a NAT exception ACLs to prevent address translation for traffic going to the VPN pool addresses from the OOB management addresses
- Enforce remote access authentication
- Configure a VPN idle timeout to ensure VPN tunnels do not stay up indefinitely

The following sample VPN configuration fragment on the ASA firewall illustrates these best practices. This example uses pre-shared keys and TACACS+ for authentication and 3DES for encryption. PKI and AES can also be used for stronger authentication and encryption:

```
! create VPN Pool of addresses from within the management subnet range
ip local pool vpnpool <MGMT-subnet-address-pool>
! create NAT exception lists to prevent NAT to/from the VPN pool of addresses from OOB
interface addresses
access-list nonat extended permit ip <MGMT-Subnet> 255.255.255.0
<MGMT-subnet-address-pool> <VPN-Pool-subnet>
! assign the NAT exceptional ACL to the inside NAT configuration command
nat (inside) 0 access-list nonat
! define crypto maps and assign to outside interface facing inband network
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto dynamic-map rtpdynmap 20 set transform-set myset
crypto map mymap 20 ipsec-isakmp dynamic rtpdynmap
crypto map mymap interface outside
crypto isakmp identity address
crypto isakmp enable outside
! define isakmp policies
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto isakmp policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
! define group-policy
group-policy clientgroup internal
! define VPN idle timeout
group-policy clientgroup attributes
 vpn-idle-timeout 20
! define tunnel attributes including VPN address pool and authentication type
tunnel-group rtptacvpn type remote-access
tunnel-group rtptacvpn ipsec-attributes
 pre-shared-key *
tunnel-group rtpvpn type remote-access
tunnel-group rtpvpn general-attributes
```

```
 address-pool vpnpool
 authentication-server-group tacacs-servers
 authorization-server-group LOCAL
 default-group-policy clientgroup
tunnel-group rtpvpn ipsec-attributes
 pre-shared-key *
```

Network Time Synchronization Design Best Practices

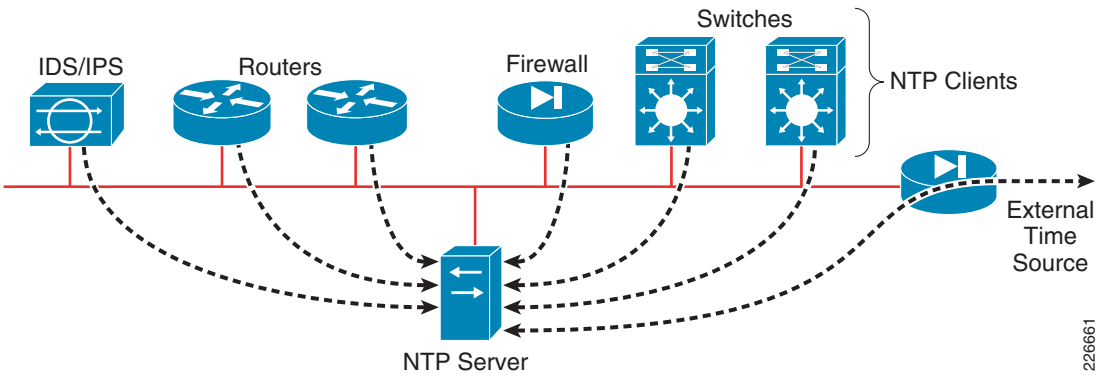
Time synchronization using Network Time Protocol (NTP) for network and security devices is critical for network-wide security event analysis and correlation. Enabling NTP on all infrastructure components is a fundamental requirement. Time servers should be deployed at the headquarters on a secured network segment such as in the Management network module. Internal time servers will be synchronized with external time sources unless you have in-house atomic or GPS-based clock.

The following best common practices should be considered when implementing NTP:

- Deploy a hierarchical NTP design versus a flat design. Hierarchical designs are preferred because they are highly stable, scalable, and provide most consistency. A good way to design a hierarchical NTP network is by following the same structure as the routing architecture in place.
- Use a common, single time zone across the entire infrastructure to facilitate the analysis and correlation of events.
- Control which clients and peers can talk to an NTP server.
- Enable NTP authentication.

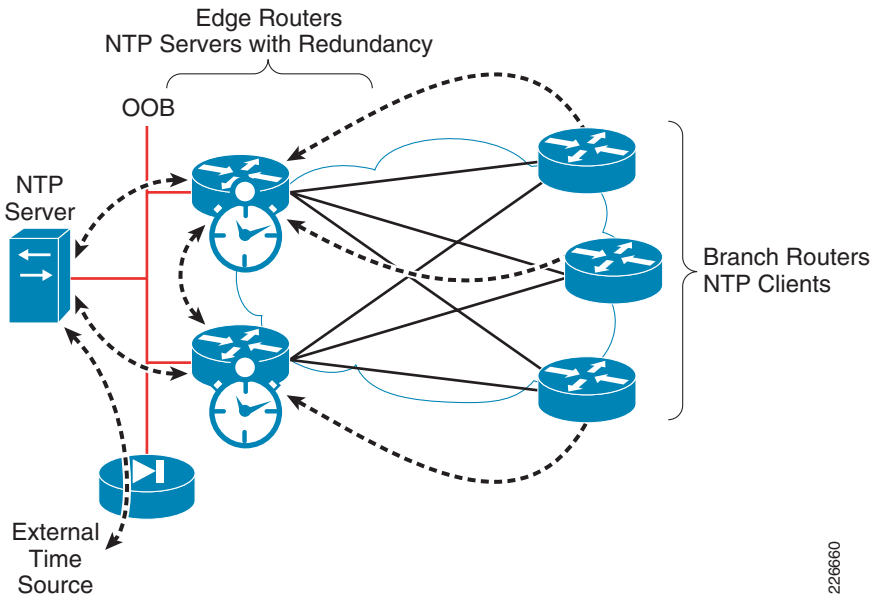
For devices being managed through the OOB management network at the headquarters, transporting NTP over the OOB network flattens and simplifies the design. In this scenario, all routers and switches may be configured as clients (non-time servers) with a client/server relationship with the internal time servers located within the OOB management network. These internal time servers are synchronized with external time sources. This design is illustrated in Figure 9-3.

Figure 9-3 NTP Design Leveraging an OOB Management Network



Branch offices are typically aggregated at one or more WAN edge routers that can be leveraged in the NTP design. Following the routing design, the WAN edge routers should be configured as time servers with a client/server relationship with the internal time servers, and the branch routers may be configured as clients (non-time servers) with a client/server relationship with the WAN edge routers. This design is depicted in Figure 9-4.

Figure 9-4 NTP Design for the WAN Edge and Remote Offices



Management Module Infrastructure Security Best Practices

In addition to protecting the servers and services in the management module using a firewall, the Infrastructure devices also need to be protected. All routers, switches, firewalls, and terminal servers should be hardened following the best practices described in Chapter 2, "Network Foundation Protection."

The following are the key areas of the baseline security applicable to securing the access layer switches:

- Infrastructure device access
  - Implement dedicated management interfaces to the OOB management network.
  - Limit the accessible ports and restrict the permitted communicators and the permitted methods of access.
  - Present legal notification.
  - Authenticate and authorize access using AAA.
  - Log and account for all access.
  - Protect locally stored sensitive data (such as local passwords) from viewing and copying.
- Routing infrastructure
  - Authenticate routing neighbors.
  - Log neighbor changes.
- Device resiliency and survivability
  - Disable unnecessary services.
  - Filter and rate-limit control-plane traffic.
  - Implement redundancy.
- Network telemetry

  - Implement NTP to synchronize time to the same network clock.
  - Maintain and monitor device global and interface traffic statistics.
  - Maintain system status information (memory, CPU, and process).
  - Log and collect system status, traffic statistics, and device access information.
- Network policy enforcement
  - Implement management and infrastructure ACLs (iACLs).

Terminal Server Hardening Considerations

In general, the same best practices described in Chapter 2, "Network Foundation Protection," should be followed to harden the terminal servers. In addition to adopting these best practices for hardening the terminal servers, there are a few important considerations that should be noted.

Typically, Telnet access to devices should be denied and a secure protocol such as SSH should be used. However, in the case of routers acting as terminal servers, console access to network, and security devices may require the use of reverse Telnet. Reverse access is also supported with SSH and it is highly recommended, though this feature may not be always available.

Securing reverse access requires the hardening of the terminal (TTY) lines used to connect to the console ports of the managed network and security devices. Inbound ACLs should be applied to the TTY lines to restrict access to the console ports by permitting and denying access to the reverse SSH/Telnet ports as warranted. In addition, session timeout values should be implemented on the TTY lines to restrict connection from staying connected indefinitely. It is recommended that the timeout values match the corresponding timeout values configured on the console ports of the managed devices. In cases where the managed devices does not support console session timeout enforcement, the timeout values on the TTY lines can be used to enforce the session timeouts for the device.

The following terminal server configuration fragment configures an inbound ACL on the TTY line to restrict access to reverse SSH/telnet ports 2001 through 2006 only from hosts in the management subnet. It also configures the session timeout values to 3 minutes.

```
! Configure extended ACL to permit access for reverse SSH/telnet ports 2001 thru 2006
access-list 113 permit tcp <MGMT-Subnet> <inverse-mask> any range 2001 2006
access-list 113 deny   ip any any log
!
line 1 16
! Configure a session timeout of 3 minutes
 session-timeout 3
! Apply inbound ACL to restrict access to only ports 2001 through 2006 from the Management
Subnet
 access-class 113 in
 no exec
! Require users to authenticate to terminal server using AAA before accessing the
connected console ports of managed devices
 login authentication authen-exec-list
 transport preferred none
! Enable SSH for reverse access to connected console ports
 transport input ssh
! Enable telnet for reverse telnet to connected console ports
 transport input telnet
transport output none
```

Firewall Hardening Best Practices

The firewalls should be hardened in a similar fashion as the infrastructure routers and switches. The following measures should be taken to harden the firewalls:

- Use HTTPS and SSH for device access
- Configure AAA for role-based access control and logging. Use a local fallback account in case AAA server is unreachable.
- Use NTP to synchronize the time
- Authenticate routing neighbors and log neighbor changes

Management access to the firewalls should be restricted to SSH and HTTPS. SSH is needed for CLI access and HTTPS is needed for the firewall GUI-based management tools such as CSM and ADSM. Additionally, this access should only be permitted for users authorized to access the firewalls for management purposes.

The following ASA configuration fragment illustrates the configuration needed to generate a 768 RSA key pair and enabling SSH and HTTPS access for devices located in the management subnet.

Note CS-MARS requires a minimum modulus size of 768 bits or greater.

```
! Generate RSA key pair with a key modulus of 768 bits
crypto key generate rsa modulus 768
! Save the RSA keys to persistent flah memory
write memory
! enable HTTPS
http server enable
! restrict HTTPS access to the firewall to CSM on the inside interface
http <CSM-IP-address> 255.255.255.255 inside
! restrict SSH access to the firewall from the Admin management server located in the
management segment on the inside interface
ssh <admin-host-IP-address> 255.255.255.255 inside
! Configure a timeout value for SSH access to 5 minutes
ssh timeout 5
```

Note SSH and HTTPS access would typically be restricted to a dedicated management interface over an OOB management network. However, since the firewall protecting the management module connects to the OOB network via its inside interface, a dedicated management interface is not used in this case.

Users accessing the firewalls for management are authenticated, authorized, and access is logged using AAA. The following ASA configuration fragment illustrates the AAA configurations needed to authenticate, authorize, and log user access to the firewall:

```
aaa-server tacacs-servers protocol tacacs+
 reactivation-mode timed
aaa-server tacacs-servers host <ACS-Server>
 key <secure-key>
aaa authentication ssh console tacacs-servers LOCAL
aaa authentication serial console tacacs-servers LOCAL
aaa authentication enable console tacacs-servers LOCAL
aaa authentication http console tacacs-servers LOCAL
aaa authorization command tacacs-servers LOCAL
aaa accounting ssh console tacacs-servers
```

```
aaa accounting serial console tacacs-servers
aaa accounting command tacacs-servers
aaa accounting enable console tacacs-servers
aaa authorization exec authentication-server
! define local username and password for local authentication fallback
username admin password <secure-password> encrypted privilege 15
```

The routing protocol running between the OOB firewall and the core should be secured. The following ASA configuration fragment illustrates the use of EIGRP MD5 authentication to authenticate the peering session between the outside firewall interface and the core routers:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.242.50.1 255.255.255.0
 authentication key eigrp 1 <strong-key> key-id 10
 authentication mode eigrp 1 md5
```

As with the other infrastructure devices in the network, it is important to synchronize the time on the firewall protecting the management module using NTP. The following configuration fragment illustrates the NTP configuration needed on an ASA to enable NTP to an NTP server located behind the inside interface:

```
ntp authentication-key 10 md5 *
ntp authenticate
ntp trusted-key 10
ntp server <NTP-Server-address> source inside
```

Threats Mitigated in the Management

Table 9-1 Management Threat Mitigation Features

	Unauthorized Access	DoS, DDoS	MITM Attacks	Privilege Access	Intrusions	Password Attacks	IP Spoofing	Visibility	Control
Firewall	Yes	Yes			Yes		Yes	Yes	Yes
AAA	Yes			Yes	Yes	Yes		Yes	Yes
OOB Network	Yes	Yes	Yes				Yes	Yes	Yes
VPN	Yes		Yes	Yes	Yes				Yes
SSH	Yes		Yes	Yes	Yes				Yes
Strong Password Policy	Yes		Yes	Yes	Yes	Yes			Yes
Management ACLS	Yes	Yes		Yes	Yes				Yes
iACLs	Yes	Yes		Yes	Yes		Yes		Yes

Table 9-1 Management Threat Mitigation Features (continued)

NetFlow, Syslog								Yes	
Router Neighbor Authentication									Yes