Basic Infrastructure Security

Before deploying firewalls, ACLs, IDS, or any other security technologies, each router and switch in the data center should have a baseline security configuration. If attackers gain access to network devices, chances are very high that other devices in the network can be compromised. This chapter describes these basic security precautions and includes the following topics:

Hardening Control Protocols

This section describes how to harden control protocols as a basic security precaution that should be performed on all applicable devices in the data center. It includes the following topics:

Neighbor Router Authentication

This section contains configuration listings for neighbor router authentication.

Configuration with Layer 3 Links

Routing between the aggregation switches and the core routers uses MD5 authentication as illustrated by the following configuration for OSPF (the relevant configurations are highlighted in italics):

```
router ospf 20
  auto-cost reference-bandwidth 10000
  area 20 authentication message-digest
  area 20 nssa
```

```
 timers spf 1000 1000 1000
 !
 ! Define the N2 routes that you want to leak to the core
 ! And in the core remember to prevent the N2 from leaking
 ! into the rest of the network if not necessary
 !
 redistribute static subnets route-map redistribute-list
 !
 passive-interface default
 no passive-interface vlan3
 !
 ! If using L3 links
 no passive-interface TenGigabitEthernet1/1
 no passive-interface TenGigabitEthernet1/2
 ! If using L3 VLANs (VLAN 13 goes to core1 and VLAN 14 goes to core2)
 ! no passive-interface Vlan13
 ! no passive-interface Vlan14
 !

 network 10.20.5.0 0.0.0.255 area 20
 network 10.20.10.0 0.0.0.255 area 20
 network 10.20.30.0 0.0.0.255 area 20
 network 10.10.0.0 0.0.255.255 area 20
 network 10.10.10.0 0.0.0.255 area 20
 network 10.21.0.0 0.0.255.255 area 20
```

Note Be sure to filter the redistributed routes with the **redistribute static subnets route-map** <*route-map-name*> command.

The following shows the configuration on the Layer 3 interfaces:

```
interface TenGigabitEthernet1/1
description to_core1
  ip address 10.21.0.1 255.255.255.252
  no ip redirects
  no ip proxy-arp
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 0 <clear-text password>
  ip ospf network point-to-point
!
```

When the routing between the aggregation switches and the core routers uses EIGRP, the configuration is as follows:

```
Router(config)#key chain AGG
Router(config-keychain)#key 1
Router(config-keychain-key)#key-string <key>

Router(config)#interface TenGigabitEthernet1/1
Router(config-if)#ip authentication mode eigrp 10  md5
Router(config-if)#ip authentication key-chain eigrp 10 AGG
```

For more information, see the following URL:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/

Configuration with Layer 3 VLANs

When deploying the traffic capturing solution with Cisco IOS releases prior to 12.2(18)SXE, you need to use Layer 3 VLANs connecting the aggregation switches to the core instead of Layer 3 links because of CSCdy22529. In the latest releases, it is possible to mix PSPAN with VSPAN, so this configuration

might not be necessary. The configuration differs based on whether or not a CSM is present in the chassis. When a CSM is present in the chassis, all VLANs are trunked to the CSM, which prevents autostate from detecting that a link connecting to the core has gone down.

Configuration without a CSM in the Chassis

Following is the configuration without a CSM in the chassis:

```
!
vlan 13
 name l3linkcore1
!
vlan 14
 name l3linkcore2
!
interface TenGigabitEthernet1/1
 no ip address
 switchport
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast
 no shut
!
interface TenGigabitEthernet1/2
 no ip address
 switchport
 switchport access vlan 14
 switchport mode access
 spanning-tree portfast
 no shut
!
router ospf 20
  log-adjacency-changes
  auto-cost reference-bandwidth 10000
  area 20 authentication message-digest
  area 20 nssa
  timers spf 1000 1000 1000
  !
  ! Define the N2 routes that you want to leak to the core
  ! And in the core remember to prevent the N2 from leaking
  ! into the rest of the network if not necessary
  !
  redistribute static subnets route-map redistribute-list
  !
  passive-interface default
  no passive-interface vlan3
  !
  ! If using L3 links
  ! no passive-interface TenGigabitEthernet1/1
  !no passive-interface TenGigabitEthernet1/2
  ! If using L3 VLANs (VLAN 13 goes to core1 and VLAN 14 goes to core2)
  no passive-interface Vlan13
  no passive-interface Vlan14
  !
!
  network 10.20.5.0 0.0.0.255 area 20
  network 10.20.10.0 0.0.0.255 area 20
  network 10.20.30.0 0.0.0.255 area 20
  network 10.10.0.0 0.0.255.255 area 20
  network 10.10.10.0 0.0.0.255 area 20
  network 10.21.0.0 0.0.255.255 area 20
```

Note Be sure to filter the redistributed routes with the **redistribute static subnets route-map** <*route-map-name*> command.

The following shows the configuration on the Layer 3 VLANs:

```
interface Vlan13
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
!
interface Vlan14
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 no shut
```

Configuration with a CSM in the Chassis

If a CSM is present in the chassis, configure the OSPF timers to accelerate the detection of the link failure or to clear the trunk between the CSM and the Catalyst 6500 from unnecessary VLANs.

Modify the configuration from the previous section as follows:

```
interface Vlan13
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
!
interface Vlan14
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
```

```
! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
```

Alternatively, you can clear the port channel/trunk connecting the Catalyst 6500 to the CSM from unnecessary VLANs. Use **show etherchannel summary** to find out the port channel assigned to the CSM, and then use the **range** command from Po255 to the CSM port channel to clear the configuration from unused VLANs:

```
agg1#show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        u - unsuitable for bundling
Number of channel-groups in use: 4
Number of aggregators:           4

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SU)         LACP      Gi8/1(P)   Gi8/2(P)   Gi8/3(P)   Gi8/4(P)
                                 Gi8/5(P)   Gi8/6(P)   Gi8/7(P)   Gi8/8(P)
255    Po255(SD)        -
260    Po260(SU)        -         Gi4/1(P)   Gi4/2(P)   Gi4/3(P)   Gi4/4(P)
272    Po272(SD)        -         Gi3/1(D)   Gi3/2(D)   Gi3/3(D)   Gi3/4(D)
                                 Gi3/5(D)   Gi3/6(D)
```

In the previous screen, you can see that the channel between the Catalyst 6500 and the CSM is Po260.

```
interface range Po255 - 260
  switchport trunk allowed vlan <CSM VLAN list>
!
```

SNMP

Network management traffic should be out-of-band or on a dedicated VLAN. ACLs should restrict SNMP access. Change the community strings from the default to match the community of the SNMP manager and the agent.

Disable SNMP if not in use (**no snmp-servers**).

For more information, see the following URL:
http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

Network Time Protocol

Network Time Protocol (NTP) is essential for timestamp accuracy when logging, because logs are collected from several devices, and also for certificate management. Carry the NTP traffic on the out-of-band management network if possible. NTP is then disabled on all the interfaces of an aggregation router of a data center; (this disables the device from providing NTP services, not from acting as a client). All network devices in the server farm synchronize out-of-band on a dedicated network:

```
interface Vlan10
 description database
 ip address 10.20.10.2 255.255.255.0
 standby 1 ip 10.20.10.1
 standby 1 timers 1 3
 standby 1 priority 120
 standby 1 preempt delay minimum 180
 no ip unreachables
 no ip redirects
 no ip proxy-arp
! >> Disable NTP services <<
 ntp disable
 no shut
!
```

For more information, see the following URLs:

- http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml
- http://www.cisco.com/en/US/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml (document 24330)

If using Catalyst IOS, see "Catalyst 4000, 5000, and 6000 Series Configuration and Management Best Practices" at the following URL: http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml.

Use at least three lower stratum servers for redundancy. The following is an example of NTP configuration for Pacific Standard Time (PST) on a Catalyst 6500 with Cisco IOS software:

```
clock timezone PST -8
clock summer-time PDT recurring
ntp authentication-key 1 md5 <password>
ntp update-calendar
ntp trusted-key 1
ntp authenticate
ntp server <IP address> key 1
ntp server <IP address 2>
ntp server <IP address 3>
ntp source loopback0
```

The following is the output of the **show** command when NTP is synchronized:

```
agg#show clock
14:04:36.353 PST Fri Feb 11 2005

agg#show ntp status
Clock is synchronized, stratum 2, reference is 172.28.214.42
nominal freq is 250.0000 Hz, actual freq is 249.9981 Hz, precision is 2**18
reference time is C5B7A9F8.D05B917E (14:02:32.813 PST Fri Feb 11 2005)
clock offset is -0.0793 msec, root delay is 0.82 msec
root dispersion is 0.17 msec, peer dispersion is 0.05 msec

agg#show ntp associations
      address         ref clock     st  when  poll reach  delay  offset    disp
*~172.28.214.42    .LOCL.            1     7   128  377     0.8   -0.04     0.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

The following is an example of NTP configuration for PST on an IDS sensor:

```
service Host
timeParams
offset -480
standardTimeZoneName PST
summerTimeParams
active-selection recurringParams
```

```
recurringParams
summerTimeZoneName PDT
startSummerTime
monthOfYear apr
weekOfMonth first
dayOfWeek sun
timeOfDay 02:00:00
exit
endSummerTime
monthOfYear oct
weekOfMonth last
dayOfWeek sun
timeOfDay 02:00:00
exit
exit
exit
ntpServers ipAddress <NTP server>
keyId 1
keyValue <password>
exit
exit
exit
```

The following is an example of NTP configuration for PST on the SSLSM:

```
clock timezone PST -8
clock summer-time PDT recurring first Sunday April 02:00 last Sunday October 02:00 60
ntp authentication-key 1 md5 <password>
ntp trusted-key 1
ntp clock-period 17179879
ntp server <NTP server> key 1
ntp authenticate
```

Loopback

The loopback interface provides several advantages, both for the purpose of routing protocols as well as for security. The loopback should be set as the source for NTP, logging, AAA, and so on.

The following is an example configuration:

```
Interface loopback0
 ip address 10.10.10.1 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
```

For more information, see the following URL:
http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html.

Disabling Unused Services

Disabling services that are not required on a specific device is a basic security precaution that should be performed on every device in the data center. This section describes how to disable some of the services that may not be required on specific devices in the data center and that represent particular security risks.

If you do not need the BOOTP or the DHCP relay and/or snooping function (this is often used in server farms to image the servers), you can disable the DHCP and the BOOTP service by entering the following commands:

```
no ip bootp server
no service dhcp
```

To disable the finger service, enter the following command (by default this is already off):

```
 no ip finger
no service finger
```

If you need to use HTTP for configuration purposes, configure authentication and ACLs to limit the devices that are allowed to access this service, and use a different port than 80. In this SRND, the HTTP service is used to download the CiscoView Device Manager (CVDM) applet to the management station. The CVDM tool sends configuration commands via SSH. You need to configure a username with privilege 15 for the web-based management:

```
username webadmin privilege 15 secret 0 <password>
ip http server
ip http port 8768
ip http authentication local
ip http access-class 5
ip http path bootflash:
access-list 5 permit <mgmt-station-ip-address>
```

If you do not plan to use the web-based interface, disable the HTTP service on devices where it is not required by entering the following command:

```
 no ip http server
```

Note Some design documents in this SRND use the CVDM tool for configuration purposes. This tool executes on the network management PC browser, but it requires that an applet be downloaded from the Catalyst 6500. For this reason, the HTTP server needs to be configured on the Catalyst 6500 switch. The CVDM tool sends commands to the Catalyst switch via SSH.

If available, use HTTPS instead of HTTP. To enable HTTPS, enter the following command:

```
ip http server-secure
```

To disable source routing, enter the following command:

```
no ip source-route
```

Disable TCP small servers and UDP small servers by entering the following commands:

```
no service tcp-small-servers
no service udp-small-servers
```

For more information, see the following URL:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml.

The following configuration summarizes the commands to enter from global configuration mode:

```
no service pad
no ip source-route
no ip finger
no service finger
no ip bootp server
no service tcp-small-servers
no service udp-small-servers
no  boot network
no service config
service password-encryption
```

Disable broadcasts should be disabled to prevent certain attacks, such as the smurf attack, by entering the following command:

```
Router(config-if)# no ip directed-broadcast
```

In server farms, applications often use messages to a broadcast address, in which case you need to ensure that "directed-broadcast" is enabled on the interface. ACLs are then used to limit the use of broadcast addresses to specific UDP ports. ICMP traffic and TCP traffic directed to a broadcast address should be prevented. The following is the configuration for a VLAN interface on the routing engine:

```
interface Vlan5
 ip address 10.20.5.2 255.255.255.0
 standby 1 ip 10.20.5.1
 standby 1 timers 1 3
 standby 1 priority 120
 standby 1 preempt delay minimum 180
! In presence of Messaging Middleware uncomment the following
! ip directed-broadcast
! mls ip directed-broadcast exclude-router
 no ip unreachables
 no ip redirects
 no ip proxy-arp
! >> Disable NTP services <<
 ntp disable
 no shut
!
```

Proxy ARP allows access across LAN segments as if these segments were part of the same segment. Most of the time, this service is not necessary, unless legacy systems are present.

To disable proxy ARP, enter the following command:

```
no ip proxy-arp
```

To disable ICMP redirect, enter the following command:

```
no ip redirects
```

The following configuration summarizes the commands to enter from interface configuration mode:

```
no ip redirects
no ip directed-broadcasts
no ip proxy-arp
```

Cisco Discovery Protocol (CDP) is very useful for troubleshooting. CDP should be enabled globally and disabled on a per-interface basis on those physical interfaces that connect to the servers.

```
interface GigabitEthernet8/18
 no ip address
 switchport
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
! >> Port Security <<
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
```

Preventing Unauthorized Access

Authorization, Authentication, and Accounting (AAA) helps prevent unauthorized access by providing login authentication, command authorization, and accounting of user information. You can either define usernames and passwords on the local database of each switch, or on a centralized access control server. The latter approach is recommended, using AAA technology in conjunction with a Terminal Access Controller Access Control System (TACACS+) or with a Remote Authentication Dial-in User Service (RADIUS) server.

Use a TACACS+ server (Cisco Secure ACS), which maintains a central location of username and password information, for scalability and manageability. TACACS also provides more granular access control. Username and passwords in the local database can be used in case the access control server becomes unavailable.

TACACS+ encrypts the entire body of the access-request packet between the client and the server. RADIUS, on the other hand, encrypts only the password in the access-request packet from the client to the server. This leaves other information such as username, authorized services, and accounting open to capture by a third party.

Local AAA implementations use the local username and password database on the switch to authenticate user login attempts. Command authorization per user can be performed by setting the individual user privilege level in the local username and password database. At least enabling local AAA on each data center switch, router, and firewall is required for providing a minimum level of security.

To define a local username and password, enter the following command:

```
username local username secret 0 <password>
```

To define the password for privileged mode, enter the following command:

```
enable secret 0 <password>
```

For more information, see the following URLs:

- http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/supcfg.html
- http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfpass.html

The following configuration allows access to the network devices from a virtual terminal line (VTY) using TACACS servers and falls back to local authentication if the TACACS server is unavailable.

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ if-authenticated local
tacacs-server host <server IP address>
tacacs-server key <same key as the server>
```

For more information, see the following URL:
http://www.cisco.com/en/US/docs/ios/internetwrk_solutions_guides/splob/guides/dial/aaasub/aaasols.html.

Access to the console can be authenticated using the access control server, or if the authentication is completed on the commserver, access to the switch or router can be given automatically. In the initial deployment, the following configuration prevents getting locked out:

```
aaa authentication login LOCALAUTHC local
line con 0
  exec-timeout 5 0
  password 0 <password>
  login authentication LOCALAUTHC
```

This configuration relies on local authentication and does not involve the use of the TACACS server. However, it provides better security than no authentication at all.

The use of the LOCALAUTHC authentication list overrides the default authentication list. You can also use the line password instead of local authentication. In that case, the configuration is as follows:

```
aaa authentication login LOCALAUTHC line
```

Some commands, such as **enable** or **username**, provide the option to encrypt the password by using the **secret** keyword. To prevent saving passwords in clear text on configuration files, use the **service password-encrypt** option.

For more information, see the following URL:
http://www.cisco.com/en/US/docs/ios/12_1/security/command/reference/srdpass.html.

It is good practice to not give privilege 15 to any users (except for web-based administration). You can configure local username and passwords as follows:

```
username administrator privilege 1 secret 0 <password>
no enable password
enable secret 0 <password>
```

The following configuration allows access to the switch or router over a VTY line, controlled with an access list and identifying the preferred transport protocol as SSH. It is good practice to specify the timeout value and to configure “service tcp-keepalive-in” to avoid consuming VTY resources with dropped sessions. An access list specifies the allowed IP addresses and logs the users.

```
service tcp-keepalives-in
service tcp-keepalives-out
line vty 0 4
  access-class 101 in
  exec-timeout 5 0
  login local
  transport input ssh
!
access-list 101 permit tcp host <management-host> host 0.0.0.0 eq 22 log-input
access-list 101 deny ip any any log-input
```

For more information about interactive access to the router/switch, see the following URL:
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml.

Before you can use the **transport input ssh** command in this configuration, you must first complete the following steps.

Configure initial authentication (either local or using an ACS server).

To define a domain name, enter the following command:

```
ip domain-name name
```

To generate the crypto key pairs**,** enter the following command**:**

```
crypto key gen rsa usage-key modulus key size
```

To define a timeout for the I/O response, enter the following command:

```
ip ssh time-out timeout
```

To define the number of password attempts that the client is allowed, enter the following command:

```
ip ssh authentication-retries number of retries
```

To specify the SSH version, enter the following command:

```
ip ssh version ssh versio
```

Certain commands should not be available to users logged with privilege level 1:

```
privilege exec level 15 show firewall
privilege exec level 15 show ssl-proxy
privilege exec level 15 ssh
privilege exec level 15 show ip access-list
privilege exec level 15 show access-list
privilege exec level 15 show logging
privilege exec level 15 connect
privilege exec level 15 telnet
!
! Bring all the other "show" command to level 1
!
privilege exec level 1 show
```

Logging

To simplify troubleshooting and security investigation, monitor router subsystem information received from the logging facility (syslog). You can adjust the amount of detail in the logging information. A good level of general logging for everyday use is “informational”. You can capture much more detail using the “debug” level, but that level should be used only on a temporary basis. The syslog messages should be sent to a server, because when you log messages to the memory buffer, the information is lost when the switch or router is reset.

Logging to the console is not recommended because administrators do not spend much time actually connected to the console after initial installation and configuration is complete. The commands for basic logging configuration are as follows.

To configure timestamps for the log messages, enter the following command:

```
service timestamps log datetime msec localtime show-timezone
```

To configure a syslog server, enter the following commands:

```
service timestamps debug datetime localtime
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
! >> local logging <<
no logging console
no logging monitor
logging buffered 100000 informational
!
! >> logging on syslog server <<
! ACLs log at the informational level - 6
!
logging <syslog-server-IP-address>
logging source-interface loopback 0
! the following is also the default
logging trap informational
```

Template for Server Ports and VLAN Interfaces

The following configuration template can be used for server ports. It includes basic Layer 2 security to limit the number of MAC addresses that the server can originate on a port. This protects against MAC flooding attacks, such as those generated by tools such as *macof*, and it prevents a server from changing the Spanning Tree topology by using Bridge Protocol Data Units (BPDUs). The number of MAC

addresses that a port expects to receive might be restricted to three in the presence of NIC teaming, but other server ports might see more MAC addresses coming out of the same NIC because of the presence of multiple virtual machines on a single server. For this reason, it is better to allow a higher number of MAC addresses (ten in this example).

Note Port security operates by associating a MAC address with the port where it was first learned, and does not allow a MAC address move to another secure port in the same VLAN until a timer has expired. Port security does not interoperate with certain HA cluster implementations where the move of a "group" causes a move of the MAC address. Port security does not interoperate well with a Virtual Machines move either, because the Virtual Machine may carry the MAC address with it. Port security does not interoperate correctly with the failback of teaming software where the primary NIC coming back online preempts the secondary NIC. This is because the preemption is not associated with a linkdown of the secondary NIC, which is required to flush the port security MAC association table.

```
interface GigabitEthernet8/8
 no ip address
 switchport
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
! >> Port Security <<
! >> do not use with Virtual Machines, HA clusters, NIC teaming
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
```

The following configuration template can be used for VLAN interfaces on the routing engine that provides the default gateway function for the servers:

```
interface Vlan5
 ip address 10.20.5.2 255.255.255.0
 standby 1 ip 10.20.5.1
 standby 1 timers 1 3
 standby 1 priority 120
 standby 1 preempt delay minimum 180
 ! If need directed broadcast:
 ! ip directed-broadcast
 ! mls ip directed-broadcast exclude-router
 no ip unreachables
 no ip redirects
 no ip proxy-arp
! >> Disable NTP services <<
 ntp disable
 no shut
!
```

Configurations

The baseline configuration for basic infrastructure security follows. This configuration assumes that traffic capturing is used, and that a CSM is in the chassis.

```
!
! CATALYST SWITCH CONFIGURATION
```

```
! ==============================
!
hostname agg1
!
! NTP CONFIGURATION
! =================
!
clock timezone PST -8
clock summer-time PDT recurring first Sunday April 2:00 last Sunday October 2:00
!
! More information on NTP @
! http://www.cisco.com/warp/public/126/ntpm.html
!
ntp authentication-key 1 md5 C1sC0!
ntp authenticate
ntp update-calendar
ntp trusted-key 1
ntp server <ntp-server-IP-address> key 1
!
! 3 lower stratum sources should be used at least
! ntp server <server2>
! ntp server <server3>
!
ntp source loopback 0
!
! DNS CONFIGURATION
! =================
ip domain-lookup source-interface Vlan82
ip domain-name example.com
ip name-server <dns-server-ip-address>
!
! If you do not use DNS names to reference other
! devices in the configuration you can disable the
! DNS lookup function. I am using them so I don't disable
! it
!
! no ip domain-lookup

!
! BASIC HARDENING
! ===============
!
no snmp-servers
no service pad
no ip finger
no service finger
no ip source-route
no service tcp-small-servers
no service udp-small-servers
no boot network
no service config
!
! If you do not need the BOOTP relay function
! for the servers disable the BOOTP service
!
no ip bootp server
!
! If you do not need the DHCP helper or DHCP Snooping function
! to address the servers disable the DHCP service
!
no service dhcp
!
!
! ENABLE PASSWORD ENCRYPTION
```

```
!
service password-encryption
!
! SSH
! ===
!
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh version 2
!
! CONFIGURATION TO SUPPORT CVDM
! ============================
!
! web-based administration requires privilege 15
!
username webadmin privilege 15 secret 0 C1sC0!w3B
!
! Change the web access to use port different from port 80
!
ip http server
ip http port 8768
ip http authentication local
ip http access-class 5
ip http path bootflash:
!
! ACCESS CLASS TO CONTROL CONFIGURATION ACCESS
! ===========================================
!
access-list 5 permit <source-ip-of-mgmt-station>
!
! LOCAL AUTHENTICATION
! ====================
!
line console 0
 login local
 exec-timeout 5 0
 ! transport input none
!
! If possible keep one VTY accessible by a local host
! only in case all the other VTYs become inaccessible
!
!
service tcp-keepalives-in
service tcp-keepalives-out
!
line vty 0 4
 login local
 transport input telnet ssh
 transport output none
 access-class 101 in
 exec-timeout 5 0
!
access-list 101 permit tcp host <management-host> host 0.0.0.0 eq 22 log-input
access-list 101 permit tcp host <management-host> host 0.0.0.0 eq 23 log-input
access-list 101 deny ip any any log-input
!
! Do not give privilege > 1 to a user by default
!
! Make sure to use "secret"
! Make sure the password is at least 8 characters
! lowercase, uppercase, numbers and special characters
!
username administrator privilege 1 secret 0 C1sC0!v7Y
```

```
!
! USE ENABLE SECRET INSTEAD OF ENABLE PASSWORD
! Make sure that the enable secret is different
! from any other password
!
no enable password
enable secret 0 3N@8l3p4SSw0r!
!
! CHANGE THE PRIVILEGE LEVELS
! Prevent "show firewall [vlan-group]"
! from being executed at user exec mode
!
privilege exec level 15 show firewall
privilege exec level 15 show ssl-proxy
privilege exec level 15 ssh
privilege exec level 15 show ip access-list
privilege exec level 15 show access-list
privilege exec level 15 show logging
privilege exec level 15 connect
privilege exec level 15 telnet
!
! Bring all the other "show" command to level 1
!
privilege exec level 1 show
!
! LOOPBACK ADDRESSES
! ==================
!
interface loopback0
 ip address <loopback-address> 255.255.255.255
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no shut
!
! SNMPv3 (RFC3414) CONFIGURATION
! ==============================
!
! If SNMP not in use
no snmp-server
!
! If SNMP in use:
! snmp-server engineID local <24-character local-engineID>
! snmp-server engineID remote <remote-ip-addr> <24-character remote-engineID>
! snmp group <group-name> v3 priv [read <readview>]
! ! By default the readview is every object belonging to the Internet (1.3.6.1) OID
! snmp-server user <user-name> <group-name> auth md5 <password>
! ! Specify the recipient of SNMP TRAPS
! snmp-server host <remote-ip-addr> traps v3 priv <community-string>
! snmp-server enable traps
!
! LOGGING CONFIGURATION
! =====================
!
! System messages on the 6k:
! http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/msgguide/emsg.htm
!
! http://www.sans.org/rr/whitepapers/logging/
!
! L2 LOGGING LEVEL INFORMATION:
! sys/5, dtp/5, pagp/5, mgmt/5, mls/5, cdp/4, udld/4, all other facilities: 2
!
!
service timestamps debug datetime localtime
```

```
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
! >> local logging <<
no logging console
no logging monitor
logging buffered 100000 informational
!
! >> logging on syslog server <<
! ACLs log at the informational level - 6
!
logging <syslog-server-IP-address>
logging source-interface loopback 0
! the following is also the default
logging trap informational
!
! FOR MORE INFORMATION
! ====================
! Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release
12.3
!
!
! CRASHDUMP INFORMATION
! =====================
!
ip ftp username <username>
ip ftp password 0 C1sC0!f7P
exception core-file dcrouter-agg1
exception protocol ftp
!
exception dump <ftp-server-ipaddress>
!
! VTP and Spanning-Tree
! =====================
!
vtp domain mydomain
vtp mode transparent
!
power redundancy-mode combined
!
spanning-tree mode rapid-pvst
spanning-tree loopguard default
spanning-tree extend system-id
spanning-tree vlan 1-1000 root primary
spanning-tree pathcost method long
!
! VLAN CONFIGURATION
!
vlan internal allocation policy descending
!
vlan 2
 name native-vlan
!
vlan 5
 name webappoutside
!
vlan 10
 name databaseoutside
!
vlan 13
 name l3linkcore1
!
vlan 14
 name l3linkcore2
```

```
vlan 15
 name clientsandca
!
vlan 30
 name l3linkagg1agg2
!
vlan 44
 name msfc-csm
!
vlan 45
 name sslsm-csm
!
vlan 82
 name mgmt-vlan
!
vlan 100
 name CSMfaulttolerant
!
vlan 105
 name webappinside
!
vlan 110
 name databaseinside
!
vlan 200
 name fwsm_failover_vlan
!
vlan 201
 name fwsm_flink
!
vlan 300
 name rspan
 remote-span
!
! You can use Gig6/1 or Gig6/2 as management ports
! but in presence of SVCS modules it's better to have
! a mgmt VLAN for direct access to the SVCS modules
!
! INTERFACE CONFIGURATION
!
! L3 INTERFACES: IF YOU DO NOT USE SPAN USE THE FOLLOWING CONFIGURATION
!
! interface TenGigabitEthernet1/1
!  description to_core1
!  ip address 10.10.70.2 255.255.255.0
!  no ip redirects
!  no ip proxy-arp
!  ntp disable
!  ip ospf authentication message-digest
!  ip ospf message-digest-key 1 md5 0 C1sC0!
!  ip ospf network point-to-point
!  no shut
! !
! interface TenGigabitEthernet1/2
!  description to_core2
!  ip address 10.10.80.2 255.255.255.0
!  no ip redirects
!  no ip proxy-arp
!  ntp disable
!  ip ospf authentication message-digest
!  ip ospf message-digest-key 1 md5 0 C1sC0!
!  ip ospf network point-to-point
!  no shut
! !
```

```
!
! CONNECTIVITY TO THE CORE WITH L3VLANs
! TO BE ABLE TO USE SPAN WITH RELEASES PRIOR TO 12.2(18)SXE
!
interface TenGigabitEthernet1/1
 no ip address
 switchport
 switchport access vlan 13
 switchport mode access
 spanning-tree portfast
 no shut
!
interface TenGigabitEthernet1/2
 no ip address
 switchport
 switchport access vlan 14
 switchport mode access
 spanning-tree portfast
 no shut
!
! USE A MGMT VLAN FOR THE CATALYST SWITCH, FWSM, CSM
!
interface GigabitEthernet5/2
 description managementport
 media-type rj45
 no ip address
 switchport
 switchport access vlan 82
 switchport mode access
 spanning-tree portfast
 no shut
!
! don't mix the STP of the DC with the mgmt network
!
 spanning-tree bpdufilter enable
 no shut
!
interface range GigabitEthernet8/1 - 8
 description agg-connection
 switchport
 switchport mode trunk
 switchport nonegotiate
 channel-protocol lacp
 channel-group 2 mode active
 no shut
!
interface Port-channel2
 no ip address
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport nonegotiate
 ! >> use a != native VLANs on trunks than on access ports <<
 switchport trunk native vlan 2
 ! >> do not trunk VLAN 13 , 14 , 82 <<
 switchport trunk allowed vlan 5,10,30,44,45,100,105,110,200,201,300
 no shut
!
interface GigabitEthernet8/15
 description web-server-port
 no ip address
 switchport
 switchport access vlan 105
 switchport mode access
```

```
 spanning-tree portfast
 ! >> Port Security <<
 ! >> do not use with Virtual Machines, HA clusters, NIC teaming
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
 ! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
interface GigabitEthernet8/16
 description application-server
 no ip address
 switchport
 switchport access vlan 105
 switchport mode access
 spanning-tree portfast
 ! >> Port Security <<
 ! >> do not use with Virtual Machines, HA clusters, NIC teaming
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
 ! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
interface GigabitEthernet8/17
 description database
 no ip address
 switchport
 switchport access vlan 110
 switchport mode access
 spanning-tree portfast
 ! >> Port Security <<
 ! >> do not use with Virtual Machines, HA clusters, NIC teaming
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
 ! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
interface GigabitEthernet8/18
 description multicast-src
 no ip address
 switchport
 switchport access vlan 5
 switchport mode access
 spanning-tree portfast
 ! >> Port Security <<
 ! >> do not use with Virtual Machines, HA clusters, NIC teaming
 switchport port-security maximum 10
 switchport port-security violation shutdown
 spanning-tree bpduguard enable
 ! >> Disable CDP on server ports <<
 no cdp enable
 no shut
!
interface GigabitEthernet8/25
 description toids1
 no ip address
 switchport
 switchport access vlan 300
 switchport mode access
```

```
 no shut
!
interface GigabitEthernet8/26
 description toids2
 no ip address
 switchport
 switchport access vlan 300
 switchport mode access
 no shut
!
interface GigabitEthernet8/27
 description toids3
 no ip address
 switchport
 switchport access vlan 300
 switchport mode access
 no shut
!
! SVI CONFIGURATION
! =================
!
!
interface Vlan5
 description webapp
 ip address 10.20.5.2 255.255.255.0
 standby 1 ip 10.20.5.1
 standby 1 timers 1 3
 standby 1 priority 120
 standby 1 preempt delay minimum 180
 ! If need directed broadcast:
 ! ip directed-broadcast
 ! mls ip directed-broadcast exclude-router
 no ip unreachables
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 no shut
!
interface Vlan10
 description database
 ip address 10.20.10.2 255.255.255.0
 standby 1 ip 10.20.10.1
 standby 1 timers 1 3
 standby 1 priority 120
 standby 1 preempt delay minimum 180
 ! If need directed broadcast:
 ! ip directed-broadcast
 ! mls ip directed-broadcast exclude-router
 no ip unreachables
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 no shut
!
interface Vlan30
 description l3vlan
 ip address 10.20.30.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
```

```
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
!
interface Vlan13
 description to_core1
 ip address 10.21.0.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 ! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 !
 no shut
!
interface Vlan14
 description to_core2
 ip address 10.21.0.13 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ! >> Disable NTP services <<
 ntp disable
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 0 C1sC0!
 ip ospf network point-to-point
 ! If a CSM is present in the chassis
 ip ospf hello-interval 1
 ip ospf dead-interval 3
 no shut
!
! USE A VLAN NOT A PORT AS MGMT INTERFACE, IN ORDER TO
! SUPPORT OOB MGMT FOR THE SCVS MODULES
!
interface Vlan82
 description mgmt_interface
 ip address 172.28.214.8 255.255.255.0
 ! Do NOT Disable NTP services on the management interface
 no ip redirects
 no ip proxy-arp
 no shut
!
! ROUTING CONFIGURATION
! =====================
!
router ospf 20
  log-adjacency-changes
  auto-cost reference-bandwidth 10000
  area 20 authentication message-digest
  area 20 nssa
  timers throttle spf 1000 1000 1000
!
! Define the N2 routes that you want to leak to the core
! And in the core remember to prevent the N2 from leaking
! into the rest of the network if not necessary
!
  redistribute static subnets route-map redistribute-list
  passive-interface default
```

```
  no passive-interface vlan3
!
! If using L3 links
! no passive-interface TenGigabitEthernet1/1
! no passive-interface TenGigabitEthernet1/2
!
  no passive-interface Vlan13
  no passive-interface Vlan14
!
  network 10.20.5.0 0.0.0.255 area 20
  network 10.20.10.0 0.0.0.255 area 20
  network 10.20.30.0 0.0.0.255 area 20
  network 10.10.0.0 0.0.255.255 area 20
  network 10.10.10.0 0.0.0.255 area 20
  network 10.21.0.0 0.0.255.255 area 20
  exit
!
! REDISTRIBUTION CONTROL
!
route-map redistribute-list
  match ip address 20
  exit
!
! MODIFY THE ACCESS-LIST TO INCLUDE ONLY THE
! NECESSARY STATIC ROUTES
!
access-list 20 deny any
!
!
! FWSM CONFIGURATIONS
! ===================
! DISABLE THE SPAN REFLECTOR IF NOT NEEDED
no monitor session servicemodule
!
firewall multiple-vlan-interfaces
firewall vlan-group 3  5,10,82,105,110,200
firewall module 3 vlan-group 3
!
! SSLSM CONFIGURATIONS
! ====================
!
ssl-proxy module 7 allowed-vlan 82
!
```