Network Security Checklist - Cisco Layer 2 Switch

Version 7, Release 1.6

19 December 2008

Developed by DISA for the DOD

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

NET0180 V0002990 CAT II Non-registered or unauthorized IP addresses.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all public address ranges used on the NIPRNet are properly registered with the .MIL Network Information Center (NIC).

Vulnerability Discussion If network address space is not properly configured, managed, and controlled, the network could be accessed by unauthorized personnel resulting in security compromise of site information and resources. Allowing subscribers onto the network whose IP addresses are not registered with the .Mil NIC may allow unauthorized users access into the network. These unauthorized users could then monitor the network, steal passwords, and access classified information.

Checks

NET Registered IP Address

On NIPRNet connect via the web to www.nic.mil or on SIPRNet connect to nic.smil.mil or www.scc.smil.mil and click on search whois under DISN services. Enter the first three octets of the local site IP range into the keyword search section and then select all categories and submit the request. Verify that the site is registered for the range.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Registered IP Address

The IAO will ensure all users accessing the network have a legitimate need and will submit any unregistered IP addresses to the .Mil Network Information Center (NIC) for registration.

Notes:

NET0185 V0003157 CAT II Unauthorized addresses within SIPRNet enclave

8500.2 IA Control: DCSP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all addresses used within the site's SIPRNet infrastructure are authorized .smil.mil or .sgov.gov addresses that have been registered and assigned to the activity. RFC1918 addresses are not permitted.

Vulnerability Discussion The SIPRNet enclave will have full reachability from SIPRNet Connection Approval Office to perform remote scans.

Checks

NET Sipr RFC1918

Inspect the network topology diagrams as well as all configured router interfaces to determine what addresses are being utilized. Private addresses in accordance with RFC 1918 are not permitted within the SIPRNet enclave.

Default Finding Details The site is using unauthorized addresses within their SIPRNet enclave.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Sipr RFC1918

The IAO will ensure that the site uses only authorized .smil.mil or .sgov.gov addresses that have been registered and assigned to the activity for the SIPRNet.

Notes:

NET0240 V0003143 CAT I Devices exist that have standard default passwords

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all default manufacturer passwords are changed.

Vulnerability Discussion Devices not protected with strong password schemes provide the opportunity for anyone to crack the password thus gaining access to the device and causing network, device, or information damage, or denial of service. Not changing the password in a timely manner increases the likelihood that someone will capture or crack the password and gain unauthorized access to the device.

Checks

NET Password Protection

Interview the network administrator and attempt to logon to several devices.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Password Protection

Ensure all communication devices are in compliance with password policy.

Notes:

NET0340 V0003013 CAT II Warning banner compliance to 8500.2 ECWM-1.

8500.2 IA Control: ECWM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with JTF-GNO CTO 08-008A, Policy on Use of Department of Defense (DoD) Standard Notice and Consent Banner and User Agreement.

Vulnerability Discussion Failure to display the required login banner prior to logon attempts will limit the sites ability to prosecute unauthorized access and also presents the potential to give rise to criminal and civil liability for systems administrators and information systems managers. Not displaying the proper banner will also hamper the sites ability to monitor device usage.

Checks

NET Warning Banners

Have the network administrators sign onto each managed network device to ensure the DoD approved warning banners are displayed at login.

Default Finding Details DOD approved warning banners are not displayed on network managed devices.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Warning Banner

Display the approved DOD login banner prior to a login attempt on all network devices allowing Telnet, File Transfer Protocol (ftp), or Hyper Text Transfer Protocol (http) access.

Notes:

NET0440 V0003966 CAT II Emergency accounts limited to one.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure when an authentication server is used for administrative access to the device, only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).

Vulnerability Discussion Authentication for administrative access to the router is required at all times. A single account can be created on the routers local database for use in an emergency such as when the authentication server is down or connectivity between the router and the authentication server is not operable.

Checks

NET Emergency Account

Base Procedure: Review the running configuration and verify that only one local account has been defined.

NET0440 - CISCO

username xxxxxxx password 7 xxxxxxxxxxx

Default Finding Details More than one local account has been defined to the router.

The username and password is not stored in a sealed envelope kept in a safe.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Emergency Account

Insure that only one local account has been defined on the router and store the username and password in a secured manner.

Notes:

NET0441 V0015434 CAT I Emergency account privilege level is not set

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the emergency account defaults to the lowest authorization level and the password is in a locked safe.

Vulnerability Discussion The emergency account must be protected by the IAO in a protected safe and assigned the lowest privilege level.

Checks

NET emergency Acct privilege

The default CISCO privilege level 1 should be explicitly overriden with level 0. Level 0 allows the enable command to be executed. The CISCO example below details how this can be set up:

username emergency-acct privilege 0 password Xx1!abcd

DEFAULTS:
Privilege Level 0 Includes the disable, enable, exit, help, and logout commands

Privilege Level 1 Includes all user-level commands at the router> prompt

Privilege Level 15 Includes all enable-level commands at the router# prompt

Default Finding Details Emergency account privilege level is not set to lowest privilege level.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Emergency Acct privileges

Configure the emergency account with the lowest privilege level. The user using this account should be able to use the enable command. If the user knows the enable secret password, recovery and/or admistrative privileges should work.

Notes:

NET0460 V0003056 CAT I Group accounts or user accounts without passwords

8500.2 IA Control: IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure each user accessing the device locally have their own account with username and password.

Vulnerability Discussion Without passwords on user accounts, one level of complexity is removed from gaining access to the network device. If a default userid has not been changed or is guessed by an attacker, the network could be easily compromised as the only remaining step would be to crack the password.

Sharing group accounts on any device is strictly prohibited. If these group accounts are not changed when someone leaves the group, that person could possibly gain control of the network device. Having group accounts does not allow for proper auditing of who is accessing or changing the network.

Checks

NET Group Accounts

Review configuration for local accounts. If an authentication server is being used, examine those accounts with access to the device.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Group Accounts

The SA will ensure that all user accounts without passwords are removed.

The administrator will ensure that individual user accounts are created for each authorized administrator. The IAO will ensure that any group or duplicate account will be removed.

Notes:

NET0465 V0003057 CAT II Assign lowest privilege level to user accounts.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.

Vulnerability Discussion By not restricting administrators and operations personnel to their proper privilege levels, access to restricted functions may be allowed before they are trained or experienced enough to use those functions. Network disruptions or outages could be caused by mistakes made by inexperienced administrators.

Checks

NET Lowest Privilege Level

BASE Procedure: The levels can be mapped to commands, which have set privilege levels--or you can reassign levels to commands. Usernames with corresponding passwords can be set to a specific level.

Default Finding Details The following user accounts exist that are assigned higher privilege levels than are required for the performance of the users duties:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Lowest Privilege Level

The administrator will assign accounts with the least privilege rule. Each user will have access to only the privileges they require to perform their respective duties. Access to the highest privilege levels should be restricted to a few users.

Notes:

NET0470 V0003058 CAT II Unnecessary or unauthorized accounts exist.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will immediately have accounts removed from the authentication server or device, which are no longer required.

Vulnerability Discussion Allowing unnecessary or unauthorized accounts may allow for them to be compromised by unauthorized users who could then gain full control of the device. Denial of service, interception of sensitive information or other destructive actions could then take place.

Checks

NET Account Administration

Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts defined locally or in the authentication server.

Default Finding Details The following unnecessary or unauthorized accounts exist on the router:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Account Administration

The administrator will ensure that procedures are in place to enforce proper account administration. The administrator will ensure that any account that is no longer needed will be disabled or removed from the system.

Notes:

NET0700 V0003160 CAT II Minimum operating system release level

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will implement the latest stable operating system on each device IAW the current Network Infrastructure Security Checklist.

Vulnerability Discussion Network devices that are not running the latest tested and approved versions of software are vulnerable to network attacks. Running the most current, approved version of system and device software helps the site maintain a stable base of security fixes and patches, as well as enhancements to IP security. Viruses, denial of service attacks, system weaknesses, back doors and other potentially harmful situations could render a system vulnerable, allowing unauthorized access to DoD assets.

Checks

NET OS Current

Base Procedure

Have the SA display the OS version currently in operation. Verify the release is not End of Life. The OS must be current with related fixes and patches.

NET0700 - CISCO

Have the router administrator execute the show version command on all of the Cisco routers to verify that the installed IOS version.
Base Release 12.4(7) is current with a migration path to 12.4(10). Software Major Release 12.4(10) was posted to CCO 14 March 2006.

T Family Release; 12.4(6)T7 is current with a migration path 12.4(11)T1.

You will find in some cases version 12.2 is the most current version, typically in the CAT IOS switch family.

12.2(18) - 12.2(44) are a range to be considered. Pending the platform. Example: 12.2(18)SX is current (Aug 2007) with a migration path 12.2(33)SXH March 2008.)

These various 12.2 platforms are to large in number to list, however the procedure is to review the IOS releases available and ensure the version is current to avoid IAVM open findings. The recommendation is to have the latest IOS or one version prior to the current version.

Default Finding Details Base Release - 12.4(7) or later has not been implemented.
T Family Release - 12.4(6)T7 or later has not been implemented.

12.2(18) - 12.2(44) are required to mitigate CISCO IAVMs. The 12.2 release varies pending the platform. A recommended release is one older than the current for the particular 12.2 platform. Reference the CISCO site for details of available releases.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET OS Current

Later OS Software releases contain vulnerabilities which may not have been addressed in current versions.

Operating Systems are not IAW with Network Infrastructure Security Checklist

Update Operating Systems on all routers.

Notes:

NET0810 V0003019 CAT III Two NTP servers have not been specified

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the enclave has two Network Time Protocol (NTP) servers defined to synchronize time.

Vulnerability Discussion Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers, you will find it very hard to develop a reliable picture of an incident.

Checks

NET NTP - Two required

Base Procedure: Review the router configurations and verify that NTP servers have been defined.

NET0810 - CISCO

ntp update-calendar
ntp server 129.237.32.2
ntp server 142.181.31.6

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually drift, and the software clock and hardware clock will become out of synch with each other. The ntp update-calendar command will enable the hardware clock to be periodically updated with the time specified by the NTP source. CAVEAT: Since IOS uses the software clock for logging, synching the hardware clock is not a requirement—only a best practice. Lower end models such as 2500/2600 series do not have hardware clocks, so this command is not available on those platforms.

Default Finding Details The router is not configured to accept NTP messages from two authorized NTP servers.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET NTP Two requireed

Specify two NTP server IP addresses on the routers to prevent NTP messages from being received from non-authorized sources.

Notes:

NET0894 V0003969 CAT II SNMP write access to the router is enabled.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.

Vulnerability Discussion Enabling write access to the router via SNMP provides a mechanism that can be exploited by an attacker to set configuration variables that can disrupt network operations.

Checks

NET SNMP Read/Write Access

Base Procedure: Review all configurations to ensure SNMP access from the network management stations is read only.

NET0894 - CISCO

The configuration should look similar to the following:

```
access-list 10 permit host 7.7.7.5
snmp-server community xxxxxxxxx ro 10
```

Default Finding Details Write access to the router via SNMP is enabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SNMP Read/Write Access

Disable SNMP write access to the router.

Notes:

NET0990 V0017820 CAT II OOBM switch not connected to the NE OOBM interface

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The OOBM access switch is not physically connected to the managed network element OOBM interface.

Vulnerability Discussion The OOBM access switch will connect to the management interface of the managed network elements. The management interface of the managed network element must be directly connected to the OOBM network to ensure seperation. An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device.

Checks

NET0990

Examine the connection from the OOBM access switch to the managed network elements. Verify which interface is being used at the managed network elements so that it can be determined if the interface is a true OOBM interface.

Default Finding Details The OOBM access switch is not physically connected to the managed network element OOBM interface.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET0990

Physically connected the OOBM access switch to the managed network element OOBM interface.

Notes:

NET0994 V0017824 CAT II Management interface is assigned to a user VLAN.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The management interface is an access switchport and has not been assigned to a separate management VLAN.

Vulnerability Discussion The OOBM access switch will connect to the management interface of the managed network elements. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network element will be directly connected to the OOBM network. If the device does not have an OOBM port, the interface functioning as the management interface must be configured so that management traffic does not leak into the managed network and that production traffic does not leak into the management network.

Checks

NET0994 - CISCO

Review the managed switch configuration and verify that the access port connected to the OOBM access switch has been assigned to the management VLAN. By default, the management VLAN is VLAN 1; however, the management VLAN must be configured to a different VLAN. As shown in the following configuration example, FastEthernet0/1 is the port connected to the OOBM access switch and VLAN 101 is the management VLAN.

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 2
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 2
 switchport mode access
```

This can also be verified by entering a Privileged EXEC show vlan command on the switch CLI as illustrated in the following example output of a Cisco 2950:

```
2950#show vlan
VLAN Name                Status    Ports
---- ------------------------- --------- -------------------------------
2    Production          active    Fa0/2, Fa0/3, Fa0/4, Fa0/5,
                                   ...
                                   Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   Management          active    Fa0/1
```

Default Finding Details The management interface is an access switchport and has not been assigned to a separate management VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET0994

If the management interface is an access switchport, assign it to a separate management VLAN while the remainder of the access switchports can be assigned to user VLANs belonging to the managed network. This provides some level of separation between the management network and the managed network.

Notes:

NET0995 V0017825 CAT III Management VLAN has invalid addresses

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability An address has not been configured for the management VLAN from space belonging to the OOBM network assigned to that site.

Vulnerability Discussion The OOBM access switch will connect to the management interface of the managed network elements. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network element will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device.

Checks

NET0995 - CISCO

Review the managed switch configuration and verify that an address has been configured for management VLAN from space belonging to the OOBM network that has been assigned to that site.

```
interface VLAN10
 ip address 10.1.1.10 255.255.255.0
 description Management VLAN
```

Note: The IP address of the switch can be accessed only by nodes connected to ports that belong to the management VLAN.

A default gateway address as shown below must be configured using the address of the OOBM gateway router interface connecting to the OOBM access switch. This will ensure that all management traffic is forwarded toward the NOC using the switchport attached to the OOBM access switch.

```
ip default-gateway 10.1.1.1
```

Default Finding Details An address has not been configured for the management VLAN from space belonging to the OOBM network assigned to that site.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET0995

Assign an IP address to the management VLAN from the address space belonging to the OOBM network.

Notes:

NET0996 V0017826 CAT II Invalid ports with membership to the mgmt VLAN

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The access switchport connecting to the OOBM access switch is not the only port with membership to the management VLAN.

Vulnerability Discussion The OOBM access switch will connect to the management interface of the managed network elements. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network element will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device.

Checks

NET0996 - CISCO

The management VLAN must be pruned from any VLAN trunk links belonging to the managed network's infrastructure. By default all the VLANs that exist on a switch are active on a trunk link. Since the switch is being managed via OOBM connection, management traffic should not traverse any trunk links. The following Catalyst IOS configuration is an example of a trunk link with the management VLAN (i.e. 10) pruned from a trunk.

```
interface fastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode dynamic desirable
 switchport trunk native vlan 3
 switchport trunk allowed vlan 2-9
```

This can also be verified with the show interface trunk command as shown below:

```
Switch-A# show interface trunk
Port     Mode         Encapsulation  Status        Native vlan
Fa0/1    desirable    802.1q         trunking      3
Port     Vlans allowed on trunk
Fa0/1    2-9
Port     Vlans in spanning tree forwarding state and not pruned
Fa0/1    2-5
```

Note: VTP pruning allows the switch to not forward user traffic for VLANs that are not active on a remote switch. This feature dynamically prunes unneeded traffic across trunk links. VTP pruning needs to be enabled on the server for the VTP domains—after which all VTP clients in the VTP domain will automatically enable VTP pruning. To enable VTP pruning on a Cisco IOS switch, you use the vtp pruning VLAN configuration or global configuration command. Since, the management VLAN will be active on all managed switchs, VTP will never prune this VLAN. Hence, it will have to be manually removed as shown above.

Default Finding Details The access switchport connecting to the OOBM access switch is not the only port with membership to the management VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET0996

Ensure that the access switchport connecting to the OOBM access switch is the only port with membership to the management VLAN

Notes:

NET0997 V0017827 CAT III The management VLAN is not pruned from trunk links

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The management VLAN is not pruned from any VLAN trunk links belonging to the managed network's infrastructure.

Vulnerability Discussion The OOBM access switch will connect to the management interface of the managed network elements. The management interface can be a true OOBM interface or a standard interface functioning as the management interface. In either case, the management interface of the managed network element will be directly connected to the OOBM network.

An OOBM interface does not forward transit traffic; thereby, providing complete separation of production and management traffic. Since all management traffic is immediately forwarded into the management network, it is not exposed to possible tampering. The separation also ensures that congestion or failures in the managed network do not affect the management of the device. If the device does not have an OOBM port, the interface functioning as the management interface must be configured so that management traffic does not leak into the managed network and that production traffic does not leak into the management network. ISL and 802.1q trunking enables multiple VLANs to traverse the same physical links between layer 2 switches or between a layer 2 switch and a router. If the management VLAN is not pruned from any VLAN trunk links belonging to the managed network's infrastructure, management traffic has the potential to leak into the production network.

Checks

NET0997 - CISCO

The management VLAN must be pruned from any VLAN trunk links belonging to the managed network's infrastructure. By default all the VLANs that exist on a switch are active on a trunk link. Since the switch is being managed via OOBM connection, management traffic should not traverse any trunk links. The following Catalyst IOS configuration is an example of a trunk link with the management VLAN (i.e. 10) pruned from a trunk.

```
interface fastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode dynamic desirable
 switchport trunk native vlan 3
 switchport trunk allowed vlan 2-9
```

This can also be verified with the show interface trunk command as shown below:

```
Switch-A# show interface trunk
Port     Mode         Encapsulation  Status       Native vlan
Fa0/1    desirable    802.1q         trunking     3
Port     Vlans allowed on trunk
Fa0/1    2-9
Port     Vlans in spanning tree forwarding state and not pruned
Fa0/1    2-5
```

Note: VTP pruning allows the switch to not forward user traffic for VLANs that are not active on a remote switch. This feature dynamically prunes unneeded traffic across trunk links. VTP pruning needs to be enabled on the server for the VTP domains—after which all VTP clients in the VTP domain will automatically enable VTP pruning. To enable VTP pruning on a Cisco IOS switch, you use the vtp pruning VLAN configuration or global configuration command. Since, the management VLAN will be active on all managed switchs, VTP will never prune this VLAN. Hence, it will have to be manually removed as shown above.

Default Finding Details The management VLAN is not pruned from any VLAN trunk links belonging to the managed network's infrastructure.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET0997

Prune the management VLAN from any VLAN trunk links belonging to the managed network's infrastructure.

Notes:

NET1003 V0017832 CAT II Mgmt VLAN does not have correct IP address

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The management VLAN is not configured with an IP address from the management network address block.

Vulnerability Discussion If the management systems reside within the same layer 2 switching domain as the managed network elements, then separate VLANs will be deployed to provide separation at that level. In this case, the management network still has its own subnet while at the same time it is defined as a unique VLAN.

Checks

NET1003

Review the switch configuration and verify that the management VLAN has been assigned an IP address from the management network address block. Following is an example for a Cisco Catalyst switch:

```
interface VLAN 10
 description Management VLAN
 ip address 10.1.1.10 255.255.255.0
```

Note: The IP address of the switch can be accessed only by nodes connected to ports that belong to the management VLAN.

Default Finding Details The management VLAN is not configured with an IP address from the management network address block.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET1003

Configure the management VLAN with an IP address from the management network address block.

Notes:

NET1004 V0017833 CAT II No ingress ACL on management VLAN interface

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability An inbound ACL for the management network VLAN interface is not configured on the MLS used to provide inter-VLAN routing.

Vulnerability Discussion If the management systems reside within the same layer 2 switching domain as the managed network elements, then separate VLANs will be deployed to provide separation at that level. In this case, the management network still has its own subnet while at the same time it is defined as a unique VLAN. inter-VLAN routing or the routing of traffic between nodes residing in different subnets requires a router or multi-layer switch (MLS). Access control lists must be used to enforce the boundaries between the management network and the network being managed.

Checks

NET1004

Review the MLS configuration and verify that an inbound ACL has been configured for the management VLAN interface to block non-management traffic. The following example for a Cisco Catalyst multi-layer switch:

```
interface VLAN 10
 description Management VLAN
 ip address 10.1.1.1 255.255.255.0
 ip access-group 108 in
!
access-list 108 permit …
```

Default Finding Details An inbound ACL for the management network VLAN interface is not configured on the MLS used to provide inter-VLAN routing.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET1004

If an MLS is used to provide inter-VLAN routing, configure an inbound ACL for the management network VLAN interface.

Notes:

NET1021 V0004584 CAT III Router must log severity levels.

8500.2 IA Control: ECAT-1, ECAT-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will configure all devices to log severity levels 0 through 7 and send log data to a syslog server.

Vulnerability Discussion Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Syslog levels 0-7 are the levels required to collect the necessary information to help in the recovery process.

Checks

NET Log Severity Levels

Base Procedure: Review all router configurations to ensure that all routers log messages for severity levels 0 through 7.

Logging
Level Severity Level Description
Emergencies 0
Alerts 1 Immediate Action Required
Critical 2 Critical Conditions
Errors 3 Error Conditions
Warnings 4 Warning Conditions
Notifications 5 Normal but Significant Conditions
Informational 6 Informational Messages
Debugging 7 Debugging Messages

Default Finding Details The router is not configured to log message severity levels 0-7 or the router is not configured to send syslog messages to the syslog server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Log Severity Levels

The router administrator will configure the router to log message severity levels 0-7 and send syslog messages to the syslog server.

Notes:

NET1365 V0005642 CAT II More than one emergency account has been defined.

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that when an authentication server is used for administrative access to the switch, only one account can be defined locally on the switch for use in an emergency (i.e., authentication server or connection to the server is down).

Vulnerability Discussion Authentication for administrative access to the switch is required at all times. A single account can be created on the switchs local database for use in an emergency such as when the authentication server is down or connectivity between the switch and the authentication server is not operable.

Checks

NET SW Local Accounts

Reference procedure guide

Default Finding Details More than one local account has been defined to the switch.

The username and password is not stored in a sealed envelope kept in a safe.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Local Accounts

Ensure that only one local account has been defined on the switch and store the username and password in a secured manner.

Notes:

NET1410 V0005628 CAT II The VLAN1 is being used for management traffic.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure VLAN1 is not used for in-band management traffic. The IAO/NSO will assign a dedicated management VLAN to keep management traffic separate from user data and control plane traffic.

Vulnerability Discussion All ports, including the internal sc0 interface, are configured by default to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Checks

NET SW VLAN1 In-Band MGT

If switch clustering is used, review the configuration of the VLAN command switch and look for the command cluster management-vlan. The new management VLAN ID follows this command.

For unclustered switches, review the configuration of each switch. All ports, including the internal management interface (sc0), are configured by default to be members of VLAN 1. The management VLAN can be identified by its switch virtual interface (SVI) defined that contains the IP address for the internal management interface. Note the IP address defined for the sc0 interface. The IP address of the sc0 interface can be accessed only by hosts connected to ports that belong to the management VLAN. Below is an example of disabling VLAN 1 and creating an SVI that could be used for the management VLAN.

```
interface VLAN1
no ip address
shutdown
interface VLAN10
ip address 10.0.1.10 255.255.255.0
no shutdown
```

Note: The management VLAN can also be defined by the set command when configuring the IP address of the Sc0.

```
set interface sc0 10.0.1.10 255.255.255.0
```

Default Finding Details VLAN 1 is being used for in-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW VLAN1 In-Band MGT

Best practices for VLAN-based networks is create a dedicated management VLAN, prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

Notes:

NET1411 V0003970 CAT II The management VLAN is not secured.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the management VLAN is not configured on any trunk or access port that does not require it.

Vulnerability Discussion All ports, including the internal sc0 interface, are configured by default to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Checks

NET SW Mgt VLAN restrict use

Review the switch configurations and note any ports assigned to the management VLAN. Only ports that should belong to the management VLAN are the trunk ports and the access ports of the switch administrator. It is possible that not all trunk ports need to belong to the management VLAN—trunk traffic is only required from the switches that have management workstations attached.

Default Finding Details The management VLAN is configured on unnecessary trunk.

The management VLAN is configured on unnecessary access port.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Mgt VLAN restrict use

Best practices for VLAN-based networks is create a dedicated management VLAN, prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

Notes:

NET1412 V0003971 CAT II VLAN 1 is being used as a user VLAN.

8500.2 IA Control:

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure VLAN1 is not used for user VLANs.

Vulnerability Discussion In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

Checks

NET SW VLAN1 Shutdown

Review the switch configurations and verify that no access ports have been assigned membership to the VLAN 1. A good method of ensuring there is not membership to VLAN 1 is to have the following configured:

```
interface VLAN1
no ip address
shutdown
```

This technique does not prevent switch control plane protocols such as CDP, DTP, VTP, and PAgP from using VLAN 1.

A show vlan 1 command can be used to verify what ports are assigned to VLAN 1.

Default Finding Details VLAN 1 is being used as a user VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW VLAN1 Shutdown

Best practices for VLAN-based networks is to prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

Notes:

NET1413 V0003972 CAT III VLAN 1 traffic traverses across unnecessary trunk

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure VLAN1 is pruned from all trunk and access ports that do not require it.

Vulnerability Discussion VLAN 1 is a special VLAN that tags and handles most of the control plane traffic such as Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all VLAN 1 tagged traffic. VLAN 1 is enabled on all trunks and ports by default. With larger campus networks, care needs to be taken about the diameter of the VLAN 1 STP domain; instability in one part of the network could affect VLAN 1, thereby influencing control-plane stability and therefore STP stability for all other VLANs.

Checks

NET SW VLAN1 Port Useage

Review the switch configurations and note any ports assigned to VLAN 1. A show vlan command can also be used to verify what ports are assigned to VLAN 1.

Default Finding Details VLAN 1 traffic traverses across unnecessary trunk links.

VLAN 1 is configured on unnecessary access ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW VLAN1 Port Useage

Best practice for VLAN-based networks is to prune unnecessary ports from gaining access to VLAN1 and insure that it does not traverse trunks not requiring VLAN1 traffic.

Notes:

NET1416 V0005623 CAT II Ensure trunking is disabled on all access ports.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure trunking is disabled on all access ports (do not configure trunk on, desirable, non-negotiate, or auto—only off).

Vulnerability Discussion Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victims MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attackers VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victims VLAN ID is used by the switch as the next hop and sent out the trunk port.

Checks

NET SW Trunking on Access Port

Review the switch configurations and examine all access ports. Verify that the port is not in trunk mode (i.e. for Catalyst using IOS the interface should have the command switchport mode access—not switchport mode trunk or older switches trunk off and not trunk on). A show trunk command can also be used to display all ports in trunk mode. Trace the connections from the physical port with trunk mode. This should be a Gigabit Ethernet or Fast Ethernet connection to another switch or router—it should not be connected to a workstation.

Default Finding Details Trunk mode is configured on access ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Trunking on Access Port

Disable trunking on all access ports.

Notes:

NET1417 V0005622 CAT II A dedicated VLAN is required for all trunk ports.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure when trunking is necessary; a dedicated VLAN is configured for all trunk ports.

Vulnerability Discussion Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victims MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attackers VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victims VLAN ID is used by the switch as the next hop and sent out the trunk port.

Checks

NET SW Trunk Dedicated VLAN

Review the switch configurations and examine all trunk ports. Verify that they belong to their own VLAN. Following is an example of assigning a trunk port to a VLAN:

```
interface FastEthernet0/23
description Trunk Port
no ip address
no cdp enable
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native
vlan 55
no shutdown
```

A show vlan command can also be used to verify what VLAN the trunked ports are assigned to.

Default Finding Details A dedicated VLAN is not configured for trunking.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Trunk Dedicated VLAN

To ensure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

Notes:

NET1418 V0003984 CAT II Access ports are assigned to the trunk VLAN.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure access ports are not assigned to the dedicated trunk VLAN.

Vulnerability Discussion Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

Checks

NET SW Access Port restriction

Review the switch configurations and examine all access ports. Verify that they do not belong to the trunk VLAN.

Default Finding Details Access ports are assigned to the dedicated trunk VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Access Port restriction

To insure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

Notes:

NET1434 V0007542 CAT II Switch Access Control SRV using weak EAP protocol

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure when utilizing 802.1X, a secure EAP type (EAP-TLS, EAP-TTLS or PEAP) resides on the authentication sever and within the operating system or application software on the client devices.

Vulnerability Discussion EAP methods/types are continually being proposed, however, the three being considered secure are EAP-TLS, EAP-TTLS, and PEAP.

PEAP is the preferred EAP type to be used in DoD because of its ability to support a greater number of operating systems and its capability to transmit statement of health information, per NSA NAC study.

Lightweight EAP (LEAP) is a CISCO proprietary protocol providing an easy-to-deploy one password authentication. LEAP is vulnerable to dictionary attacks. A "man in the middle" can capture traffic, identify a password, and then use it to access a WLAN. LEAP is inappropriate and does not provide sufficient security for use on DOD networks.

EAP-MD5 is functionally similar to CHAP and is susceptible to eavesdropping because the password credentials are sent as a hash (not encrypted). In addition, server administrators would be required to store unencrypted passwords on their servers violating other security policies. EAP-MD5 is inappropriate and does not provide sufficient security for use on DOD networks.

Checks

NET SW EAP Type not Secure

Have the switch administrator identify the Access Control Server providing the authentication. Typically these have a GUI interface. Verify the server is not using a vulnerable EAP type as described in the STIG.

PEAP is the preferred EAP type to be used in DoD because of its ability to support a greater number of operating systems and its capability to transmit statement of health information. Per NSA NAC study.

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW EAP Type not Secure

Have the switch administrator use a EAP type as described in the STIG.

Notes:

NET1435 V0003973 CAT III Disabled ports are not kept in an unused VLAN.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure disabled ports are placed in an unused VLAN (do not use VLAN1).

Vulnerability Discussion It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.

Checks

NET SW Disabled Ports

Review the switch configurations and examine all interfaces. Each interface not in use should have membership to a VLAN that is not used for any other purpose. Below would be an example.interface FastEthernet0/5switchport mode accessswitchport access vlan 999shutdownFor older switches such as the Catalyst 1900, you would see something like the following:interface FastEthernet0/5vlan-membership static 999shutdown

Default Finding Details Disabled ports are not kept in an unused VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Disabled Ports

Assign all disabled ports to an unused VLAN. Do not use VLAN1.

Notes:

NET1436 V0005626 CAT I Wall Jack is not secured by switch configuration.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure wall jacks are secured with MAC address definitions on switch ports or 802.1X port authentication is used on all access ports.

Vulnerability Discussion Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

Checks

NET SW Port Security or 802.1x

Determine if the site is using 802.1x authentication or a MAC address filtering. If the enclave implementation uses only MAC filtering inspect the wall plates and determine if the communication ports are enclosed by security boxes such as the Hoffman box . If the area is not approved Open Storage the box is required. The MAC filtering or 802.1x requirement is required regardless of the area classification. Notify the Traditional review when 802.1x is not implemented.

1) Physical security (ISS - 240: CAT I) is not a mitigation for port authentication (802.1x) or MAC filtering as defined in (NET1436: CAT 1). If the enclave has 802.1x implemented than mark as not a finding. If the site has Mac filtering implemented proceed to step 2.

2) Physical security (ISS - 240: CAT I) remains a requirement when MAC filtering is implemented instead of port authentication (802.1x) as defined in (NET1436: CAT 1). The key word is MAC filtering. If the enclave has MAC filtering implemented without 802.1x, than the physical security requirement (ISS - 240) remains a required safeguard if the area is not certified as Open Storage Secret. Communicate with the Traditional review.

MAC Filtering examples:

Catalyst Procedure: Port Security: Have the switch administrator issue a show port [mod[/port]] or look for the following command. set port security 2/1 enable

IOS Procedure: 802.1x: Having the switch administrator issue a show port [mod[/port]] will also provide the detail.

```
aaa new-model
aaa authentication dot1x
default group radius
dot1x system-auth-control

interface fastethernet 5/1
dot1x port-control auto
```

Default Finding Details Switch port filtering via MAC addresses or 802.1x is not implemented on all access ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Port Security or 802.1x

Enable Port Security or 802.1x on all switch ports.

Notes:

NET1438 V0004608 CAT II 802.1x ports must start in unauthorized state.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure if 802.1X Port Authentication is implemented, all access ports start in the unauthorized state.

Vulnerability Discussion Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

Checks

NET SW Port Unauth State

802.1 Security: Have the switch administrator issue a show dot1x all or look for the following command.

dot1x port-control force-unauthorized

Default Finding Details 802.1x access ports are not configured in an unauthorized initial configuration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW Port Unauth State

Configure the 802.1x ports to come up with an unauthorized initial status.

Notes:

NET1439 V0005624 CAT II Re-authentication must occur every 60 minutes.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure if 802.1x Port Authentication is implemented, re-authentication must occur every 60 minutes.

Vulnerability Discussion Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

Checks

NET SW 802.1x Reauthenticate

802.1 Security: Review the switch configuration for the following command.
dot1x re-authenticate [interface interface-id]

Default Finding Details 802.1x access ports are not configured for Re-authentication every 60 minutes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SW 802.1x Reauthenticate

Ensure 802.1x reauthentication occurs every 60 minutes.

Notes:

NET1623 V0004582 CAT I Devices are not password protected for out-of-band

8500.2 IA Control: IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all OOB management connections to the device require passwords.

Vulnerability Discussion Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

Checks

NET OOB PSW Protected

Base Procedure: Verify the console port and the aux ports used by the OOBM network are restricted by passwords.

NET1623 - CISCO

The console port and the aux ports used by the OOBM network should look similar to the following example; however the authentication list could default to the AAA method-list “default” on the aux port. The aaa new-model command immediately applies local authentication to all lines and interfaces (except console line; line con 0).

```
login authentication admin_only
exec-timeout 10 0
transport input ssh
```

Default Finding Details Access to the console does not require a password.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET OOB PSW Protected

The site will ensure that all out-of-band management connections to the device have passwords.

Notes:

NET1624 V0003967 CAT II Console port is not configured to timeout-10 min

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure the console port is configured to time out after 10 minutes or less of inactivity.

Vulnerability Discussion Routers have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to fifteen minutes or less increases the level of protection afforded critical routers.

Checks

NET OOB Timeout

Base Procedure: Ensure the console port is configured to time out after 10 minutes or less of inactivity.

NET1624 - CISCO

Note: The default is 10 minutes and may not appear in the display of the configuration. The Con port should contain the following command:
exec-timeout 10 0

Default Finding Details The console port is not configured to timeout after 10 minutes of inactivity.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET OOB Timeout

The system administrator will ensure that the timeout for unattended console port is set for no longer than 10 minutes.

Notes:

NET1636 V0003175 CAT I In-band management connections require passwords

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all in-band management connections to the router require passwords.

Vulnerability Discussion Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

Checks

NET In-band PSW Protected

Review each device's configuration to ensure that SA login is prompted for authentication.

NET1636 - CISCO

The vty ports should look similar to the following example; however the authentication list could default to the AAA method-list "default" on the aux port. The aaa new-model command immediately applies local authentication to all lines and interfaces.The configuration should look similar to the following:

```
line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh
```

Default Finding Details Routers are not password protected for in-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET In-band PSW Protected

The site will ensure that all in-band management connections require passwords.

Notes:

NET1637 V0005611 CAT II In-band management is not filtered

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure that the device only allows in-band management sessions from authorized IP addresses from the internal network.

Vulnerability Discussion Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment, can acquire the router account and password information. With this intercepted information they could gain access to the router and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

Checks

NET In-band from Auth IP Addr

Base Procedure: Review all router configurations and verify that only authorized internal connections are allowed on Inband management ports.

NET1637 - CISCO

The configuration should look similar to the following on the VTY interface:
access-list 3 permit 192.168.1.10 log
access-list 3 permit 192.168.1.11 log
access-list 3 deny any
…..
line vty 0 4
access-class 3 in

Default Finding Details ACLs are not in place to restrict access to the VTY ports to authorized users.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET In-band Auth IP Addr

The router administrator will create an ACL for each router that restricts the use of VTY ports for remote router administration, to only authorized internal connections.

Notes:

NET1638 V0003069 CAT II Inband traffic must be secured by FIPS requirement

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure in-band management access to the device is secured using FIPS 140-2 approved encryption or hash algorithms such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment can acquire the router account and password information. With this intercepted information they could gain access to the router and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

Checks

NET encrypt inband sessions

Base Procedure: Review the Inband management interfaces and determine if the access to the device is encrypted as required.

NET1638 - CISCO

The configuration should look similar to the following:
line vty 0 4
transport input ssh

Default Finding Details FIPS compliant encryption or Hash such as SSH is not being used to access the router through VTY ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET encrypt inband sessions

The router administrator will ensure that only SSH connections are allowed to access VTY ports.

Notes:

NET1639 V0003014 CAT II In-band Mgt not configured to timeout in 10 min.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.

Vulnerability Discussion Routers have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to ten minutes or less increases the level of protection afforded critical routers.

Checks

NET In-band Timeout 10 min

Base Procedure: Review the SA access to manage the device. Ensure the device is configured to time-out in 10 minutes or less.

NEt1639

Note: The default is 10 minutes and may not appear in the display of the configuration. The VTY ports should contain the following command:
exec-timeout 10

Default Finding Details The timeout for in-band management access is set for longer than 10 minutes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET In-band Timeout 10 min

The SA will ensure that the timeout for unattended telnet is no longer than 10 minutes.

Notes:

NET1640 V0003070 CAT III Log all in-band management access attempts

8500.2 IA Control: ECAT-1, ECAT-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.

Vulnerability Discussion Audit logs are necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

Checks

NET In-band Logging

Base Procedure: Review each configuration to ensure that all attempts to access the device are logged.

NET1640 - CISCO

Review each Cisco router configuration to ensure that all connection attempts to the VTY ports are logged.

```
access-list 3 permit 192.168.1.10 log
access-list 3 permit 192.168.1.11 log
access-list 3 deny any log
.
line vty 0 4
access-class 3 in
```

Default Finding Details The log parameter is not being used to log access to the VTY ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Inband Logging

The system administrator will configure the device to log all access to the device.

Notes:

NET1645 V0005612 CAT II Secure Shell timeout is not 60 seconds or less

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.

Vulnerability Discussion Reducing the broken telnet session expiration time to 60 seconds or less strengthens the router from being attacked by use of an expired session.

Checks

NET SSH Timeout 60 sec

Base Procedure: Review the configuration or have the system administrator verify the timeout is set for 60 seconds or less. The SSH server terminates the connection if protocol negotiation—including user authentication—is not complete within this timeout.

NEt1645 - CISCO

ip ssh time-out 60

Default Finding Details Expired Secure Shell sessions dont expire in 60 seconds or less.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SSH Timeout 60 sec

Implement Secure Shell Timeout.

Notes:

NET1646 V0005613 CAT II SSH login attempts value is greater than 3

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.

Vulnerability Discussion Setting the authentication retry to 3 or less strengthens against a Brute Force attack.

Checks

NET SSH Login Attempts

Base Procedure: Review the configuration or have the syetem administrator verify the authentication retry is set for 3.

NET1646 - CISCO

ip ssh authentication-retries 3

Default Finding Details Secure shell Authentication Retry set greater than 3.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SSH Login Attempts

Implement Secure Shell Authentication retries.

Notes:

NET1647 V0014717 CAT II SSH version 2 is not implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure SSH version 2 is implemented.

Vulnerability Discussion SSH Version 1 is a protocol that has never been defined in a standard. Since SSH-1 has inherent design flaws which make it vulnerable to, e.g., man-in-the-middle attacks, it is now generally considered obsolete and should be avoided by explicitly disabling fallback to SSH-1.

Checks

NET SSH V2

Base Procedure: Review the configuration and verify controls are in place to ensure the use of SSH v2.

NET1647 - CISCO

To prevent the management session from falling back to the undefined protocol (Version 1), you must use the “ip ssh version” command and specify Version 2.
ip ssh version 2

Default Finding Details SSH version 2 is not implemented .

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SSH V2

Implement version 2 of SSH.

Notes:

NET1660 V0003196 CAT I An insecure version of SNMP is being used.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the SNMP Version 3 Security Model (FIPS 140-2 compliant algorithms such as both SHA-1 packet authentication and AES encryption of the PDU) is used across the entire network infrastructure.

Vulnerability Discussion SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an attacker or other unauthorized user may gain access to detailed network management information and use that information to launch attacks against the network.

Checks

NET SNMP Version

Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category II.

To verify the appropriate patches on CISCO devices: Check IAVMs associated with SNMP. As of 11/01/2007 there were four (V0005835, V0005809, V0005942, V0012769).

To verify the appropriate patches on other vendors: Reference this website: http://www.cert.org/advisories/CA-2002-03.html

Default Finding Details SNMP V1 or V2 has been enabled on the network infrastructure.

SNMP V3 has been enabled on the network infrastructure without the V3 User-based Security Model authentication and privacy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SNMP Version

The NSO will ensure that the SNMP Version 3 Security Model (FIPS 140-2 compliant such as, both SHA-1 packet authentication and AES encryption of the PDU) will be used across the entire network infrastructure.

Notes:

NET1665 V0003210 CAT I System community names or usernames use defaults

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all SNMP community strings are changed from the default values.

Vulnerability Discussion Community strings default to the name PUBLIC. This is known by those wishing to exert an attack against the devices in the network. This must be changed to something that is in compliance with DISA password guidelines. Not all individuals need write access to the device. Compromising the read password will have less of an impact if it cannot be used to change information. An erroneous message being sent to the NMS can cause network managers to act inappropriately in responding to an alarm or warning. It is important that the information being received is from valid managed devices.

Checks

NET SNMP Community Strings

Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

Default Finding Details

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SNMP Community Strings

Most network management systems (NMSs) default to a community sign on name of public. This community name will be changed to something that is not easily guessed. It will be protected in the same way as any password is protected.

Notes:

NET1675 V0003043 CAT II Exclusive use of privileged and non-privileged

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

Vulnerability Discussion Numerous vulnerabilities exist with SNMP, therefore, without unique SNMP community names, the risk of compromise is dramatically increased. This is especially true with vendors default community names which are widely known by hackers and other networking experts. If a hacker gains access to these devices and can easily guess the name, this could result in denial of service, interception of sensitive information, or other destructive actions.

Checks

NET SNMP Least Privilege

Review the configuration of all managed nodes (SNMP agents) to ensure that different community names or usernames are used for read-only and read-write access.

Default Finding Details SNMP community names have not been changed from their default values and privilege levels are not set correctly.

The following community names have not been changed:

The following name appears on multiple devices:

The following privilege levels are set incorrectly:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET SNMP Least Privilege

The NSO will ensure that SNMP community names are changed from the default public values to unique community names and developed IAW the Network Infrastructure STIG.

The NSO will ensure these names do not match any other network device passwords, keys or strings.

The NSO will ensure that unique community names are used for different access types, including read-only, read and write.

Notes:

NET1910 V0015240 CAT II IPv6 vlans are not pruned and leak IPv4 broadcast

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure trunks supporting IPv6 vlans are pruned and do not leak IPv4 broadcast in Split Domain Architecture.

Vulnerability Discussion RFC 4554 describes the use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, described as Split Domain Enterprise Architecture in this document. The architecture utilizes VLANs that can be readily used to deploy IPv6 networking in an enterprise, which focuses on the scenario of early deployment prior to availability of IPv6-capable switch-router equipment. In this method, IPv6 may be routed in parallel with the existing IPv4 in the enterprise and delivered at Layer 2 via VLAN technology. The IPv6 connectivity to the enterprise may or may not enter the site via the same physical link.

Sites migrating to dual-stack networking will either upgrade existing switch-router equipment to support IPv6 or procure new equipment that supports IPv6. If a site already has production routers deployed that support IPv6, the procedures described in this section are not required. In the interim, however, a method is required for early IPv6 adopters that enable IPv6 to be deployed in a structured, managed way to some or all of an enterprise network that currently lacks IPv6 support in its core infrastructure.

In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

To prevent IPv4 frames from leaking onto the trunk supporting IPv6, the IPv4 VLANs will be pruned from the IPv6 trunk.

Checks

NET IPv4 leaking on trunk

Base Procedure: Review the switch configurations and note switchports assigned to each VLAN. Identify which IP version (IPv4 or IPv6) is running on the Interface. Then identify the vlans on each trunk. Trunks designated for IPv6 should have all IPv4 vlans pruned from the IPv6 trunk.

NET IPv4 leaking on trunk IOS

IOS Procedure: A show vlan command can also be used to verify what ports are assigned to the VLAN. A show trunk interface will identify which VLANs are defined on the trunk.

Default Finding Details IPv6 vlans are not pruned and leak IPv4 broadcast in Split Domain architecture.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET IPv4 leaking on trunk

Correct the architecture to prevent IPv4 from leaking into the IPv6 trunk.

Notes:

NET1911 V0015241 CAT II IPv4 vlans are not pruned and leak IPv6 broadcast

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure trunks supporting IPv4 vlans are pruned and do not leak IPv6 broadcast in Split Domain Architecture.

Vulnerability Discussion RFC 4554 describes the use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, described as Split Domain Enterprise Architecture in this document. The architecture utilizes VLANs that can be readily used to deploy IPv6 networking in an enterprise, which focuses on the scenario of early deployment prior to availability of IPv6-capable switch-router equipment. In this method, IPv6 may be routed in parallel with the existing IPv4 in the enterprise and delivered at Layer 2 via VLAN technology. The IPv6 connectivity to the enterprise may or may not enter the site via the same physical link.

Sites migrating to dual-stack networking will either upgrade existing switch-router equipment to support IPv6 or procure new equipment that supports IPv6. If a site already has production routers deployed that support IPv6, the procedures described in this section are not required. In the interim, however, a method is required for early IPv6 adopters that enable IPv6 to be deployed in a structured, managed way to some or all of an enterprise network that currently lacks IPv6 support in its core infrastructure.

Many IPv4 enterprise networks are utilizing VLAN technology. Where a site does not have IPv6-capable Layer 2/3 switch-router equipment, but VLANs are supported, a simple yet effective method exists to gradually introduce IPv6 to some or all of that site's network in advance of the site's core infrastructure having dual-stack capability.

This architecture can be accomplished by deploying a parallel IPv6 routing infrastructure (which is likely to be a different platform to the site's main infrastructure equipment, i.e., one that supports IPv6 where the existing equipment does not), and then using VLAN technology to "overlay" IPv6 links onto existing IPv4 links.

In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

To prevent IPv6 frames from leaking onto the trunk supporting IPv4, the IPv6 VLANs will be pruned from the IPv4 trunk.

Checks

NET IPv6 leaking on trunk

Base Procedure: Review the switch configurations and note switchports assigned to each VLAN. Identify which IP version (IPv4 or IPv6) is running on the Interface. Then identify the vlans on each trunk. Trunks designated for IPv4 should have all IPv6 vlans pruned from the IPv4 trunk.

NET IPv6 leaking on trunk IOS

IOS Procedure: A show vlan command can also be used to verify what ports are assigned to the VLAN. A show trunk interface will identify which VLANs are defined on the trunk.

Default Finding Details IPv4 vlans are not pruned and leak IPv6 broadcast in a Split Domain Architecture.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET IPv6 leaking on trunk

Correct the architecture to prevent IPv6 from leaking into the IPv4 trunk

Notes:

NET1914 V0015242 CAT II IPv6 must not be enabled on Dual Stack IPv4 trunk

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability IAO/NSO will ensure interfaces on the Dual Stack device connecting to the IPv4 trunk do not have IPv6 enabled in Split Domain Architecture.

Vulnerability Discussion In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

The implementation of this architecture requires the following guidelines be implemented. Referencing the Split Domain diagram in the STIG, interfaces I1.A and P1.B will not receive any IPv4 traffic by not enabling IPv4 on I1.B. The SA will configure the architecture so that interfaces I1.D and P1.C will not receive any IPv6 traffic by not enabling IPv6 on I1.C.

Checks

NET IPv6 on IPv4 Trunk

Review the architectural drawing in the STIG to become familiar with where the filter location should reside. Review the Site implementation and architecture. Ensure IPv6 is not enabled on the IPv4 trunk.

Default Finding Details IPv6 is enabled on Dual Stack device connecting to IPv4 trunk.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET IPv6 on IPv4 Trunk

Disable IPv6 on the IPv4 trunk.

Notes:

NET1915 V0015249 CAT II IPv4 must not be enabled on Dual Stack IPv6 trunk

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure interfaces on the Dual Stack device connecting to the IPv6 trunk do not have IPv4 enabled in Split Domain Architecture.

Vulnerability Discussion In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

The implementation of this architecture requires the following guidelines be implemented. Referencing the Split Domain diagram in the STIG, interfaces I1.A and P1.B will not receive any IPv4 traffic by not enabling IPv4 on I1.B. The SA will configure the architecture so that interfaces I1.D and P1.C will not receive any IPv6 traffic by not enabling IPv6 on I1.C.

Checks

NET IPv4 on IPv6 Trunk

Review the architectural drawing in the STIG to become familiar with where the filter location should reside. Review the Site implementation and architecture. Ensure IPv4 is not enabled on the IPv6 trunk.

Default Finding Details IPv4 is enabled on Dual Stack device connecting to IPv6 trunk.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET IPv4 on IPv6 Trunk

Disable IPv4 on the IPv6 trunk.

Notes:

NET1918 V0015250 CAT II Split Domain IPv6 interface has 6to4 tunnel

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Split Domain IPv6 interface must not have IPv4 in IPv6 tunnel traffic.

Vulnerability Discussion In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

Review the diagram in the STIG. In the Split Domain architecture there must not be any IPv4 in IPv6 tunnel traffic between interfaces I1.A and P1.B.

Checks

NET Split Domain-IPv6-tunnel

If the Site has implemented Split Domain architecture, verify the IPv6 interface supporting the trunk does not have tunnel traffic.

Default Finding Details Split Domain IPv6 interface must not have IPv4 in IPv6 tunnel traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Split Domain-IPv6-tunnel

Remove tunnel from the Split Domain architecture.

Notes:

NET1919 V0015253 CAT II Split Domain IPv4 interface has 6to4 tunnel

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure interfaces supporting IPv4 in Split Domain Architecture do not have any IPv4 in IPv6 tunnel traffic between the interfaces.

Vulnerability Discussion In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

Review the diagram in the STIG. In the Split Domain architecture there must not be any IPv4 in IPv6 tunnel traffic between interfaces I1.D and P1.C.

Checks

NET Split Domain-IPv4-tunnel

If the Site has implemented Split Domain architecture, verify the IPv4 interface supporting the trunk does not have tunnel traffic.

Default Finding Details Split Domain IPv4 interface must not have IPv4 in IPv6 tunnel traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Split Domain-IPv4-tunnel

Remove tunnel from the Split Domain architecture.

Notes:

NET1920 V0015261 CAT II Split Domain has IPv6 transition mechanism.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the enclave boundary does not have any other IPv6 Transition Mechanisms implemented when supporting Split Domain.

Vulnerability Discussion In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

The enterprise will not have any other IPv6 Transition Mechanisms implemented in the enclave when supporting Split Domain architecture.

Checks

NET Split Domain-Transition Me

If the enclave has a Split Domain architecture, review the remaining enclave and determine if a transition mechanism such as the ones described in the STIG have been defined. Interview the DNS, IAO and Router Administrator.

Default Finding Details Split Domain architecture has IPv6 transition mechanisms.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Fixes

NET Split Domain-Transition Me

Determine the technology required and remove the other to satisfy the guidelines.

Notes: