



Network Security Checklist - Layer 2 Switch

Version 7, Release 1.1

20 November 2007

Developed by DISA for the DOD

UNCLASSIFIED

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				

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 IA0/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 IA0/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 DODI 8500.2 ECWM-1.

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 before the password prompt and after a correct login.

Default Finding Details DOD approved warning banners, adhering to Appendix C of the Network Infrastructure STIG, 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:

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

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 The management VLAN is configured on unnecessary trunk.

Details

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 IAQ/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 Usage

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 Usage

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 A dedicated VLAN is not configured for trunking.
Details

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 Access ports are assigned to the dedicated trunk VLAN.

Details

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 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.

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

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.

**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

Port Security or 802.1x is not turned on.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure either Port Security 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

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 Port Security or 802.1x is not turned on.

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:

NET1437 **V0005625** **CAT II** **Port Security with MAC Addresses is not configured**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/NSO will ensure if Port Security has been implemented, the MAC addresses are statically configured 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 Secured MAC ADDR

Have the switch administrator issue a show port [mod[/port]] or look for the following command.

set port security mod/port enable MAC address

Default Finding Details Port Security is not configured with MAC addresses defined.

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

Fixes

NET SW Port Secured MAC ADDR

Enable Port Security with MAC Addresses.

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 IA/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:

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 (both MD5 packet authentication and DES 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 (both MD5 packet authentication and DES 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 IPv6 vlans are not pruned and leak IPv4 broadcast in Split Domain architecture.

Details

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

Details

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: