



Network Security Checklist - Cisco Layer 3 Infrastructure 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				

NET0162

V0004622 CAT I

AG ingress ACL is not configured to secure enclave

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure premise router interfaces that connect to an AG (i.e., ISP) are configured with an ingress ACL that only permits packets with destination addresses within the site's address space.

Vulnerability Discussion Any enclave with one or more AG connections will have to take additional steps to ensure that neither their network nor the NIPRNet is compromised. Without verifying the destination address of traffic coming from the site's AG, the premise router could be routing transit data from the Internet into the NIPRNet. This could also make the premise router vulnerable to a DoS attack as well as provide a backdoor into the NIPRNet. The DOD enclave must ensure that the premise router's ingress packet filter for any interface connected to an AG is configured to only permit packets with a destination address belonging to the DOD enclave's address block.

Checks

NET AG Ingress

Review the running config of the router that connects to an AG and verify that each permit statement of the ingress ACL is configured to only permit packets with destination addresses of the site's NIPRNet address space or that belonging to the address block assigned by the AG network service provider.

Default Finding Details AG ingress ACL is not configured to only permit packets with a destination address belonging to the sites address block.

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

Fixes

NET AG Ingress

Insure the ingress ACL for any interface connected to an AAG is configured to only permit packets with a destination address belonging to the sites address block.

Notes:

NET0164 **V0004623** **CAT I** **AG router has a routing protocol to the enclave.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the premise router does not have a routing protocol session with a peer router belonging to an AS (Autonomous System) of the AG service provider. A static route is the only acceptable route to an AG.

Vulnerability Discussion The premise router will not use a routing protocol to advertise NIPRNet addresses to the AG. Most ISPs use Border Gateway Protocol (BGP) to share route information with other autonomous systems (AS), that is, any network under a different administrative control and policy than that of the local site. If BGP is configured on the premise router, no BGP neighbors will be defined as peer routers from an AS belonging to any AG. The only method to be used to reach the AG will be through a static route.

Checks

NET AG Routes

Review the configuration of the router connecting to the AG and verify that there are no BGP neighbors whose remote AS belongs to the AG service provider.

Default Finding Details The router connecting to an AG is configured to use a routing protocol between the AAG network service provider and the Enclave.

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

Fixes

NET AG Routes

The only method to be used to reach the AG will be through a static route.

Notes:

NET0166 **V0004624** **CAT III** **AG Network IP addresses are advertised in enclave**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the AG network service provider IP addresses are not redistributed into or advertised to the NIPRNet or any router belonging to any other Autonomous System (AS) i.e. to another AG device in another AS.

Vulnerability Discussion Unsolicited traffic that may inadvertently attempt to enter the NIPRNet by traversing the enclave's premise router can be avoided by not redistributing NIPRNet routes into the AG.

Checks

NET AG IP Addresses

Review the configuration of the router connecting to the AG and verify that there are no routes being redistributed into the enclave from the AG.

Default Finding Details AG Network Service Providers IP addresses are advertised or redistributed to the NIPRNet.

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

Fixes

NET AG IP Addresses

Use distribute lists prefix lists to insure AG routes are not redistributed into the NIPRNet BGP or sites IGP (OSPF, EIGRP, RIP, etc).

Notes:

NET0167 **V0014632** **CAT II** **AG must adhere to PPS boundary 13 and 14 policies**

8500.2 IA Control: DCP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the route to the AG network adheres to the PPS CAL boundary 13 and 14 policies and is in compliance with all perimeter filtering defined in the perimeter and router sections of the Network STIG.

Vulnerability Discussion The enclave perimeter requirement for filtering, to include JTF-GNO PPS filtering rules, and monitoring traffic will be enforced for any traffic from the AG. All traffic entering the enclave from the AG must enter through the firewall and be monitored by internal IDS. All traffic leaving the enclave, regardless of the destination--AG or NIPRNet addresses, will be filtered by the premise router's egress filter to verify that the source IP address belongs to the enclave.

Checks

NET AG PPS policy

The enclave perimeter requirement for filtering, to include JTF-GNO PPS filtering rules, and monitoring traffic will be enforced for any traffic from the AG. All traffic leaving the enclave, regardless of the destination--AG or NIPRNet addresses, will be filtered by the premise router's egress filter to verify that the source IP address belongs to the enclave.

Default Finding Details

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

Fixes

NET AG PPS policy

Ensure the perimeter is protected from this path. A deny by default policy is enforced at this connection and the site is in compliance with all PPS 13 and 14 boundaries.

Notes:

NET0190 **V0003005** **CAT III** **LAN addresses are not protected from the public.**

8500.2 IA Control: EBB-1, EBB-2, EBB-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that workstation clients' real IPv4 addresses are not revealed to the public by implementing NAT on the firewall or the router.

Vulnerability Discussion NAT works well with the implementation of RFC 1918 addressing scheme, it also has the privacy benefit of hiding real internal addresses. An attacker can learn more about a site's private network once it has discovered the real IP addresses of the hosts within.

Checks

NET NAT Requirement

Review the firewall or premise router configuration to determine if NAT has been implemented.

Default Finding Details NAT has not been implemented. Mark this as N/A for SIPRNet enclaves that have not implemented NAT.

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

Fixes

NET NAT Requirement

Implement Network Address Translation (NAT) on the firewall or premise router for NIPRNet Enclaves.

Notes:

NET0201 V0014637 CAT II IPv6 route advertisements must be suppressed

8500.2 IA Control: DCBP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all external interfaces on Premise, AG, or Backdoor have router advertisements suppressed.

Vulnerability Discussion Many of the known attacks in stateless autoconfiguration are define in RFC 3756 were present in IPv4 ARP attacks. IPSec AH was originally suggested as mitigation for the link local attacks, but has since been found to have bootstrapping problems and to be very administrative intensive. Due to first requiring an IP address in order to set up the IPSec security association creates the chicken-before-the-egg dilemma. There are solutions being developed (Secure Neighbor Discovery and Cryptographic Generated Addressing) to secure these threats but are not currently available at the time of this writing.

To mitigate these vulnerabilities, links that have no hosts connected such as the interface connecting to external gateways will be configured to suppress router advertisements.

Checks

NET IPv6 RA suppress IOS

Base Procedure:

On the network perimeter router's external interface suppress the router advertisements.

IOS Procedure:

interface faste0/0

ipv6 nd ra suppress

Default Finding Details IPv6 route advertisements must be suppressed

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

Fixes

NET IPv6 RA suppress

Base Procedure:

On the network perimeter router's external interface suppress the router advertisements.

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 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:

NET0400

V0003034 CAT II

Interior routing protocols are not authenticated

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure neighbor authentication with IPSec AH or MD5 Signatures are implemented for interior routing protocols with all peer routers within the same or between Autonomous Systems (AS).

Vulnerability Discussion A rogue router could send a fictitious routing update to convince a site's premise router to send traffic to an incorrect or even a rogue destination. This diverted traffic could be analyzed to learn confidential information of the site's network, or merely used to disrupt the network's ability to effectively communicate with other networks.

Checks

NET MD5 Authentication

Determine what routing protocols have been implemented with internal neighbors. After identifying the routing protocol ensure neighbor authentication is implemented using MD5. The following interior routing protocols support MD5: OSPFv2, IS-IS, EIGRP, and RIP V2.

NET0400-CISCO

```
OSPF
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip ospf message-digest-key 10 md5 mypassword

router ospf 10
network 10.10.0.0 0.0.255.255 area 0
area 0 authentication message-digest
```

Note: Authentication has to be enabled for each area. In OSPF, an interface belongs to only one area; hence, there would always be a network statement under the OSPF process ID for each interface that has OSPF traffic. The network statement defines the area in which the network belongs. The MD5 key-id and password is defined under each interface connected to an OSPF neighbor.

```
EIGRP
interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 mypassword
key chain mypassword
key 12345
key-string abcdefg
accept-lifetime infinite
router eigrp 1
network 10.0.0.0
no auto-summary
```

Default Finding MD5 is not used to authenticate routing protocol neighbors.

Details

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

Fixes

NET MD5 Authentication

The router administrator will configure the routers so that MD5 authentication is used to authenticate routing protocol neighbors.

Notes:

NET0408 V0014665 CAT II Exterior routing protocols must authenticate

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure neighbor authentication systems with MD5 or IPSec is implemented for all BGP routing protocols with all peer routers within the same or between autonomous systems (AS).

Vulnerability Discussion Unlike OSPF ships-in-the-night, the protocol BGP exchanges information on IPv4 and IPv6 routes concurrently. Two mechanisms available to protect the integrity of BGP peers are TCP MD5 Signature and IPSec.

The simplest way to create havoc in a network is to inject bogus routes. On the other hand, an attack could be much more sophisticated. A rogue router or device could send a fictitious routing update to convince an edge router to send traffic to an incorrect or rogue destination. This diverted traffic could be analyzed to learn confidential information regarding the site's network, or merely used to disrupt the network's ability to effectively communicate with other networks.

An autonomous system (AS) can advertise incorrect information through BGP update messages passed to routers from a neighboring AS. A malicious AS can advertise a prefix originated from another AS and claim that it is the originator. Neighboring autonomous systems receiving this announcement will believe that the malicious AS is the prefix owner and route packets to it. The prefix owner will not receive the traffic that is supposed to be bound for it. Spoofed TCP segments could be introduced into the connection streams for LDP sessions used to build LSPs. LDP hellos from peers that have no password are ignored. By configuring strict authentication between LSR peers, LDP and RSVP sessions can be restricted and the integrity of LSPs can be guarded.

Checks

NET BGP Authentication

Base Procedure

Determine what routing protocols have been implemented on the edge. MD5 Signature is most common in current BGP implementations, and sets up an effective signature for the TCP packets based on a cryptographic protection. You can apply IPSec to BGP traffic. IPSec is a protocol suite used for protecting IP traffic at the packet level. IPSec is based on security associations (SAs). A security association is a simple connection that provides security services to the packets carried by the SA. After configuring the security association, you can apply the SA to BGP peers. Following are some sample configurations for BGP neighbor authentication using MD5. Reference the example in OSPFv3 for an IPSec examples. The protocol would obviously change to BGP. Verify the authentication is implemented correctly.

NET0408 - CISCO

Following are some sample configurations for BGP neighbor authentication using MD5. Reference the example in OSPFv3 for an IPSec example. The protocol would obviously change to BGP.

```
router bgp 100
neighbor external-peers peer-group
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.90 password xxxxxxxxxx
neighbor 171.69.232.100 password xxxxxxxxxx
```

```
router bgp 100
neighbor IPv6-external-peers peer-group
neighbor 2001:100:3:4::1 remote as 200 ! for EBGP peering, over IPv6
neighbor 2001:100:3:4::1 peer-group IPv6-external-peers
neighbor 2001:100:3:4::1 password xxxxxxxxxx
```

Note: The neighbor/password statement can be applied to either the peer-group or the neighbor definition.

Default Finding Exterior routing protocols do not authenticate.
Details

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

Fixes

NET BGP Authentication

The router administrator will configure the routers so that MD5 or IPSec AH authentication is used to authenticate routing protocol neighbors.

Notes:

NET0425

V0007009 CAT I

An Infinite Lifetime key has not been implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the lifetime of a MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.

Note: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Vulnerability Discussion Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. When configuring authentication for routing protocols that provide key chains, configure two rotating keys with overlapping expiration dates—both with a 180-day lifetime. A third key must also be defined with an infinite lifetime. Both of these steps will ensure that there will always be a key that can be placed into service by all peers. If a time period occurs during which no key is activated, authentication cannot occur; hence, route updates will not occur. The lifetime key should be changed 7 days after successful key rotation and synchronization has occurred with all peers.

Checks

NET MD5 Lifetime Key

Review the running configuration to determine if key authentication has been defined with an infinite lifetime.

RIP 2 Example

EIGRP Example

```
interface ethernet 0
```

```
ip rip authentication key-chain trees
ip rip authentication mode md5
```

```
interface ethernet 0
```

```
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 trees
```

```
router rip
```

```
router eigrp 1
```

```
network 172.19.0.0
version 2
```

```
network 172.19.0.0
```

```
key chain trees
```

```
key chain trees
```

```
key 1
```

```
key 1
```

```
key-string willow
```

```
key-string willow
```

```
accept-lifetime 22:45:00 Feb 10 2005 22:45:00 Aug 10 2005
```

```
accept-lifetime 22:45:00 Feb 10 2005 22:45:00 Aug 10 2005
```

```
send-lifetime 23:00:00 Feb 10 2005 22:45:00 Aug 10 2005
```

```
send-lifetime 23:00:00 Feb 10 2005 22:45:00 Aug 10 2005
```

```
key 2
```

```
key 2
```

```
key-string birch
```

```
key-string birch
```

```
accept-lifetime 22:45:00 Aug 9 2005 22:45:00 Feb 10 2006
```

```
accept-lifetime 22:45:00 Dec 10 2005 22:45:00 Feb 10 2006
```

```
send-lifetime 23:00:00 Aug 9 2005 22:45:00 Feb 10 2006
```

```
send-lifetime 23:00:00 Dec 10 2005 22:45:00 Jan 10 2006
```

```
key 9999
```

```
key 9999
```

```
key-string maple
```

```
key-string maple
```

```
accept-lifetime 22:45:00 Feb 9 2005 infinite
```

```
accept-lifetime 22:45:00 Feb 9 2005 infinite
```

```
send-lifetime 23:00:00 Feb 9 2005 infinite
```

```
send-lifetime 23:00:00 Feb 9 2005 infinite
```

Notes: Note: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains

Notes: When using MD5 authentication keys, it is imperative the site is in compliance with the NTP policies. The router has to know the time!

Notes: Must make this a high number to ensure you have plenty of room to put keys in before it. All subsequent keys will be decremented by one (9998, 9997...)

Default Finding Details An Infinite Lifetime key has not been implemented for EIGRP or RIPv2.

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

Fixes

NET MD5 Lifetime Key

This check is in place to ensure keys do not expire creating a DOS due to adjacencies being dropped and routes being aged out. The recommendation is to use two rotating six month keys with a third key set as infinite lifetime. The lifetime key should be changed 7 days after the rotating keys have expired and redefined.

Notes:

NET0433

V0015432 CAT II

AAA Method list is not applied or implemented

8500.2 IA Control:

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure an authentication method list is applied to all interfaces via an explicit definition or by use of default key word.

Vulnerability Discussion The AAA authentication login statement identifies the method list name and the method used to authenticate. A named list of authentication methods must be defined and applied to each interfaces using the authentication method. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

Checks

NET AAA Method list implemente

If the following "Default List is coded in the AAA configuration than explicit Method Lists are not required on each interface.

CISCO Example:
aaa authentication login default local

If the default method list is not defined a configuration similar to the following should be defined for each interface.

CISCO Example:
aaa authentication login "listname"

line vty 0 4
login authentication "listname"

Default Finding Details An authentication method list is not applied to all interfaces via an explicit definition or by use of default key word.

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

Fixes

NET AAA Method implemented

Have the SA define a Default Method list or apply a method list to each interface.

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 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 administrative privileges should work.

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 router administrators 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: There are 16 possible privilege levels that can be specified for users in the router configuration. The levels can map 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.

NET0465 - CISCO

There would be several username name password password followed by username name privilege level. The user will automatically be granted that privilege level upon logging in. Below is an example of assigning a privilege level to a local user account and changing the default privilege levels of the configure terminal command.

```
username junior-engineer1 privilege 7 password xxxxxx  
username senior-engineer1 privilege 15 password xxxxxx  
privilege exec level 7 configure terminal
```

Note The above example only covers local accounts, you will still need to check the accounts and their associated privilege levels configured in the authentication server. You can also use TACACS for even more granularity at the command level.

Below is an example of CiscoSecure TACACS+ server defining the privilege level.

```
user = junior-engineer1 {  
  password = clear "xxxxx"  
  service = shell {  
    set priv-lvl = 7  
  }  
}
```

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 router administrator will assign router 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:

NET0700

V0003160 CAT II

Minimum operating system release level

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will implement the latest stable operating system on each router 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 is at 12.3 or later. Software Major Release 12.3 was posted to CCO May 19, 2003. You will find in some cases version 12.2 is the most current version, typically in the CAT IOS 6000 switch family only.

Default Finding IOS version 12.3 has not been implemented on all Cisco routers.

Details

JUNOS version is at 7.3 on J, M and T series and 5.3.2 on E series..

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:

NET0710

V0003077 CAT III

The Cisco discovery protocol (CDP) is not disabled

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure CDP is disabled on all active external interfaces on Cisco premise routers.

Vulnerability Discussion CDP is primarily used to obtain protocol addresses of neighboring devices and discover platform capabilities of those devices. Use of SNMP with the CDP Management Information Base (MIB) allows network management applications to learn the device type and the SNMP agent address of neighboring devices; thereby, enabling the application to send SNMP queries to those devices. CDP is also media- and protocol-independent as it runs over the data link layer; therefore, two systems that support different network-layer protocols can still learn about each other. Allowing CDP messages to reach external network nodes is dangerous as it provides an attacker a method to obtain information of the network infrastructure that can be useful to plan an attack.

Checks

NET CDP Internal Only

Review all Cisco router configurations to ensure that no cdp run is included in the global configuration or no cdp enable is included for each active external interface.

Default Finding Details The Cisco discovery protocol (CDP) is enabled on the edge router(s) external interfaces.

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

Fixes

NET CDP Internal Only

Ensure that no cdp run is included in the global configuration or no cdp enable is included for each active external interface.

Notes:

NET0720 V0003078 CAT III TCP and UDP small server services are not disabled

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure TCP & UDP small servers are disabled.

Vulnerability Discussion Cisco IOS provides the "small services" that include echo, chargen, and discard. These services, especially their User Datagram Protocol (UDP) versions, are infrequently used for legitimate purposes. However, they have been used to launch denial of service attacks that would otherwise be prevented by packet filtering. For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to the Cisco's UDP echo port, the result would be the Cisco sending a DNS packet to the server in question. No outgoing access list checks would be applied to this packet, since it would be considered locally generated by the router itself. The small services are disabled by default in Cisco IOS 12.0 and later software. In earlier software, they may be disabled using the commands `no service tcp-small-servers` and `no service udp-small-servers`.

Checks

NET TCP/UDP small -servers

IOS Procedure: Review all Cisco router configurations to verify that service `udp-small-servers` and service `tcp-small-servers` are not found.

Note: The TCP and UDP small servers are enabled by default on Cisco IOS Software Version 11.2 and earlier. They are disabled by default on Cisco IOS Software Versions 11.3 and later.

Default Finding Details TCP and UDP small server services are enabled on the router(s).

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

Fixes

NET TCP/UDP small-servers

The router administrator will change the router configuration files to include the following CISCO commands: `no service tcp-small-servers` and `no service udp-small-servers`, for each router running an IOS version prior to 12.0. This is the default for IOS versions 12.0 and later (I.E., these commands will not appear in the running configuration.)

Notes:

NET0722 **V0005614** **CAT III** **Service Pad is enabled on the router.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure PAD services are disabled unless approved by the DAA.

Vulnerability Discussion Packet Assembler Disassembler (PAD) is an X.25 component seldom used. It collects the data transmissions from the terminals and gathers them into a X.25 data stream and vice versa. PAD acts like a multiplexer for the terminals. If enabled, it can render the device open to attacks. Some voice vendors use PAD on internal routers.

Checks

NET PAD Services

IOS Procedure: Review all Cisco router configurations to verify that service pad is not found.

Default Finding Details Service Pad is enabled on the router.

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

Fixes

NET PAD Services

The router administrator will change the router configuration files to include the following CISCO commands: no service pad

Notes:

NET0724 **V0005615** **CAT III** **TCP Keep-Alives for Telnet Session must be enabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure TCP Keep-Alives for Telnet Session are enabled.

Vulnerability Discussion Idle logged-in telnet sessions can be susceptible to unauthorized access and hijacking attacks. By default, routers do not continually test whether a previously connected TCP endpoint is still reachable. If one end of a TCP connection idles out or terminates abnormally, the opposite end of the connection may still believe the session is available. These "orphaned" sessions use up valuable router resources and can also be hijacked by an attacker. To mitigate this risk, routers must be configured to send periodic keepalive messages to check that the remote end of a session is still connected. If the remote device fails to respond to the keepalive message, the sending router will clear the connection and free resources allocated to the session.

Checks

NET TCP Keep-alives

IOS Procedure: Review all Cisco router configurations to verify that tcp-keepalives-in are enabled.

Default Finding Details TCP Keep-Alives for Telnet Session are not enabled.

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

Fixes

NET TCP Keep-alives

The router administrator will change the router configuration files to include the following CISCO commands: service tcp-keepalives in

Notes:

NET0726 **V0005616** **CAT III** **Identification support is enabled.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure identification support is not enabled.

Vulnerability Discussion Identification support allows one to query a TCP port for identification. This feature enables an unsecured protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. Identification support, can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply. This is another mechanism to learn the router vendor, model number, and software version being run.

Checks

NET IDENT Support disabled

Review all Cisco router configurations to verify that identification support is not enabled via ip identd IOS command.

Default Finding Details Identification support is enable and must be disabled.

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

Fixes

NET IDENT Support Disabled

The router administrator will change the router configuration files to include the following CISCO commands: no identd if its enabled.

Notes:

NET0730 **V0003079** **CAT III** **The finger service is not disabled on all routers.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure Finger is disabled.

Vulnerability Discussion The IOS finger service supports the UNIX finger protocol, which is used for querying a host about the users that are logged on. This service is not necessary for generic users. If an attacker would find out who is using the network, they may use social engineering practices to try to elicit classified DOD information.

Checks

NET Finger Disabled

Base Procedure:
Ensure finger has not been implemented in the configuration by verifying the vendor default and reviewing the configuration.

NET0730 - CISCO

Review all Cisco router configurations to verify that the IOS command, no ip finger for IOS version 12.0 and higher and no service finger for earlier version, is included.

Default Finding Details The finger service is enabled on the router(s).

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

Fixes

NET Finger Disabled

Verify the finger service is disabled.

Notes:

NET0740 **V0003085 CAT II** **HTTP server is not disabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure HTTP servers are disabled.

Vulnerability Discussion The additional services that the router is enabled for increases the risk for an attack since the router will listen for these services. In addition, these services provide an unsecured method for an attacker to gain access to the router. Most recent software versions support remote configuration and monitoring using the World Wide Web's HTTP protocol. In general, HTTP access is equivalent to interactive access to the router. The authentication protocol used for HTTP is equivalent to sending a clear-text password across the network, and, unfortunately, there is no effective provision in HTTP for challenge-based or one-time passwords. This makes HTTP a relatively risky choice for use across the public Internet. Any additional services that are enabled increase the risk for an attack since the router will listen for these services.

Checks

NET HTTP Server

IOS Procedure: Verify http-server is not defined in the configuration. The feature is disabled by default in IOS version 12.0; hence the no ip http-server command will not appear in the running configuration.

Default Finding Details The following servers were enabled on the router:

HTTP

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

Fixes

NET HTTP Server

The router administrator will change the router configuration files to include the Cisco command, no ip http-server, for all routers with an IOS version after 11.3 and prior to 12.0. IOS versions 12.0 and later have this disabled by default and this will not appear in the running configuration.

Notes:

NET0742 **V0014668** **CAT II** **FTP server is not disabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure FTP server is disabled.

Vulnerability Discussion The additional services enabled on a router increases the risk for an attack since the router will listen for these services. In addition, these services provide an unsecured method for an attacker to gain access to the router.

Checks

NET FTP Server

Base Procedure:

Ensure ftp server has not been implemented in the configuration by verifying the vendor default and reviewing the configuration.

NET0742 - CISCO

IOS Procedure: Verify ftp-server is not defined in the configuration. The feature is disabled by default in IOS version 12.0; hence the no ip ftp-server command will not appear in the running configuration.

Default Finding Details FTP server is not disabled on the router.

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

Fixes

NET FTP Server

The router administrator will disable ftp server features for all routers.

Notes:

NET0744 V0014669 CAT II BSD commands are not disabled

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure BSD r command services are disabled.

Vulnerability Discussion Berkeley Software Distribution (BSD) "r" commands allow users to execute commands on remote systems using a variety of protocols. The BSD "r" commands (e.g., rsh, rlogin, rcp, rdump, rrestore, and rdist) are designed to provide convenient remote access without passwords to services such as remote command execution (rsh), remote login (rlogin), and remote file copy (rcp and rdist). The difficulty with these commands is that they use address-based authentication. An attacker who convinces a server that he is coming from a "trusted" machine can essentially get complete and unrestricted access to a system. The attacker can convince the server by impersonating a trusted machine and using IP address, by confusing DNS so that DNS thinks that the attacker's IP address maps to a trusted machine's name, or by any of a number of other methods

Checks

NET BSD 'r' commands

Base Procedure:

Ensure ftp server has not been implemented in the configuration by verifying the vendor default and reviewing the configuration.

NET0744 - CISCO

Verify the BSD 'r' commands are not defined in the configuration. The feature is disabled by default in IOS version 12.0. Some of the common commands are: ip rcmd rcp-enable, ip rcmd rsh-enable

Default Finding BSD commands are not disabled on the router.

Details

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

Fixes

NET BSD 'r' commands

The router administrator will change the router configuration to remove BSD commands from all routers.

Notes:

NET0750 **V0003086** **CAT III** **The bootp service is not disabled on all routers.**

8500.2 IA Control: ECSD-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure Bootp server is disabled.

Vulnerability Discussion Bootp is a user datagram protocol (UDP) that can be used by Cisco routers to access copies of Cisco IOS Software on another Cisco router running the Bootp service. In this scenario, one Cisco router acts as a Cisco IOS Software server that can download the software to other Cisco routers acting as Bootp clients. In reality, this service is rarely used and can allow an attacker to download a copy of a routers Cisco IOS Software.

Checks

NET Bootp Disabled

IOS Procedure: Review all Cisco router configurations to verify that the IOS command no ip bootp server is present.

Default Finding Details The bootp service is enabled on the following routers:

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

Fixes

NET Bootp Disabled

The router administrator will change the router configuration files to include the Cisco command, no ip bootp server, for each router.

Notes:

NET0760 **V0003080** **CAT II** **Configuration auto-loading must be disabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure configuration auto-loading is disabled.

Vulnerability Discussion The routers can find their startup configuration either in their own NVRAM or load it over the network via TFTP or Remote Copy (rcp). Obviously, loading in from the network is taking a security risk. If the startup configuration was intercepted by an attacker, it could be used to either gain access to the router.

Checks

NET Boot Network

IOS Procedure: Ensure the commands boot network and service config are not included. Note: Disabled by default in version 12.0 , not be displayed in the running configuration.

Default Finding Details The no boot network and no service config commands are not employed to restrict auto-loading of the startup configuration via TFTP.

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

Fixes

NET Boot Network

The router administrator will change the router configuration files to include the CISCO commands, no boot network and no service config, for each router.

Notes:

NET0770 **V0003081** **CAT II** **IP Source Routing is not disabled on all routers.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure IP source routing is disabled.

Vulnerability Discussion Source routing is a feature of IP, whereby, individual packets can specify routes. This feature is used in several different network attacks.

Checks

NET Source-Route Disabled

Base Procedure: Review the configuration to determine if source routing is turned on. Verify the vendor defaults do not enabled this function.

NET0770 - CISCO

Ensure the command no ip source-route is included.

Default Finding Details IP Source Routing is enabled on the router(s).

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

Fixes

NET Source-Route Disabled

The router administrator will change the router configuration files to include the CISCO command, no ip source-route, for each router.

Notes:

NET0780 **V0003082** **CAT II** **Proxy ARP must be disabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure Proxy ARP is disabled.

Vulnerability Discussion When proxy ARP is enabled on a Cisco router, it allows that router to extend the network (at Layer 2) across multiple interfaces (LAN segments). Because proxy ARP allows hosts from different LAN segments to look like they are on the same segment, proxy ARP is only safe when used between trusted LAN segments. Attackers can leverage the trusting nature of proxy ARP by spoofing a trusted host and then intercepting packets. You should always disable proxy ARP on router interfaces that do not require it, unless the router is being used as a LAN bridge.

Checks

NET IP Proxy-arp disabled

IOS Procedure: Ensure the command no ip proxy-arp is included for every active interface.

Default Finding Details The IP proxy Address Resolution Protocol (ARP) service is enabled on the router interface.

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

Fixes

NET IP Proxy-arp disabled

The router administrator will change the router configuration files to include the no ip proxy-arp command for each interface of every router.

Notes:

NET0781 **V0005618** **CAT II** **Gratuitous ARP must be disabled.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure Gratuitous ARP is disabled.

Vulnerability Discussion A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used to inform the network about a hosts IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

Checks

NET Gratuitous Arp Disabled

IOS Procedure: Review all router configurations and verify ip gratuitous-arps is not configured. Disabled by default in 12.3 and above.

Default Finding Details The IP gratuitous Address Resolution Protocol (ARP) service is enabled on the router interface.

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

Fixes

NET Gratuitous Arp Disabled

The router administrator will ensure the router configuration files do not include ip gratuitous-arps command.

Notes:

NET0790 V0003083 CAT III IP directed broadcasts are not disabled.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure IP directed broadcast is disabled on all router interfaces.

Vulnerability Discussion An IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, which is connected directly to the target subnet, can conclusively identify a directed broadcast.

IP directed broadcasts are used in the extremely common and popular smurf, or Denial of Service (DoS), attacks. In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified. This service should be disabled on all interfaces when not needed to prevent smurf and DoS attacks.

Checks

NET Direct Broadcast

IOS Procedure: IP directed broadcast is disabled by default in IOS version 12.0 and higher so the command no ip directed-broadcast will not be displayed in the running configuration—verify that the running configuration does not contain the command ip directed-broadcast. For versions prior to 12.0 ensure the command no ip directed-broadcast is displayed in the running configuration.

Default Finding IP directed broadcasts are not disabled on the following routers:

Details

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

Fixes

NET Direct Broadcast

The router administrator will change the router configuration files to disable the IP directed broadcast on all interfaces.

Notes:

NET0800

V0003084 CAT II

Filter ICMP on external interface

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.

Vulnerability Discussion The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: Host unreachable, Redirect, and Mask Reply.

Checks

NET ICMP Unreachables

Base Procedure:

Review the active configuration to determine if controls have been defined to ensure the router does not send ICMP unreachable, redirects, and mask replies out any external interfaces.

NET0800 - CISCO

For IOS version 12.0 and later review the running configuration of the premise router and ensure the following commands are not present on all external interfaces: ip unreachable, ip redirects, and ip mask-reply. For versions prior to 12.0, ensure the following commands are present: no ip unreachable, no ip redirects, and no ip mask-reply. The configuration should look similar to the following:

```
interface FastEthernet 0/0
ip address 199.36.92.1 255.255.255.252
ip access-group 101 in
no ip redirects
no ip unreachable
no ip mask-reply
```

In addition, host unreachable messages will be sent in reply to black-hole routes. Be sure that the Null0 interface also has no ip unreachable defined if there are static routes destined for this interface.

```
interface null0
no ip unreachable
```

Default Finding Details The following ICMP messages are not disabled on routers external interfaces:

Details

Host unreachable
Redirect
Mask Reply

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

Fixes

NET ICMP Unreachables

The router administrator will change the router configuration files to ensure no ip unreachable, no ip redirects and no ip mask-reply are enabled in the OS.

Notes:

NET0812 **V0005620 CAT III** **NTP clients must receive services from premise**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all internal routers are configured to use the premise router to synchronize time in an external trusted NTP implementation.

Vulnerability Discussion NTP is insecure and without peering within the enclave Network Time Protocol can be used by an attacker to send NTP packets to crash or overload the router.

Checks

NET NTP Client use Premise

Base Procedure: Review the router configurations and verify that NTP clients have been defined to use the premise router.

NET0812 - CISCO

IOS Procedure: Review the router configurations and verify that NTP clients have been defined similar to the following example:
ntp server 129.237.32.2 (source IP address of server)

Default Finding Details The router is not configured to a local NTP server.

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

Fixes

NET NTP Client use Premise

Implement a secure NTP process using a local NTP server.

Notes:

NET0813

V0014671 CAT II

MD5 authentication not used for NTP

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability When the NTP source originates from an internal clock, the router administrator will ensure all routers use MD5 to authenticate the time source.

Vulnerability Discussion Since NTP is used to ensure accurate log file timestamp information, NTP could pose a security risk if a malicious user were able to falsify NTP information. Implementing MD5 authentication between NTP peers can mitigate this risk. When MD5 authentication is enforced, there is a greater level of assurance that NTP updates are from a trusted source.

Checks

NET NTP MD5 use

Base Procedure: Review router configurations to verify NTP sessions are authenticated using MD5.

NET NTP MD5 use IOS

IOS Example:
You should find a configuration similar to the example below:
ntp server 129.237.32.2
...
ntp authenticate
ntp authentication-key 999 md5 xxxxxxxxx
ntp trusted-key 10

Default Finding Details NTP authentication is not implemented when the NTP source originates from an internal clock.

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

Fixes

NET NTP MD5 use

Ensure that routers use MD5 to authenticate the time source from internal clocks.

Notes:

NET0820 V0003020 CAT III DNS servers must be defined for client resolver.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the DNS servers are defined if the router is configured as a client resolver.

Vulnerability Discussion The susceptibility of IP addresses to spoofing translates to DNS host name and IP address mapping vulnerabilities. For example, suppose a source host wishes to establish a Telnet connection with a destination host and queries a DNS server for the IP address of the destination host name. If the response to this query is the IP address of a host operated by an attacker, the source host will establish a connection with the attackers host, rather than the intended target. The user on the source host might then provide logon, authentication, and other sensitive data.

Checks

NET DNS Servers for Client

Base Procedure: Review the running configuration to ensure that DNS servers have been defined if the router had been configured as a client resolver.

NET0820 - CISCO

The configuration should look similar to one of the following examples:

```
! configure as client resolver and specify DNS server
ip domain-lookup
ip name-server 192.168.1.253
```

or

```
! disable client resolver
no ip domain-lookup    Note: ip domain-lookup is enabled by default.
```

Default Finding Details The primary and secondary DNS server addresses are not set on the router.

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

Fixes

NET DNS Servers for Clients

The router administrator will change the router configuration files to include the primary and secondary domain servers for each router.

Notes:

NET0890 **V0003021** **CAT II** **SNMP access is not restricted by IP address**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will restrict SNMP access to the router from only authorized internal IP addresses.

Vulnerability Discussion Detailed information about the network is sent across the network via SNMP. If this information is discovered by attackers it could be used to trace the network, show the networks topology, and possibly gain access to network devices.

Checks

NET SNMP Access Restricted

Base Procedure: Review all router configurations to ensure ACLs are in place to limit SNMP access to specific NMS hosts.

NET0890 - CISCO

IOS EXample:
access-list 10 permit host 7.7.7.5
snmp-server community <clear text string> ro 10

Default Finding Details ACLs are not used to restrict access to SNMP sessions to approved IP addresses.

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

Fixes

NET SNMP Access Restricted

The router administrator will change the router configuration files to include ACLs to limit access to SNMP sessions to allowed IP addresses only.

Notes:

NET0892 **V0003022** **CAT II** **SNMP is blocked at all external interfaces**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure SNMP is blocked at all external interfaces.

Vulnerability Discussion Detailed information about the network is sent across the network via SNMP. If this information is discovered attackers, it could be used to trace the network, show the networks topology, and gain access to network devices.

Checks

NET SNMP External IP Blocked

Verify that the IP addresses permitted SNMP access to the routers belong to the internal network.

Default Finding Details SNMP access is not restricted to the internal network.

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

Fixes

NET SNMP External IP Blocked

The router administrator will change the router configuration files to include to limit access to SNMP sessions to the internal network.

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 xxxxxxxx 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:

NET0897

V0014672 CAT III

Authentication traffic does not use loopback

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating TACACS+ or RADIUS traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. TACACS+, RADIUS messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source TACACS

Base Procedure: Review the configuration and verify the loopback address is used as the source address when originating TACACS+ or RADIUS traffic.

NET Loopback source TACACS IOS

IOS Procedure:

Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255    Note: IOS allows multiple loopback interfaces to be defined.
...
ip tacacs source-interface Loopback0
ip radius source-interface Loopback0
```

Default Finding Details The router's loopback address is not used as the source address when originating TACACS+ or RADIUS traffic.

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

Fixes

NET Loopback source TACACS

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0898

V0014673 CAT III

Syslog traffic is not using loopback address

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating syslog traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. Syslog messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source SYSLOG

Base Procedure: Review the configuration and verify logging data uses the loopback interface.

NET0898 - CISCO

Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255    Note: IOS allows multiple loopback interfaces to be defined.
...
logging on
logging host 192.168.1.100
logging source-interface Loopback0
```

**Default Finding
Details**

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

Fixes

NET Loopback source SYSLOG

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0899

V0014674 CAT III

Loopback addr is not used as the source IP for NTP

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating NTP traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. NTP messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source NTP

Base Procedure: Review the configuration and verify NTP data uses the loopback interface.

NET0899

IOS Procedure: Verify that a loopback address has been configured as shown in the following example:
interface loopback 0
ip address 10.10.2.1 255.255.255.255 Note: IOS allows multiple loopback interfaces to be defined.
...
ntp update-calendar
ntp server 129.237.32.2
ntp server 142.181.31.6
ntp source Loopback0

Default Finding Details Loopback addr is not used as the source IP for NTP.

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

Fixes

NET Loopback source NTP

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0900 V0014675 CAT III SNMP traffic does not use loopback

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating SNMP traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. SNMP messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source SNMP

Base Procedure: Review the configuration and verify SNMP data uses the loopback interface.

NET0900 - CISCO

Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255      Note: IOS allows multiple loopback interfaces to be defined.
...
snmp-server trap-source Loopback0
```

Default Finding Details The router's loopback address is not used as the source address when originating SNMP traffic.

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

Fixes

NET Loopback source SNMP

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0901 V0014676 CAT III Netflow traffic is not using loopback

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating NetFlow traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. Netflow messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source NetFlow

Base Procedure: Review the configuration and verify NetFlow data uses the loopback interface.

NET0901 - CISCO

Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255     Note: IOS allows multiple loopback interfaces to be defined.
...
ip flow-sampling-mode packet-interval 100
ip flow-export destination 192.168.3.33 9991
ip flow-export source Loopback0
```

Default Finding Details The router's loopback address is not used as the source address when originating NetFlow traffic.

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

Fixes

NET Loopback source NewFlow

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0902 **V0014677 CAT III** **FTP/TFTP traffic does not use loopback**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address when originating TFTP or FTP traffic.

Vulnerability Discussion Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of routers. It is easier to construct appropriate ingress filters for router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. TFTP and FTP messages sent to management servers should use the loopback address as the source address.

Checks

NET Loopback source TFTP / FTP

Base Procedure: Review the configuration and verify FTP or TFTP data uses the loopback interface.

NET0902 - CISCO

Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255      Note: IOS allows multiple loopback interfaces to be defined.
...
ip ftp username xxxxxxxxx
ip ftp password 7 xxxxxxxxxxxxxxxxxxxx
ip ftp source-interface Loopback0
...
ip tftp source-interface
```

Default Finding Details The router's loopback address is not used as the source address when originating FTP or TFTP traffic.

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

Fixes

NET Loopback source TFTP / FTP

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0903 V0014681 CAT III BGP peering traffic does not use loopback

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the router's loopback address is used as the source address for BGP peering sessions.

Vulnerability Discussion When the loopback address is used as the source for eBGP peering, the BGP session will be harder to hijack since it is hidden. This makes it more difficult for a hacker to spoof an eBGP neighbor. A hacker must determine the eBGP speaker's source address (among other properties of the session) in order to spoof one of its eBGP neighbors. By using traceroute, a hacker can easily determine the addresses for an eBGP speaker when the IP address of an external interface is used as the source address. The routers within the iBGP mesh should also use loopback addresses as the source address when establishing BGP sessions with peers within its own autonomous system.

Checks

NET Loopback source BGP peerin

Base Procedure: Review the configuration and verify BGP peering data uses the loopback interface.

NET0903 - CISCO

Step 1: Verify that a loopback address has been configured as shown in the following example:

```
interface loopback 0
ip address 10.10.2.1 255.255.255.255      Note: IOS allows multiple loopback interfaces to be defined.
...
router bgp 100
neighbor 200.200.200.2 remote-as 200
neighbor 200.200.200.2 update-source Loopback0
```

Default Finding The router's loopback address is not used as the source address for BGP peering sessions.

Details

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

Fixes

NET Loopback source BGP peerin

Ensure that the router's loopback address is used as the source address when originating traffic.

Notes:

NET0906

V0014683 CAT II

IPv6 Undetermined Transport is not blocked

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the undetermined transport packet is blocked at the perimeter in an IPv6 enclave.

Vulnerability Discussion One of the fragmentation weaknesses known in IPv6 is the undetermined transport packet. This is a packet that contains an undetermined protocol due to fragmentation. Depending on the length of the IPv6 extension header chain, the initial fragment may not contain the layer four port information of the packet.

Checks

NET undetermined Transport

IOS Procedure: Verify that an ACL for IPv6 has been defined to deny packets with unknown or invalid payload, and log all violations. The ACL should be defined on the ingress and egress filters and should look as shown in the following example:

```
ipv6 access-list 600
remark prohibit unknown protocols
deny ipv6 any any undetermined-trans log
...
```

Default Finding Details The undetermined transport packet is not blocked at the perimeter in an IPv6 enclave.

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

Fixes

NET Undetermined Transport

Ensure the undetermined transport command is implemented.

Notes:

NET0907

V0014685 CAT II

IPv6 Routing Header is not blocked

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure the routing header extension is blocked, type 0 is rejected in an IPv6 enclave.

Vulnerability Discussion The Routing header is used by an IPv6 source to specify a list of intermediate nodes that a packet has to traverse on the path to its destination. If the packet cannot take the path, it is returned to the source node in an ICMPv6 unreachable error message. This header supports a function very similar to the IPv4 packet Loose Source Routing. The routing header can be used maliciously to send a packet through a path where less robust security is in place, than through the presumably preferred path by routing protocols. Use of the routing extension header has few legitimate uses other than as implemented by Mobile IPv6. The Routing header is identified by a Next Header value of 43 and should be filtered by type using an ACL.

Checks

NET Routing Header

Verify that an ACL for IPv6 has been defined to deny IPv6 packets that include a Routing Header with Routing Type 0 by all router interfaces. The ACL should be defined on the ingress and egress filters and should look as shown in the following example:

```
IOS Procedure:  
ipv6 access-list 600  
remark prohibit IPv6 routing header  
deny ipv6 any any routing-type 0 log  
...
```

Default Finding The IPv6 routing header extension is not blocked, type 0 is rejected in an IPv6 enclave.

Details

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

Fixes

NET Routing Header

Ensure the undetermined transport command is implemented.

Notes:

NET0928 **V0005607** **CAT II** **Advertising unauthorized Bogon addresses**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.

Vulnerability Discussion It is a common best practice to block packets from an area of IP address space reserved but not yet allocated by the Internet Assigned Numbers Authority (IANA) or a delegated Regional Internet Registry (RIS) are useless or forged for illegitimate purposes.

Checks

NET Route Advertisements

Inspect the router's ACLs against the IANA Unallocated and Reserved IP list and ensure they are applied to the interface if the site is in a permit any posture. If the site is in a deny all posture ensure the permit statements do not allow the bogon addresses identified at the IANA web site. The current IANA listing can be found on the <http://www.iana.org> web site. The IANA IPv4 addresses need to be verified that they are block explicitly or by deny-by-default. The router administrator will have a procedure in place to change or modify the BOGON/Martian list on a monthly basis if in a permit any any posture.

Default Finding Details The site is advertising unauthorized Bogon / Martian addresses.

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

Fixes

NET Route Advertisements

The IAO/NSO will ensure that the site uses only authorized .mil addresses that have been registered and assigned to the activity for advertisements.

Notes:

NET0948 **V0014703** **CAT II** **IPv6 Unique Local Unicast ADDR are not blocked**

8500.2 IA Control: ECSC-1

References: INTEGRATED CONTINUITY PLANNING FOR DEFENSE
INTELLIGENCE

Vulnerability The IAO/NSO will ensure IPv6 Unique Local Unicast Addresses are blocked on the ingress and egress filter, (FC00::7).

Vulnerability Discussion The IANA has assigned the FC00::/7 prefix to Unique Local Unicast addresses. Unique Local Address (ULA) is a routable address that is not intended to be on the Internet. Site border routers and firewalls should be configured to block any packets with ULA source or destination addresses outside of the site. This will ensure that packets with Local IPv6 destination addresses will not be forwarded outside of the site via a default route.

Checks

NET IPv6Unique Local Unicast F

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict the IP addresses explicitly, or inexplicitly. Verify that ingress and egress ACLs for IPv6 have been defined to deny the Unique Local Unicast addresses and log all violations.

Default Finding Details IPv6 Unique Local Unicast addresses are not blocked by the enclave.

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

Fixes

NET IPv6 Unique Local Unicast

The router administrator will configure the router ACLs to restrict IP addresses that contain any Unique Local Unicast addresses.

Notes:

NET0949 **V0005645 CAT II** **Routers are not configured with CEF enabled**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will enable CEF to improve router stability during a SYN flood attack to the network.

Vulnerability Discussion The Cisco Express Forwarding (CEF) switching mode replaces the traditional Cisco routing cache with a data structure that mirrors the entire system routing table. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably when presented with large volumes of traffic addressed to many destinations such as a SYN flood attacks that. Because many SYN flood attacks use randomized source addresses to which the hosts under attack will reply to, there can be a substantial amount of traffic for a large number of destinations that the router will have to handle. Consequently, routers configured for CEF will perform better under SYN floods directed at hosts inside the network than routers using the traditional cache.

Note: Junipers FPC (Flexible PIC Concentrator) architecture with the integrated Packet Forwarding Engine provides similar functionality and capabilities and is far superior than the traditional routing cache that is vulnerable to a DoS attack described above. The forwarding plane on all Juniper M and T Series platforms are built around this architecture and therefore is not configurable. The forwarding plane on all Juniper M and T Series platforms are built around the FPC (Flexible PIC Concentrator) architecture that has similar capabilities as CEF. FPC is not configurable and is totally integrated with the Packet Forwarding Engine; hence, this will always be not a finding.

Checks

NET CEF enabled

IOS Procedure: Review all Cisco routers to ensure that CEF has been enabled. The configuration should like similar to the following: ip cef

CAVEAT: If the site has implemented SYN flood protection for the network using the perimeter firewall, there is not an additional requirement to implement it on the router.

Default Finding Details Router administrator has not configured CEF.

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

Fixes

NET CEF enabled

The IA will ensure that the ip cef command has been configured on Cisco routers.

Notes:

NET0953

V0014705 CAT II

IPv6 routers are not configured with CEF enabled

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will enable CEF to improve router stability during a SYN flood attack in an IPv6 enclave.

Vulnerability Discussion The Cisco Express Forwarding (CEF) switching mode replaces the traditional Cisco routing cache with a data structure that mirrors the entire system routing table. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably when presented with large volumes of traffic addressed to many destinations—such as a SYN flood attacks that. Because many SYN flood attacks use randomized source addresses to which the hosts under attack will reply to, there can be a substantial amount of traffic for a large number of destinations that the router will have to handle. Consequently, routers configured for CEF will perform better under SYN floods directed at hosts inside the network than routers using the traditional cache.

Note: Juniper's FPC (Flexible PIC Concentrator) architecture with the integrated Packet Forwarding Engine provides similar functionality and capabilities and is far superior than the traditional routing cache that is vulnerable to a DoS attack described above. The forwarding plane on all Juniper M and T Series platforms are built around this architecture and therefore is not configurable. The forwarding plane on all Juniper M and T Series platforms are built around the FPC (Flexible PIC Concentrator) architecture that has similar capabilities as CEF. FPC is not configurable and is totally integrated with the Packet Forwarding Engine; hence, this will always be not a finding.

Checks

NET IPv6 CEF enabled

IOS Procedure: Review all Cisco routers to ensure that CEF has been enabled. The configuration should like similar to the following: ipv6 cef

Default Finding IPv6 routers are not configured with CEF enabled.

Details

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

Fixes

NET IPv6 CEF enabled

The IAO will ensure that the ipv6 cef command has been configured on Cisco routers.

Notes:

NET0965 V0005646 CAT II Must limit TCP connection requests wait times

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will set the maximum wait interval for establishing a TCP connection request to the router to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.

Vulnerability Discussion Upon responding to the initial SYN packet that requested a connection to the router for a specific service (i.e., Telnet, SSH, BGP, etc) with a SYN ACK, a Cisco router will wait 30 seconds for the ACK from the requesting host that will establish the TCP connection. A more aggressive interval for waiting for the TCP connection to be established will reduce the risk of putting the router out of service during a SYN flood attack directed at a Cisco router. The wait time can be adjusted using the ip tcp syn wait-time command that should be set to 10 seconds or less. If the router does not have any BGP connections with BGP neighbors across WAN links, this value could be set to an even more aggressive interval.

Checks

NET TCP synwait-time 10

Base Procedure: Review the configuration and verify the TCP connection request to the device is set to 10 seconds or less or a rate limit for TCP Syn has been implemented.

NET0965 - CISCO

IOS Procedure:

Review the router configuration to ensure the ip tcp synwait-time command is in place to monitor TCP connection requests to the router. The configuration should look similar to the following:

```
ip tcp synwait-time 10
```

Default Finding Details Router administrator has not configured the router to protect itself against a TCP SYN flood attack.

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

Fixes

NET TCP synwait-time 10

The IAO will ensure that the ip tcp synwait-time has been configured on Cisco routers or rate limiting of TCP SYN traffic on Juniper routers.

Notes:

NET1020

V0003000 CAT III

A log or syslog statement does not follow all deny

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all attempts to any port, protocol, or service that is denied is logged.

Vulnerability Discussion Auditing and logging are key components of any security architecture. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment. Auditing the actions on routers provides a means to recreate an attack, or simply identify a misconfigured configuration.

Checks

NET Log Denied PPS denied

Base Procedure: Review the running configuration and verify that both the router's ingress and egress ACLs have a log keyword following every deny, discard or reject statement.

NET1020

```
access-list 100 permit tcp . . . . .
access-list 100 permit tcp . . . . .
.....
access-list 100 deny any log
```

Default Finding Details A log or syslog statement does not follow all deny, discard, or reject statements in the ingress or egress filter.

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

Fixes

NET Log Denied PPS denied

The IAO will ensure that all deny statements in the ACL of the router have a log statement that follows.

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 0-6 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 6. By specifying informational, all severity levels above will be included.

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

NET1021 - CISCO

logging on
logging host 192.168.1.22
logging console critical
logging trap informational
logging facility local7

Note: The command logging on is the default. If you see the command no logging on, then all logging except console logging will be disabled. The default trap level is informational so if a logging trap command were not present this would imply logging trap informational.

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 0-6 and send syslog messages to the syslog server.

Notes:

NET1028 **V0003033 CAT III** **Restrict messages to the Syslog Server.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The syslog administrator will configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).

Vulnerability Discussion Restrict access to the Syslog server by approved IP addresses/users. If an unauthorized user gains access to the Syslog server and it is compromised, access to critical network information would be available. This information could be used to mount attacks against the network.

Checks

NET Syslog Srv Restrict Access

Base Procedure: Review the syslog server configuration to ensure that it is configured to accept messages from only authorized devices.

NET1028 - CISCO

```
access-list 120 deny udp any x.x.x.x x.x.x.x eq syslog
```

Default Finding Details The syslog server is not configured to restrict messages, via IP ACLs, from unauthorized devices.

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

Fixes

NET Syslog Srv Restrict Access

The router administrator will configure the router to restrict syslog server messages to only authorized devices (restricting access via source and destination IP address).

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 IAO/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 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 router 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 network administrator will ensure that the timeout for unattended console port is set for no longer than 10 minutes via the exec-timeout command.

Notes:

NET1629 V0007011 CAT III Ensure that the router's auxiliary port is disable

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The system administrator will ensure that the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.

Vulnerability Discussion The use of POTS lines to modems connecting to network devices provides clear text of authentication traffic over commercial circuits that could be captured and used to compromise the network. Additional war dial attacks on the device could degrade the device and the production network.

Secured modem devices must be able to authenticate users and must negotiate a key exchange before full encryption takes place. The modem will provide full encryption capability (Triple DES) or stronger. The technician who manages these devices will be authenticated using a key fob and granted access to the appropriate maintenance port, thus the technician will gain access to the managed device (router, switch, etc.). The token provides a method of strong (two-factor) user authentication. The token works in conjunction with a server to generate one-time user passwords that will change values at second intervals. The user must know a personal identification number (PIN) and possess the token to be allowed access to the device.

Checks

NET Aux Port Disabled

Base Procedure: View the router's configuration to ensure that the auxiliary port is disabled unless a secured modem providing encryption and authentication is connected.

NET1629 - CISCO

The following commands disable the aux port:

Line aux 0
No exec
Transport input none

Default Finding Details The device auxiliary port is not disabled or a secured modem providing encryption and authentication is not connected.

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

Fixes

NET Aux Ports Disabled

The router administrator will disable the auxiliary ports on all routers.

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 router's configuration to ensure that the VTY ports require a login prompt.

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 (except console line; line con 0). 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 to the router 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

Encryption required on In-band

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 an encryption 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 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 in-band management interface 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 network administrator will ensure that the timeout for unattended consoles and telnet ports 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 connection attempts to the telnet ports 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 add the log parameter to all access lists protecting the VTY ports.

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 router administrator verify the timeout is set for 60 seconds or less. Sets a timeout period in seconds. 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 router 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 (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:

NET1930

V0015266 CAT II

Egress interface is not the only accepting IPv6

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the internal router's egress interface is the only interface accepting native IPv6 traffic.

Vulnerability Discussion Because native IPv6 is not permitted in the Intra-Enclave Security Zone in this architecture, it must be encapsulated inside of IPv4. The IPv6 in IPv4 tunnel is established between Enclave Interior devices.

Review the diagram in STIG. The following diagram prevents native IPv6 from reaching the perimeter router and the DISN core. IPv6 traffic flow will enter the internal router egress interface only toward the defined enclave-security zone.

Checks

NET Security Zone Egress

If the enclave has established tunnels for IPv6, review the architecture design to determine if it conforms to the diagram in the STIG (GRE or VPN). Ensure IPv6 data flow leaving the enclave passes through the Intra-Enclave Security Zone. IPv6 traffic should not be leaving the enclave. It should all be encapsulated in the tunnel.

Default Finding Details Internal router's egress interface is not the only interface accepting native IPv6 traffic

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

Fixes

NET Security Zone Egress

Modify IPv6 data flow exiting the enclave to pass through the enclave security zone.

Notes:

NET1931

V0015269 CAT II

Ingress interfaces must not allow native IPv6

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the internal router's ingress interfaces does not allow native IPv6 traffic.

Vulnerability Discussion Because native IPv6 is not permitted in the Intra-Enclave Security Zone in this architecture, it must be encapsulated inside of IPv4. The IPv6 in IPv4 tunnel is established between Enclave Interior devices.

Review the diagram in STIG. The following diagram prevents native IPv6 from reaching the perimeter router and the DISN core. IPv6 traffic flow will enter the internal router egress interface only toward the defined enclave-security zone. IPv6 traffic will not enter the ingress interface.

Checks

NET Security Zone Ingress

If the enclave has established tunnels for IPv6, review the architecture design to determine if it conforms to the diagram in the STIG (GRE or VPN). Ensure IPv6 data flow entering the enclave passes through the Intra-Enclave Security Zone. IPv6 traffic should not be entering the enclave. It should all be encapsulated in the tunnel.

Default Finding Details Internal router's ingress interfaces must not allow native IPv6 traffic.

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

Fixes

NET Security Zone Ingress

Modify IPv6 data flow entering the enclave to pass through the enclave security zone.

Notes:

NET1934 **V0015272** **CAT II** **Ingress interfaces must not allow IPv6 NLRI**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the internal router's ingress interfaces do not allow native IPv6 NLRI exchanges.

Vulnerability Discussion Because native IPv6 is not permitted in the Intra-Enclave Security Zone in this architecture, it must be encapsulated inside of IPv4. The IPv6 in IPv4 tunnel is established between Enclave Interior devices.

Review the diagram in STIG. The following diagram prevents native IPv6 from reaching the perimeter router and the DISN core. NLRI from BGP will not reach the internal router.

Checks

NET Security Zone NLRI

If the enclave has established tunnels for IPv6, review the architecture design to determine if it conforms to the diagram in the STIG (GRE or VPN). Ensure IPv6 NLRI is not reaching the internal router by verifying BGP IPv6 neighbor and IPv6 address-family definitions are not defined on the internal router.

Default Finding Details Internal router's ingress interfaces must not allow IPv6 NLRI exchanges.

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

Fixes

NET Security Zone NLRI

Remove BGP IPv6 statements from the internal router.

Notes:

NET1940 **V0015282** **CAT II** **Perimeter router must not route native IPv6 traffi**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability IAO/NSO will ensure the perimeter router does not route native IPv6 traffic during MO2.

Vulnerability Discussion During MO2 IPv6 traffic must be contained within the enclave.

Checks

NET MO2 IPv6 routing

During MO2 the perimeter router must not route IPv6 traffic. Review the router configuration or have the router administrator display the route table to determine if the perimeter router is routing IPv6 traffic.

Default Finding Details Perimeter router must not route native IPv6 traffic.

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

Fixes

NET MO2 IPv6 routing

Remove the configuration from the router that enables routing.

Notes:

NET1951 V0015288 CAT II ISATAP tunnels must terminate at interior router

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure ISATAP tunnels terminate at an interior router.

Vulnerability Discussion ISATAP is an automatic tunnel mechanism that does not provide authentication such as IPsec. As a result of this limitation ISATAP is thought of as a tool that is used inside the enclave among trusted hosts, which would limit it to internal attacks. ISATAP is a service versus a product and is readily available to most users. If a user knows the ISATAP router IP address they can essentially get onto the IPv6 intranet. To control the vulnerability of this tunnel mechanism it is critical to control the use of protocol 41 and use IPv4 filters to control what IPv4 nodes can send protocol 41 packets to an ISATAP router interface. Although the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as IPv6 6to4 tunneling, ISATAP is designed for transporting IPv6 packets within a site, not between sites.

ISATAP will not be allowed to cross the enclave boundary. Referencing the ISATAP diagram in the STIG, ISATAP tunnels connections must terminate at the I1.B interface. Then a single tunnel can be created to transport the traffic from the I1.A interface to the P1.B interface. This prevents unauthorized tunneling through the core and allows the NIDS to analyze the information in a supported mode.

Checks

NET ISATAP termination

Base Procedure: Ensure the ISATAP tunnel termination faces the Enclave Security Zone containing the IDS and Firewall towards the Perimeter router.

NET ISATAP termination IOS

IOS Procedure: The following example configures an ISATAP tunnel. Review the STIG diagram and verify the configuration I1A is the interface facing the Intra Enclave Security Zone containing the IDS and Firewall towards the Perimeter router. It should not be the interface facing downstream towards the enclave. In the configuration example Ethernet interface 1 should be interface I1A in the STIG diagram.

```
interface tunnel 1
 tunnel source ethernet 1
 tunnel mode ipv6ip isatap
 ipv6 address 2001:0DB8::/64 eui-64
 no ipv6 nd suppress-ra
```

Default Finding Details ISATAP tunnels must terminate at interior router

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

Fixes

NET ISATAP termination

Correct the configuration to terminate the ISATAP tunnel at the Intra Enclave Security Zone.

Notes:

NET1970

V0015294 CAT I

Teredo is not blocked by filtering UDP port 3544

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure Teredo is blocked by filtering UDP protocol 17 port 3544 in the enclave environment.

Vulnerability Discussion Teredo is a tunneling mechanism that allows nodes located behind NAT devices to obtain global IPv6 connectivity. In a Teredo implementation the IPv6 packet is encapsulated in IPv4 UDP. Teredo IP addresses can be recognized by their well-know prefix 2001:0000::/32 or by a previous Microsoft allocation 3ffe831f::/32 followed by a routable IPv4 address. There is a lot of overhead associated with Teredo and many components within the technology itself that can be attacked forcing the technology to use intensive resources, which makes it acceptable to DoS attacks. Dual-stack Teredo clients previously hidden by NAT and assumed to be safe by NAT are fully accessible to the v6Internet with a Teredo implementation that opens holes into the NAT architecture. Teredo clients are also known to become backdoors. Teredo is not considered an acceptable transition mechanism within the DoD network and will be blocked by filtering protocol 17, port 3544.

Checks

NET Teredo

Ensure UDP protocol 17 port 3544 is not allowed in the enclave.

Default Finding Teredo is not blocked by filtering UDP protocol 17 port 3544.

Details

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

Fixes

NET Teredo

Block UDP protocol 17 port 3544.

Notes: