



# Network Security Checklist - Cisco Perimeter Router

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

<b>Site Name</b>	
<b>Address</b>	
<b>Phone</b>	

<b>Position</b>	<b>Name</b>	<b>Phone Number</b>	<b>Email</b>	<b>Area of Responsibility</b>
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 IA/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 IA/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:

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

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

**Checks**

**NET Registered IP Address**

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

**Default Finding Details**

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

**Fixes**

**NET Registered IP Address**

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

Notes:

**NET0185**                      **V0003157 CAT II**                      **Unauthorized addresses within Siprnet enclave**

8500.2 IA Control: DCSP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

**Vulnerability Discussion** The SIPRNet enclave will have full reachability from SCAP office to perform remote scans.

**Checks**

**NET Sivr RFC1918**

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

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

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

**Fixes**

**NET Sivr RFC1918**

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

Notes:

**NET0190**

**V0003005 CAT III**

**LAN addresses are not protected from the public.**

8500.2 IA Control: EBBD-1, EBBD-2, EBBD-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:

**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 IAQ/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:

**NET0410                      V0003035 CAT II                      BGP sessions are not restricted.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict BGP connections to known IP addresses of neighbor routers from trusted Autonomous Systems.

**Vulnerability Discussion** Advertisement of routes by an autonomous system for networks that do not belong to any of its trusted peers pulls traffic away from the authorized network. This causes DoS on the network that allocated the block of addresses and may cause DoS on the network that is inadvertently advertising it as the originator. It is also possible that a misconfigured or compromised router within the network could re-distribute IGP routes into BGP thereby leaking internal routes.

**Checks**

**NET BGP Route Filtering**

Base Procedure

Review the running configuration to ensure that BGP connections are only from known neighbors in a trusted AS by restricting TCP port 179 to specific IP addresses.

**NET0410 - CISCO**

Using an Ingress ACL

```
interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group 101 in
.
access-list 101 permit tcp host 192.168.1.1 host 192.168.1.2 eq 179
.
access-list 101 deny ip any any
```

Using an IP Receive ACL The IP Receive ACL feature can also be used to filter traffic that is destined for the router. The filtering occurs after any ingress ACL on the interface in which the traffic enters. Following is an example using an IP Receive ACL:

```
ip receive access-list 100
access-list 100 deny icmp any any fragments
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 permit tcp host 192.168.1.1 any eq bgp
access-list 100 deny ip any any
```

Note: This feature is currently only supported on 7500 and 12000 series routers with 12.0(24)S and 12.0(22)S respectively.

**Default Finding Details** The router administrator is not using an ingress ACL to block unauthorized BGP connection attempts.

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

**Fixes**

**NET BGP Route Filtering**

The router administrator will create ingress ACL to block any unauthorized BGP connection attempts.

Notes:

**NET0412                      V0014666   CAT II                      Unique keys are not used for eBGP authentication**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** If multiple eBGP peers are defined in the network, the IAO will ensure all eBGP neighbor authentications are configured with unique passwords when TCP MD5 Signature option is implemented

**Vulnerability Discussion** If the same keys are used between eBGP neighbors, the chance of a hacker compromising any of the BGP sessions increases. It is possible that a malicious user exists in one autonomous system who would know the key used for the eBGP session. This user would then be able to hijack BGP sessions with other trusted neighbors.

**Checks**

**NET Unique eBGP keys**

Interview the IAO and router administrator to determine if unique keys are being used.

**Default Finding Details** Unique keys are not used for eBGP authentication.

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

**Fixes**

**NET Unique eBGP keys**

Configure all eBGP routers with unique keys for each eBGP neighbor that it peers with.

Notes:

**NET0422                      V0014667   CAT III                      Keys expiration exceeds 180 days.**

8500.2 IA Control: IAKM-1, IAKM-2, IAKM-3

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure a rotating key does not have a duration exceeding 180 days.

**Vulnerability Discussion** If the MD5 keys used for routing protocols are guessed, the malicious user could create havoc within the network and between subscribing networks by advertising incorrect routes and redirecting traffic. Changing the keys frequently reduces the risk of them eventually being guessed.

**Checks**

**NET MD5 Key Management**

Review key expirations. When configuring authentication for routing protocols that provide key chains, configure two rotating keys with overlapping expiration dates, both with 180-day expirations.

**Default Finding Details** Keys expiration exceeds 180 days.

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

**Fixes**

**NET MD5 Key Management**

The IAO or SA will ensure a key has an expiration of 180 days or less.

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:

**NET0434**

**V0015433 CAT II**

**Group profiles defined in AAA server**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure the AAA authentication method implements user authentication.

**Vulnerability** Group accounts are not permitted.

**Discussion**

---

**Checks**

**NET AAA Group accounts**

Review the AAA server configuration. Attempt to identify suspicious group profile definitions that do not meet the accounts user-naming convention. Example:supr-user. Below is an example of what an SA profile may be associated.

Group Profile Information

```
group = rtr_super{  
  profile_id = 40  
  profile_cycle = 1  
  service=shell {  
    default cmd=permit  
    cmd=debug {  
      deny all  
      permit .*  
    }  
  }  
}
```

Below is an example of the user definition that should be assigned with a valid ID, (not rtr-geek). Look for group accounts here:

```
user = rtr-geek{  
  profile_id = 45  
  profile_cycle = 1  
  member = rtr_super  
  password = des "*****"  
}
```

---

**Default Finding** Group profiles defined in AAA server.

**Details**

---

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

**Fixes**

**NET AAA Group Accounts**

Remove all group profiles from the AAA server.

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:

---

---

**NET0460**

**V0003056 CAT I**

**Group accounts or user accounts without passwords**

8500.2 IA Control: IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

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

---

**Checks**

**NET Group Accounts**

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

---

**Default Finding  
Details**

---

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

**Fixes**

**NET Group Accounts**

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

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

Notes:

**NET0465**

**V0003057 CAT II**

**Assign lowest privilege level to user accounts.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

**Vulnerability Discussion** By not restricting 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:

**NET0470**                      **V0003058**   **CAT II**                      **Unnecessary or unauthorized router accounts exist.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

**Checks**

**NET Account Administration**

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

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

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

**Fixes**

**NET Account Administration**

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

Notes:

**NET0580**                      **V0004583**   **CAT III**                      **Password required on the JUNOS diagnostic port.**

8500.2 IA Control: IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure a password is required to gain access to the router's diagnostics port.

**Vulnerability Discussion** If unauthorized users gain access to the routers diagnostic port, it is possible to disrupt service.

**Checks**

**NET JUNOS Diagnostic Port**

IOS Procedure: N/A A Cisco router does not have a diagnostics port.

JUNOS Procedure: Review the router configuration to ensure a password is required when gaining access to the diagnostics port similar to the following:

```
[edit system]
diag-port-authentication {
  encrypted-password "xxxxxxxxxxxxx"; # SECRET-DATA
}
```

**Default Finding Details** No password required to gain access to the routers diagnostics port.

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

**Fixes**

**NET JUNOS Diagnostic Port**

The router administrator will ensure that a password is required to access the routers diagnostic port.

Notes:

**NET0590**

**V0003061 CAT III**

**Enable secret passwords are not unique.**

8500.2 IA Control: IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure the enable secret password does not match any other username password, enable password, or any other enable secret password.

**Vulnerability Discussion** Without unique enable secret passwords on each router, the chance that a password will be compromised is increased. If an employee is terminated or leaves employment for another reason, if the password they are familiar with is changed on one router, it may still exist on other routers. This may lead to an increased ability to compromise the remaining routers. Denial of service, interception of sensitive information, or other destructive actions could take place.

---

**Checks**

**NET Enable Secret Unique**

IOS Procedure: Interview the router administrators to see if this is being enforced on all Cisco routers.

JUNOS Procedure: This is NA for Juniper routers as there is no enable mode passwords—that is, there is no password prompt to enter edit or configuration mode.

---

**Default Finding Details** The Enable secret password is not unique on each router.

---

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

**Fixes**

**NET Enable Secret Unique**

The router administrator will configure each router with a unique enable secret password and remove all others.

Notes:

**NET0600**

**V0003062 CAT I**

**Passwords are viewable when displaying the router**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).

**Vulnerability Discussion** Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that all router passwords are encrypted so they cannot be intercepted by viewing the console. If the router network is compromised, then large parts of the network could be incapacitated with only a few commands.

---

**Checks**

**NET Type 5 encryption**

IOS Procedure: Examine all Cisco router configurations to determine if the global command service password-encryption is present.

JUNOS Procedure: For JUNOS, all passwords are always shown as encrypted; hence, this would never be a finding.

---

**Default Finding Details** The service password-encryption option is not being utilized on the router.

---

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

**Fixes**

**NET Type 5 encryption**

The router administrator will configure each router using the service password encryption option. Service password-encryption is the required global config mode command.

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:

---

**NET0728**                      **V0005617**   **CAT III**                      **DHCP service is not disabled on premise**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure DHCP Services are disabled on premise routers.

**Vulnerability Discussion** By sending a large packet to the Dynamic Host Configuration Protocol (DHCP) port it is possible to freeze the routers processing engine.

---

**Checks**

**NET DHCP disabled**

IOS Procedure: Review all Cisco router configurations to verify that no service dhcp is found. Note: Service DHCP is enabled by default.

---

**Default Finding Details** DHCP Service must be disabled.

---

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

**Fixes**

**NET DHCP Disabled**

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

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:

**Details**

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 Details** IP directed broadcasts are not disabled on the following routers:

---

**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:

**NET0802                      V0014670   CAT II                      IPv6 Filter ICMPv6 on external interface**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure ICMPv6 unreachable notifications, and redirects are disabled on all external interfaces of the premise router.

**Vulnerability Discussion** The Internet Control Message Protocol version 6 (ICMPv6) supports IPv6 traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMPv6 messages under a wide variety of conditions. ICMPv6 messages are commonly used by attackers for network mapping and diagnosis: Host unreachable, and Redirect.

---

**Checks**

**NET ICMPv6 Unreachables**

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

**NET0802 - CISCO**

Ensure the following commands are not present on all external interfaces: ipv6 unreachables and ipv6 redirect,. Ensure the following commands are present: no ipv6 unreachable and no ipv6 redirects. 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 ipv6 redirects
no ipv6 unreachables
```

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 unreachables
```

---

**Default Finding Details** ICMPv6 unreachable notifications, and redirects are not disabled.

---

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

**Fixes**

**NET ICMPv6 Unreachables**

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

Notes:

**NET0810**                      **V0003019 CAT III**                      **Two NTP servers have not been specified**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure that two Network Time Protocol (NTP) servers are defined on the premise router to synchronize its time.

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

---

**Checks**

**NET NTP - Two required**

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

**NET0810 - CISCO**

```
ntp update-calendar
ntp server 129.237.32.2
ntp server 142.181.31.6
```

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

---

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

---

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

**Fixes**

**NET NTP Two required**

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

Notes:

**NET0811**

**V0005619 CAT II**

**Router acting as NTP server for external client**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure that the premise router is acting as an NTP server for only internal clients.

**Vulnerability** The NTP time-servers can not provide services for external clients due to the high vulnerability.

**Discussion**

---

**Checks**

**NET NTP Internal Clients Only**

Procedure: If NTP Servers are defined, review the router configurations and verify that NTP servers have been defined for internal clients.

---

**Default Finding** The NTP server is defined to service external clients.

**Details**

---

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

**Fixes**

**NET NTP Internal Clients Only**

Install the server to service internal clients only.

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:

**NET0910                      V0005731   CAT II                      Router is not compliant with DOD Instr. 8551.1**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The SA will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in Appendix C and DoD Instruction 8551.1 for all ports and protocols required for operational commitments.

**Vulnerability Discussion** Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

If the router is in a Deny-by-Default posture and what is allowed through the router filtering is IAW DoD Instruction 8551.1 and if the permit rule is explicitly defined with explicit ports and protocols allowed, then all requirements related to PPS being blocked would be satisfied.

When the site is in an allow-all posture, all filter statements need to be verified for compliance with DoD Instruction 8551.1, and all PPS that are mandated to be blocked will have a rule created to block these ports and protocols.

---

**Checks**

**NET 8551.1 Ports & Protocols**

Base Procedure: Review the running or active configuration of the premise router and verify that the router's filters are IAW DoD Ports Protocols Services Category Assignment List (PPS CAL) <http://iase.disa.mil/ports/index.html>.

1. Determine Boundary- Determined by Connectivity, not Destination. ACLs use source and destination addresses. PPS defines boundary by physical connectivity. All Federal Agencies are not DOD!
2. NOTE on Enclave to Enclave: If data traffic between Enclaves transverses a router not owned by the Enclave's DAA then it falls into the "Boundary 7&8 DoD Network to Enclave or other applicable category for that particular connectivity.
3. Block by specifying ports on permit statements when in deny-by-default or explicitly block all known red ports.
4. All ports and protocols allowed into the enclave should be registered in the PPS database.

Review the premise router configuration to ensure filters are in place on inbound IP addresses, filtered to permit only green or yellow ports. Red and yellow ports are permitted with conditions noted on the Category Assignment List (CAL). A DSAWG 2 year expiration date listed on the PPS CAL will indicate expiration of permits for particular red ports.

**NET0910 - CISCO**

The router configuration should look similar to following highlighted:

```

interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.
access-list 100 permit tcp [external network] [wildcard mask] any eq ##
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 deny ip any any log

```

---

**Default Finding Details** Ingress and egress ACLs do not restrict traffic in accordance with the guidelines contained in Appendix C and DoD Instruction 8551.1.

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

**Fixes**

**NET 8551.1 Ports & Protocols**

The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in DOD Instruction 8551.1 for all services and protocols required for operational commitments.

Notes:

**NET0911 V0003026 CAT II Inbound ICMP messages are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The System Administrator can permit inbound ICMP messages Echo Reply (type 0), ICMP Destination Unreachable – fragmentation needed (type 3 - code 4), Source Quench (type 4), Time Exceeded (type 11), and Parameter Problem (type 12). All other inbound ICMP messages are prohibited. The following exception: All ICMP messages must be denied from external AG addresses.

**Vulnerability Discussion** Scanning will usually be the major stage of an information gathering process a malicious computer attacker will launch against a targeted network. With this stage the malicious computer attacker will try to determine what the characteristics of the targeted network are. Techniques, such as host detection, service detection, network topology mapping, and operating system fingerprinting are often used. The data collected will be used to identify those Hosts (if any) that are running a network service, which may have a known vulnerability. This vulnerability may allow the malicious computer attacker to execute a remote exploit in order to gain unauthorized access to those systems. This unauthorized access may become the focal point to the whole targeted network.

**Checks**

**NET ICMP Ingress Filter**

Base Procedure: Review the configuration and ensure only approved ICMP types and codes are permitted into the enclave. Use source and destination filtering where appropriate. Apply the ICMP fragment filter to prevent DOS.

**NET0911 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
....
! Specifically block ICMP fragments
access-list 100 deny icmp any any fragments log
! Allow inbound ping response to edge router interface
access-list 100 permit icmp any host 199.36.92.1 echo-reply
! Allow inbound ping response to public server interface
access-list 100 permit icmp any host 199.36.90.10 echo-reply
! Allow Path MTU to function
access-list 100 permit icmp any any packet-too-big
! Allow flow control
access-list 100 permit icmp any any source-quench
! Allow time exceeded messages for loops
access-list 100 permit icmp any any time-exceeded
! Allow bad header message to return
access-list 100 permit icmp any any parameter-problem
! And explicitly block all other ICMP packets
access-list 100 deny icmp any any log
```

**Default Finding Details** Ingress filters are not configured to block exploitable ICMP messages types.

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

**Fixes**

**NET ICMP Ingress Filter**

The router administrator will configure the router to include controls to block inbound exploitable ICMP traffic message types.

Notes:

**NET0912                      V0003027   CAT II                      Outbound ICMP traffic is not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The System Administrator can permit outbound ICMP messages Source Quench (type 4), Echo Request (type 8), and Time Exceeded (type 11). All other outbound ICMP messages are prohibited. The following exception: All ICMP messages must be denied to external AG addresses.

**Vulnerability Discussion** Scanning will usually be the major stage of an information gathering process a malicious computer attacker will lunch against a targeted network. With this stage the malicious computer attacker will try to determine what the characteristics of the targeted network are. Techniques, such as host detection, service detection, network topology mapping, and operating system fingerprinting are often used. The data collected will be used to identify those Hosts (if any) that are running a network service, which may have a known vulnerability. This vulnerability may allow the malicious computer attacker to execute a remote exploit in order to gain unauthorized access to those systems. This unauthorized access may become the focal point to the whole targeted network.

**Checks**

**NET ICMP Egress Filter**

Base Procedure: Review the configuration and ensure only approved ICMP types are permitted to exit the enclave. Use source and destination filtering where appropriate.

**NET0912 - CISCO**

```
interface FastEthernet 0/0
description downstream link to our network
ip address 199.36.90.1 255.255.255.0
ip access-group 102 in
.....
! Allow outbound ping request from LAN subnet
access-list 102 permit icmp 199.36.90.0 0.0.255.255 any echo-request
! Allow Path MTU to function
access-list 102 permit icmp any any packet-too-big
! Allow flow control
access-list 102 permit icmp any any source-quench
! Allow time exceeded messages for loops
access-list 102 permit icmp any any time-exceeded
! And explicitly block all other ICMP packets
access-list 102 deny icmp any any log
```

**Default Finding** Egress ACLs are not configured to block all outbound ICMP message types other than Source Quench (type 4), Echo Request (type 8), and Time Exceeded (type 11).  
**Details**

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

**Fixes**

**NET ICMP Egress Filter**

The router administrator will configure the router to include controls to block outbound ICMP traffic message types.

Notes:

**NET0915                      V0014686   CAT II                      Inbound ICMPv6 messages are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The system administrator can permit inbound ICMPv6 messages Packet-too-big (type 2), Time Exceeded (type 3), Parameter Problem (type 4), Echo Reply (type 129), Network Discovery (type 135-136), Router, Node Response (type140). Remaining ICMPv6 messages must be blocked inbound.

**Vulnerability Discussion** Scanning will usually be the major stage of an information gathering process a malicious computer attacker will lunch against a targeted network. With this stage the malicious computer attacker will try to determine what the characteristics of the targeted network are. Techniques, such as host detection, service detection, network topology mapping, and operating system fingerprinting are often used. The data collected will be used to identify those Hosts (if any) that are running a network service, which may have a known vulnerability. This vulnerability may allow the malicious computer attacker to execute a remote exploit in order to gain unauthorized access to those systems. This unauthorized access may become the focal point to the whole targeted network.

**Checks**

**NET ICMP Ingress Filter**

Base Procedure:

Review the configuration and ensure only approved ICMP types and codes are permitted into the enclave. Use source and destination filtering where appropriate. Apply the ICMP fragment filter to prevent DOS.

**NET0915 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of
....
remark Specifically block ICMP fragments
deny icmp any any fragments log
remark Allow inbound ping response to edge router interface
permit icmp any 2001:db8:60::f14:65a1 echo-reply
remark Allow inbound ping response to public server interface
permit icmp any 2001:db8:60::f14:65b1 echo-reply
remark Allow Path MTU to function
permit icmp any any packet-too-big
remark Allow time exceeded messages for loops
permit icmp any any time-exceeded
remark Allow bad header message to return
permit icmp any any parameter-problem
remark ND ICMP types generally, but not RD
permit icmp any any nd-na
permit icmp any any nd-ns
remark And explicitly block all other ICMP packets
deny ipv6 any any log
```

**Default Finding** Required ICMP filtering is not being implemented.  
**Details**

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

**Fixes**

**NET ICMP Ingress Filter**

The router administrator will configure the router to include controls to block inbound exploitable ICMP traffic message types.

Notes:

**NET0916**

**V0014687 CAT II**

**Outbound ICMPv6 traffic is not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The system administrator can permit outbound ICMPv6 messages Packet-too-big (type 2), Echo Request (type 128), MLD (130-132), Network Discovery (type 135-136), Router Discovery (type 133-134), Node Info Query (type139).

**Vulnerability Discussion** Scanning will usually be the major stage of an information gathering process a malicious computer attacker will launch against a targeted network. With this stage the malicious computer attacker will try to determine what the characteristics of the targeted network are. Techniques, such as host detection, service detection, network topology mapping, and operating system fingerprinting are often used. The data collected will be used to identify those Hosts (if any) that are running a network service, which may have a known vulnerability. This vulnerability may allow the malicious computer attacker to execute a remote exploit in order to gain unauthorized access to those systems. This unauthorized access may become the focal point to the whole targeted network.

**Checks**

**NET ICMP Egress Filter**

Base Procedure: Review the configuration and ensure only approved ICMP types are permitted to exit the enclave. Use source and destination filtering where appropriate.

**NET0916 - CISCO**

IOS example

```
interface FastEthernet 0/0
description downstream link to our network
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
.....
remark Allow outbound ping request from LAN subnet
permit icmp 2001:db8:60::/44 2000::/3 echo-request
remark Allow Path MTU to function
permit icmp 2001:db8:60::/44 2000::/3 packet-too-big
remark Allow flow control
permit icmp 2001:db8:60::/44 2000::/3 source-quench
remark Allow time exceeded messages for loops
permit icmp 2001:db8:60::/44 2000::/3 time-exceeded
remark Allow ND ICMP types generally, but not RD
permit icmp any any nd-na
permit icmp any any nd-ns
remark Explicitly block all other ICMP packets
deny icmp any any log-input
remark And explicitly deny by default
deny ipv6 any any log-input
```

**Default Finding Details** Required outbound ICMPv6 traffic is not blocked.

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

**Fixes**

**NET ICMP Egress Filter**

The router administrator will configure the router to include controls to block outbound ICMP traffic message types.

Notes:

## NET0918 V0003028 CAT III Inbound traceroutes are not blocked

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will block all inbound traceroutes to prevent network discovery by unauthorized users.

**Vulnerability Discussion** Traceroute is a utility that prints the IP addresses of the routers that handle a packet as the packet hops along the network from source to destination. An attacker can use traceroute responses to create a map of the subnets and hosts behind the router, just as they could do with pings, which are ICMP Echo Reply messages. The traditional traceroute sends UDP packets to a target host and is dependent on receiving several TTL-expired responses from routers along the path and an ICMP port-unreachable message from the target host. Traceroute uses on its first packet UDP port number 33434 for the destination port and the UDP port number increments by one for each subsequent packet. Therefore, deny inbound traceroute by including a rule in the inbound interface access list to block UDP ports 33434 through 33534.

---

### Checks

#### NET Traceroutes blocked

Base Procedure: Review the premise router configuration to ensure that an ingress ACL is in place to block inbound UDP 33400 through 34400, which are the ports commonly used by the traditional traceroute application.

#### NET0918 - CISCO

```
interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.
access-list 100 deny udp any any range 33400 34400 log
access-list 100 deny ip any any
```

There are two methods that can be used to block the new inbound traceroute request by a Cisco router: IP Options Selective Drop Feature, which was introduced with IOS release 12.0(23), and ACL Support for Filtering IP Options Feature that is available with IOS Release 12.3(4)T or later. The IP Options Selective Drop Feature can be configured in one of two modes: drop or ignore. If the global command ip options ignore is configured, the router will still process the packet as normal while ignoring the IP Options field. The ACL Support for Filtering IP Options Feature can be used to selectively filter and drop packets based on specific option values.

The premise router must be configured to block any packet with the value of 82 in the IP Options fields either by configuring the global command ip options drop in addition to the ACL shown above to block the traditional traceroute or creating an extended named ACL for the ingress filter that would include ACL statements to block both traceroute methods. An example would look as follows:

```
interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group ingress-filter in
.
ip access-list extended ingress-filter
deny ip any any option traceroute log
deny udp any any range 33400 34400 log
.
deny ip any any
```

Note: Resource Reservation Protocol (RSVP) used by MPLS, Internet Group Management Protocol Version 2 (IGMPv2), and other protocols that use the IP options field may not function in either drop or ignore modes.

---

**Default Finding Details** Inbound traceroute is not blocked at the router(s).

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

### Fixes

#### NET Traceroutes blocked

The router administrator will configure the router to include controls to block inbound traceroutes. The configuration should look similar to the following:

```
access-list 100 deny icmp any any traceroute log
access-list 100 deny udp any any range 33400 34400 log
```

Notes:

---

---

**NET0920****V0003968 CAT II****Bind ingress / egress filters to correct interface**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE**Vulnerability** The router administrator will bind the ingress ACL filtering packets entering the network to the external interface on an inbound direction.**Vulnerability Discussion** Access lists are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of routers makes use of access lists for restricting access to services on the router itself as well as for filtering traffic passing through the router. Inbound versus Outbound; it should be noted that some operating systems default access-lists are applied to the outbound queue. The more secure solution is to apply the access-list to the inbound queue for 3 reasons:

- The router can protect itself before damage is inflicted.
- The input port is still known, and can be filtered upon.
- It is more efficient to filter packets before routing them.

---

**Checks****NET Ingress ACLs Bound to Inte**

Base Procedure:

The router administrator will bind the ingress ACL filtering packets entering the network to the external interface in an inbound direction. Note: All filters must be applied to the appropriate interfaces on an inbound direction. Ingress filtering is applied to all traffic entering the enclave. The ingress filter would be bound to all external interfaces.

**NET0920**

IOS Example:

```
interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
```

---

**Default Finding** The ingress ACL is not bound to the external interface (inbound).**Details**

---

**OPEN:**  **NOT A FINDING:**  **NOT REVIEWED:**  **NOT APPLICABLE:** **Fixes****NET ACLs Bound to Interface**

Bind the ingress ACL to the external interface (inbound) and the egress ACL to the internal interface (inbound).

Notes:

**NET0921                      V0014688   CAT II                      Bind egress filters to correct interface**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will bind the egress ACL filtering packets leaving the network to the internal interface on an inbound direction.

**Vulnerability Discussion** Access lists are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of routers makes use of access lists for restricting access to services on the router itself as well as for filtering traffic passing through the router. Inbound versus Outbound; it should be noted that some operating systems default access-lists are applied to the outbound queue. The more secure solution is to apply the access-list to the inbound queue for 3 reasons:

- The router can protect itself before damage is inflicted.
- The input port is still known, and can be filtered upon.
- It is more efficient to filter packets before routing them.

---

**Checks**

**NET Egress ACLs Bound to Inter**

Base Procedure:

The router administrator will bind the ingress egress ACL filtering packets leaving the network to the internal interface in an inbound direction. Note: All filters must be applied to the appropriate interfaces on an inbound direction. Since egress filtering is applied to all traffic leaving the enclave, this filter would be bound to all internal interfaces.

**NET0921 - CISCO**

```
interface FastEthernet 1/0
description downstream link to our network
ip address 199.36.90.1 255.255.255.0
ip access-group 102 in
```

---

**Default Finding** The more secure solution is to apply the access-list to the inbound queue for 3 reasons:

**Details**

- The router can protect itself before damage is inflicted.
- The input port is still known, and can be filtered upon.
- It is more efficient to filter packets before routing them.

---

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

**Fixes**

**NET Egress ACLs Bound to Inter**

Bind the ingress ACL to the external interface (inbound) and the egress ACL to the internal interface (inbound).

Notes:

**NET0923                      V0014689   CAT I                      IPv4 Loopback address is not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets with a local host loop back address (127.0.0.0/8).

**Vulnerability Discussion** Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network.

---

**Checks**

**NET IPv4 Loopback Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IP addresses explicitly, or inexplicitly.

**NET0923 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.....
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
```

---

**Default Finding** IPv4 Loopback address is not blocked  
**Details**

---

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

**Fixes**

**NET IPv4 Loopback Filter**

The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the local loopback address in the source field.

Notes:

**NET0924                      V0014690   CAT I                      IPv4 Link-local address is not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets with a link-local IP address range (169.254.0.0/16)

**Vulnerability Discussion** Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network.

---

**Checks**

**NET IPv4 Link-local Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IP addresses explicitly, or inexplicitly.

**NET0924 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.....
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
```

---

**Default Finding** IPv4 Link-local address is not blocked.  
**Details**

---

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

**Fixes**

**NET IPv4 Link-local Filter**

The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the link-local address in the source field.

Notes:

**NET0926                      V0014691   CAT I                      IPv4 Bogon & Martin addresses are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets having a source field from BOGON, Martian IP addresses.

**Vulnerability Discussion** Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network..

---

**Checks**

**NET IPv4 Bogon Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IP addresses explicitly, or inexplicitly. Also reference NET0928 for maintenance of filter.

**NET0926 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.....
access-list 100 deny ip 'IANA Reserved Address' 0.255.255.255 any log
access-list 100 deny ip 'IANA Unallocated Address' 0.255.255.255 any log
```

---

**Default Finding** IPv4 Bogon & Martin addresses are not blocked.  
**Details**

---

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

**Fixes**

**NET IPv4 Bogon Filter**

The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the IANA Reserved and Unallocated addresses in the source field.

Notes:

**NET0927                      V0014692 CAT I                      RFC1918 addresses are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets having a source field from RFC1918 IP addresses.

**Vulnerability Discussion** Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network..

---

**Checks**

**NET IPv4 RFC1918 Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IP addresses explicitly, or inexplicitly.

**NET0927 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.....
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
```

---

**Default Finding Details** RFC1918 addresses are not blocked.

---

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

**Fixes**

**NET IPv4 RFC1918 Filter**

The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the RFC1918 addresses in the source field.

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 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:

**NET0940**                      **V0003024 CAT I**                      **Ingress Filtering does not block Spoofed Addresses**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network, any local host loop back address (127.0.0.0/8), the link-local IP address range (169.254.0.0/16), IANA unallocated addresses or any reserved private addresses in the source field.

**Vulnerability Discussion** Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network.

---

**Checks**

**NET Ingress Spoofing Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IPv4 and/or IPv6 internal source addresses explicitly, or implicitly.

**NET0940 - CISCO**

```
interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.....
access-list 100 deny ip <internal network range> <wildcard mask> any log
and/or deny ipv6 <internal network range/prefix length> any log
```

---

**Default Finding** Inbound spoofing attacks are not prevented by restrictive ACLs. The following IP addresses are not blocked by an ingress ACL:

**Details** Internal network IP range  
Link Local default  
Reserved private address space (RFC 1918)  
Local Host

---

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

**Fixes**

**NET Ingress Spoofing Filter**

The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the internal network such as a local host addresses. These addresses could be registered .mil addresses defined locally or a RFC1918 subnet.

Notes:

---

---

**NET0941                      V0014693   CAT II                      IPv6 Site Local Unicast ADDR must not be defined**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure IPv6 Site Local Unicast addresses are not defined in the enclave, (FEC0::/10).

**Vulnerability Discussion** As currently defined, site local addresses are ambiguous and can be present in multiple sites. The address itself does not contain any indication of the site to which it belongs. The use of site-local addresses has the potential to adversely affect network security through leaks, ambiguity and potential misrouting, as documented in section 2 of RFC3879. RFC3879 formally deprecates the IPv6 site-local unicast prefix defined in RFC3513, i.e., 1111111011 binary or FEC0::/10.

---

**Checks**

**NET IPv6 Site Local Unicast Ad**

Procedure: Review the premise router configuration to ensure FEC0::/10 IP addresses are not defined.

---

**Default Finding Details** IPv6 Site Local Unicast Addresses must not be defined in the enclave.

---

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

**Fixes**

**NET IPv6 Site Local Unicast Ad**

The router administrator will configure the router using authorized IP addresses.

Notes:

**NET0942                      V0014694   CAT I                      IPv6 Site Local Unicast Addresses are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure IPv6 Site Local Unicast addresses are blocked on the ingress inbound filter, (FEC0::/10).

**Vulnerability Discussion** As currently defined, site local addresses are ambiguous and can be present in multiple sites. The address itself does not contain any indication of the site to which it belongs. The use of site-local addresses has the potential to adversely affect network security through leaks, ambiguity and potential misrouting, as documented in section 2 of RFC3879. RFC3879 formally deprecates the IPv6 site-local unicast prefix defined in RFC3513, i.e., 1111111011 binary or FEC0::/10.

---

**Checks**

**NET IPv6 Site Local Unicast Ad**

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 Site Local Unicast Addresses and log all violations.

**NET0942 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 fec0::/10 any log
deny ipv6 any fec0::/10 log
```

---

**Default Finding** IPv6 Site Local Unicast Addresses are not blocked.  
**Details**

---

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

**Fixes**

**NET IPv6 Site Local Unicast Ad**

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

Notes:

**NET0943                      V0014695   CAT I                      IPv6 Loopback ADDR is not blocked by the enclave**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any inbound IP packets with a local host loop back address, (0:0:0:0:0:0:1 or ::1/128).

**Vulnerability Discussion** The unicast address 0:0:0:0:0:0:1, also defined ::1/128 is called the loopback address. A node could use it to send an IPv6 packet to itself. It should never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface to an imaginary link that goes nowhere. The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router. A packet received on an interface with destination address of loopback must be dropped.

---

**Checks**

**NET IPv6 Loopback Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict inbound IP addresses explicitly, or inexplicitly. Verify that an ingress ACL for IPv6 has been defined to deny IPv6 Loopback, and log all violations.

**NET0943 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 ::1/128 any log
```

---

**Default Finding** IPv6 Loopback Address is not blocked by the enclave.  
**Details**

---

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

**Fixes**

**NET IPv6 Loopback Filter**

The router administrator will configure the router ACLs to restrict IP addresses that contain any Loopback addresses.

Notes:

**NET0944**

**V0014696 CAT I**

**IPv6 Unspecified ADDR is not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the premise router from accepting any IP packets from the unspecified address, (0:0:0:0:0:0:0 or ::/128).

**Vulnerability Discussion** The address 0:0:0:0:0:0:0:0, also defined ::/128 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address. The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing Headers. A router must never forward an IPv6 packet with a source address of unspecified.

**Checks**

**NET IPv6 unspecified Addresses**

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 Unspecified Address and log all violations.

**NET0944 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 ::/128 any log
deny ipv6 any ::/128 log
```

**Default Finding Details** IPv6 Unspecified Address is not blocked by the enclave.

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

**Fixes**

**NET IPv6 Unspecified Addresses**

The router administrator will configure the router ACLs to restrict IP addresses that contain any Unspecified address.

Notes:

**NET0945                      V0014697   CAT II                      IPv6 Multicast Source ADDR are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure that IPv6 well-known Multicast addresses are blocked on the ingress and egress inbound filters, (FF00::/16).

**Vulnerability Discussion** The following well-known multicast addresses are predefined and shall never be assigned to any multicast group.

Reserved Multicast Addresses:   FF00:0:0:0:0:0:0:0   FF08:0:0:0:0:0:0:0  
  FF01:0:0:0:0:0:0:0   FF09:0:0:0:0:0:0:0  
  FF02:0:0:0:0:0:0:0   FF0A:0:0:0:0:0:0:0  
  FF03:0:0:0:0:0:0:0   FF0B:0:0:0:0:0:0:0  
  FF04:0:0:0:0:0:0:0   FF0C:0:0:0:0:0:0:0  
  FF05:0:0:0:0:0:0:0   FF0D:0:0:0:0:0:0:0  
  FF06:0:0:0:0:0:0:0   FF0E:0:0:0:0:0:0:0  
  FF07:0:0:0:0:0:0:0   FF0F:0:0:0:0:0:0:0

**Checks**

**NET IPv6 Multicast Filter**

Base Procedure: Review the premise router configuration to ensure filters are in place to restrict the IP addresses. Verify that ingress and egress ACLs for IPv6 have been defined to deny the Multicast Source Addresses and log all violations.

**NET0945 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 ff00::/16 any log
deny ipv6 any ff00::/16 log
```

**Default Finding Details** IPv6 Multicast Source Address is not blocked by the enclave.

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

**Fixes**

**NET IPv6 Multicast Addresses F**

The router administrator will configure the router ACLs to restrict IP addresses that contain any Multicast addresses.

Notes:

**NET0946**

**V0014698 CAT II**

**Embedded IPv4-Compatible IPv6 ADDR are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure IPv6 addresses with embedded IPv4-compatible IPv6 addresses are blocked on the ingress and egress filters, (0::/96).

**Vulnerability Discussion** The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. IPv4-compatible IPv6 addresses should never appear as a source or destination address. These addresses begin with 0000 and have '0000' in the 16 bit field preceding the IPv4 address. RFC 4291 deprecated the IPv4-compatible addresses.

**Checks**

**NET OPv6 embedded IPv4-compati**

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 embedded IPv4-compatible IPv6 addresses and log all violations.

**NET0946 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 0::/96 any log
deny ipv6 any 0::/96 log
```

**Default Finding Details** Embedded IPv4-Compatible IPv6 addresses are not blocked.

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

**Fixes**

**NET IPv6 embedded IPv4-compati**

The router administrator will configure the router ACLs to restrict IP addresses that contain any embedded IPv4-compatible IPv6 addresses.

Notes:

**NET0947                      V0014699   CAT II                      Embedded IPv4-Mapped IPv6 ADDR are not blocked**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure that IPv6 addresses with embedded IPv4-mapped IPv6 addresses are blocked on the ingress and egress filters, (0::FFFF/96).

**Vulnerability Discussion** The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. IPv4-mapped IPv6 addresses should never appear as a source or destination address. These addresses begin with 0000 and have 'FFFF' in the 16 bit field preceding the IPv4 address. There is little use for the IPv4-mapped addresses and there has been some confusion for what their intended use was. There were three revisions of IPv6 Basic API specification (RFC 2133, 2553, and 3493). Under the current usage of the API, no packets should appear on the wire with these addresses so blocking them is the policy.

---

**Checks**

**NET IPv6 embedded IPv4-mapped**

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 embedded IPv4-mapped IPv6 addresses and log all violations.

**NET0947 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in
ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 0::FFFF/96 any log
deny ipv6 any 0::FFFF/96 log
```

---

**Default Finding** Embedded IPv4-Mapped IPv6 addresses are not blocked by the enclave.

**Details**

---

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

**Fixes**

**NET IPv6 embedded IPv4-mapped**

The router administrator will configure the router ACLs to restrict IP addresses that contain any embedded IPv4-mapped IPv6 addresses.

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 IPv6 Unique 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.

**NET0948 - CISCO**

```
interface FastEthernet 0/0
description upstream link toward DoD Backbone
ipv6 address 2001:db8:60::f14:65a1
ipv6 traffic-filter inbound-to-enclave in

ipv6 access-list inbound-to-enclave
remark prohibit use of site-local
deny ipv6 FC00::7 any log
deny ipv6 any FC00::7 log
```

---

**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:

---

---

**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 IPv6 Unique 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:

---

---

**NET0950**

**V0003164 CAT I**

**uRPF strict mode not enabled on egress interface**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field by enabling Unicast Strict mode.

**Vulnerability Discussion** Unicast Reverse Path Forwarding (uRPF) provides a mechanism for IP address spoof protection. When uRPF is enabled on an interface, the router examines all packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified. If Unicast RPF does not find a reverse path for the packet, the packet is dropped.

---

**Checks**

**NET Egress Spoofing Filter**

Base Procedure: Unicast Strict mode: Review the premise router configuration to ensure uRPF has been configured on all internal interfaces.

**NET0950 - CISCO**

```
interface FastEthernet 0/0
description downstream link to enclave LAN
ip address 199.36.90.1 255.255.255.0
ip verify unicast source reachable-via rx 102
```

```
access-list 102 deny ip any any log
```

---

**Default Finding Details** Restrictive ACLs are not in place to prevent outbound Spoofing attacks.

---

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

**Fixes**

**NET Egress Spoofing Filter**

The NSO will ensure that an ACL is configured to restrict the router from accepting any outbound IP packet that contains an external IP address in the source field.

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:

**NET0954                      V0014707   CAT II                      IPv6 Egress Outbound Spoofing Filter**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Reverse Path Forwarding in an IPv6 enclave.

**Vulnerability Discussion** Unicast Reverse Path Forwarding (uRPF) provides a mechanism for IP address spoof protection. When uRPF is enabled on an interface, the router examines all packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received. If the packet was received from one of the best reverse path routes, the packet is forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified. If Unicast RPF does not find a reverse path for the packet, the packet is dropped.

---

**Checks**

**NET IPv6 Egress Spoofing Filte**

Base Procedure: Unicast Strict mode: Review the premise router configuration to ensure uRPF has been configured on all internal interfaces.

**NET0954 - CISCO**

```
IOS example
interface FastEthernet 1/1
description downstream link to our network
ipv6 address 2001:db8:60::f15:60c2
ipv6 verify unicast source reachable-via rx outbound-to-Backbone out

ipv6 access-list outbound-to-Backbone
remark explicitly block all other packets
deny ipv6 any any log
```

---

**Default Finding Details** The router is not restricting outbound IP packets that contain an illegitimate address in the source address field via egress ACL.

---

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

**Fixes**

**NET IPv6 Egress Spoofing Filte**

The NSO will ensure that an ACL is configured to restrict the router from accepting any outbound IP packet that contains an external IP address in the source field.

Notes:

**NET0960**

**V0003165 CAT II**

**Routers are not set to intercept TCP SYN attacks**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will implement tcp intercept features provided by the router or implement a filter to rate limit tcp syn to protect servers from any TCP SYN flood attacks from an outside network.

**Vulnerability Discussion** The TCP SYN attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users.

---

**Checks**

**NET TCP SYN Protection**

Base Procedure: The NSO will ensure that the TCP Intercept command is used to intercept TCP SYN attacks from outside the network.

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.

**NET TCP SYN protection IOS**

IOS example:  
ip tcp intercept list 107

access-list 107 permit tcp any internal network wildcard mask

---

**Default Finding  
Details**

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

**Fixes**

**NET TCP SYN Protection**

Ensure that the TCP Intercept is used to intercept TCP SYN attacks from outside the network.

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:

**NET1030**

**V0003072 CAT III**

**Run and Startup configs, not synchronized**

8500.2 IA Control: COBR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator, when saving and loading configurations will ensure that the running and startup configurations are synchronized.

**Vulnerability Discussion** If the running and startup router configurations are not synchronized properly and a router malfunctions, it will not restart with all of the recent changes incorporated. If the recent changes were security related, then the routers would be vulnerable to attack.

---

**Checks**

**NET Start & Run CFGs in Sync**

IOS Procedure: With online editing, the show running-config command will only show the current running configuration settings, which are different from the IOS defaults. The show startup-config command will show the NVRAM startup configuration. Compare the two configurations to ensure they are synchronized.

JUNOS Procedure: This will never be a finding. The active configuration is stored on flash as juniper.conf. A candidate configuration allows you to make configuration changes while in configuration mode without initiating operational changes. The router implements the candidate configuration when it is committed; thereby, making it the new active configuration—at which time it will be stored on flash as juniper.conf and the old juniper.conf will become juniper.conf .1.

---

**Default Finding Details** The running and startup router configurations are not synchronized.

---

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

**Fixes**

**Start & Run CFGs in Sync**

The router administrator will ensure that all router running and startup configurations are synchronized. As part of the router configuration SOP, add procedures to keep these two configurations synchronized.

Notes:

**NET1050**

**V0003074 CAT III**

**Restrict access to stored configuration files**

8500.2 IA Control: COBR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure that on the system where the configuration files are stored, the router administrator uses the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).

The IAO/NSO will ensure only authorized router administrators are given access to the stored configuration files.

**Vulnerability Discussion** Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that router configurations are stored in a secure location where only authorized users can gain access. If the router network is compromised, then large parts of the network could be incapacitated with only a few commands.

---

**Checks**

**NET BU CFG Security**

Have the router administrator display the security features that are used to control access to the configuration files.

**NET BUs for Auth Users**

Interview the IAO/NSO to ensure that access to stored configuration files is restricted to authorized router administrators only. Password restricted access to these files will be enforced and the passwords will be changed when authorized administrators leave or change job responsibilities.

---

**Default Finding Details** There are no file access permissions in place to secure the configurations against unauthorized access. Therefore, access to stored configuration files is not restricted to authorized personnel.

---

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

**Fixes**

**NET BU CFG Security**

The router administrator will store the current and previous router configurations in a secure area (file access permissions restricting to authorized personnel).

Notes:

**NET1071**                      **V0005644**   **CAT II**                      **TFTP server access is not restricted.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** If TFTP implementation is used, the router administrator will ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.

**Vulnerability Discussion** TFTP requires restricted and limited access.

**Checks**

**NET TFTP Server on Secure LAN**

Identify TFTP server addresses and determine if LAN has traffic restrictions and devices with access to servers have ACL permissions and restrictions.

**Default Finding Details** TFTP implementation is not restricted and limited as required.

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

**Fixes**

**TFTP Server on Secure LAN**

Identify host addresses that will access the TFTP server and harden access to the server via ACL rules.

Notes:

**NET1080**                      **V0003075**   **CAT II**                      **The FTP username and password are not configured.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The router administrator will ensure the FTP username and password are configured.

**Vulnerability Discussion** Transferring IOS configuration files without using the FTP service may leave the router accounts and passwords unencrypted during the transfer. If this information is intercepted during the transfer, the router could be compromised and large parts of the network could be incapacitated with only a few commands.

**Checks**

**NET TFTP PSW Protection**

IOS Procedure: Review the running config for all routers to ensure a username and password have been configured for the router's ftp client. The configuration should look similar to the following: ip ftp username userid ip ftp password psw.

JUNOS Procedure: not applicable.

**Default Finding Details** The IP FTP command is not enabled and does not include the FTP username and password in the router configuration.

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

**Fixes**

**NET TFTP PSW Protection**

The router administrator will change the router configuration files to ensure the IP FTP command is being used to include the FTP username and password. To enable IP FTP: ip ftp username user; ip ftp password string; ip ftp source-interface ether x

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:

**NET1900**

**V0015207 CAT II**

**CE must not allow native IPv6 traffic to reach PE**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure the customer edge interface facing the core's provider edge does not allow native IPv6 traffic during MO2.

**Vulnerability Discussion** The DoD IPv6 Transition Office (DITO) Milestone Objective 2 (M02) introduced the Dual Stack as an approved architecture. The major objective for the MO2 time period beginning September 30, 2006 is to prevent any IPv6 traffic from leaking into non-participating domains or core networks.

In the Dual Stack environment the Customer Edge (CE) router facing the DISN Core (PE) can become Dual Stack. In the Dual Stack environment all devices downstream into the enclave can support IPv4, IPv6 or both. Depending on the conversion effort to the DISN Core, the function of the CE could be performed at the NIPRNet or SIPRNet hub router. In this legacy architecture the hub router can process and transfer IPv4 and IPv6 datagrams within a DoD network in a Dual Stack environment similar to the DISN Core architecture CE router.

---

**Checks**

**NET Filter IPv6**

Base Procedure: When IPv6 is found in the enclave, ensure IPv6 has not been enabled on the interface of the customer edge (CE) router facing the provider edge (PE) router. As an additional precautionary step, write an access list policy that blocks native IPv6 traffic on the interface.

**NET Filter IPv6 IOS**

IOS Procedure:

```
ipv6 enable <-----[should not be found on the interface]
```

```
ipv6 access-list block native IPv6 traffic before PE  
remark explicitly block all other ICMP packets  
deny ipv6 any any log
```

---

**Default Finding Details** Customer edge interface facing the core's provider edge allows native IPv6 traffic during MO2.

---

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

**Fixes**

**NET Filter IPv6**

Disable IPv6 on the interface facing the PE router. Write an access list policy that blocks native IPv6 traffic on the interface is also recommended.

Notes:

**NET1901                      V0015233   CAT II                      CE must not allow IPv6 NLRI traffic to reach PE**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure the customer edge interface facing the core’s provider edge does not allow native IPv6 network layer reachability information (NLRI) during MO2.

**Vulnerability Discussion** Network Layer Reachability Information (NLRI) is included in BGP routing update messages which describe a route and how to get there. In this context, an NLRI is a prefix. A BGP-update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes and other information. The NLRI will contain the prefix and length and is used in unicast and multicast.

If the multiprotocol extensions to BGP are negotiated at the time of creation, the BGP speaker can prefix the Network Layer Reachability Information (NLRI) it advertises with an address family prefix. These families include the default IPv4, but also IPv6, IPv4 and IPv6 Virtual Private Networks, and multicast BGP.

In the Dual Stack environment the Customer Edge (CE) router facing the DISN Core (PE) can become Dual Stack. In the Dual Stack environment all devices downstream into the enclave can support IPv4, IPv6 or both. Depending on the conversion effort to the DISN Core, the function of the CE could be performed at the NIPRNet or SIPRNet hub router. In this legacy architecture the hub router can process and transfer IPv4 and IPv6 datagrams within a DoD network in a Dual Stack environment similar to the DISN Core architecture CE router.

---

**Checks**

**NET IPv6 NLRI**

Base Procedure: When IPv6 is found in the enclave ensure IPv6 NLRI is not being exchanged by verify BGP neighbor statements do not contain IPv6 addresses. In addition, ensure BGP address-family IPv6 statements are not in the configuration.

---

**Default Finding Details** CE allows IPv6 NLRI traffic to reach PE during MO2.

---

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

**Fixes**

**NET IPv6 NLRI**

Remove IPv6 neighbor statements and address family statements.

**NET IPv6 NLRI IOS**

IOS Procedure: The following example describes a BGP definition. Ensure these are not found.

```
router bgp 100
neighbor 2001:100:3:4::1 remote as 100 ! for IBGP peering, over IPv6
!
address-family ipv6
neighbor 2001:100:3:4::1 activate
redistribute connected
```

Notes:

**NET1905**                      **V0015237 CAT II**                      **Perimeter must not support IPv6 in IPv4 GRE tunnel**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure in a dual stack environment the enclave perimeter device does not support IPv6 in IPv4 GRE or VPN tunnels between enclave internal devices.

**Vulnerability Discussion** The DoD IPv6 Transition Office (DITO) Milestone Objective 2 (M02) introduced the Dual Stack as an approved architecture. The major objective for the MO2 time period beginning September 30, 2006 is to prevent any IPv6 traffic from leaking into non-participating domains or core networks. This version of the Network STIG will provide security guidance for MO2 to meet these requirements.

1. All interfaces MAY accept and transmit native IPv6 traffic.
2. There MUST not be any IPv6 in IPv4 tunnel traffic between enclave internal interfaces and the perimeter of the Dual Stack router. This could be the local perimeter or the CE pending IPv6 deployment.

---

**Checks**

**NET Dual-Stack Tunnel**

Base Procedure: If the site is running Dual Stack architecture, ensure GRE and VPN tunnels are not defined to carry IPv6 traffic.

**NET Dual-Stack Tunnel IOS**

IOS Procedure: The following example describes a GRE and VPN definition. Ensure these are not found transporting IPv6 traffic in Dual Stack Architectures.

```
! Tunnel definition defining tunnel mode GRE IPv6, protocol 47
```

```
interface tunnel 0  
no ip address  
ipv6 address 2001:0DB8:1111:2222::1/64  
tunnel source Ethernet 0/0  
tunnel destination 10.0.0.2  
tunnel mode gre ipv6  
!
```

```
interface Ethernet0/0  
ip address 10.0.0.1 255.255.255.0
```

```
! Tunnel definition defining tunnel mode VPN, protocol 41
```

```
interface ethernet 0  
ip address 192.168.99.1 255.255.255.0
```

```
interface tunnel 0  
ipv6 address 3ffe:b00:c18:1::3/127  
tunnel source ethernet 0  
tunnel destination 192.168.30.1  
tunnel mode ipv6ip
```

---

**Default Finding** Perimeter supports IPv6 in IPv4 GRE tunnel.

**Details**

---

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

**Fixes**

**NET Dual-Stack Tunnel**

If the site is running Dual Stack the GRE IPv6 and VPN tunnels have to be removed.

Notes:

**NET1935**                      **V0015275**   **CAT II**                      **More than one IPv6 to IPv4 tunnel defined**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure there is only one IPv6 to IPv4 tunnel between the interfaces of the internal router's ingress interface and the perimeter router's egress interface.

**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. There should only be one tunnel defined between the enclave internal device and the enclave perimeter.

**Checks**

**NET One Security Zone**

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 there is only one tunnel defined for IPv6 encapsulation between the internal device and the perimeter device.

**Default Finding Details** More than one IPv6 to IPv4 tunnel defined in enclave.

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

**Fixes**

**NET One Security Zone**

Remove additional tunnels.

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:

**NET1942**

**V0015283 CAT II**

**IPv6 must be filtered on non IPv6 interfaces.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure an access list is applied on all interfaces not supporting IPv6 that blocks native IPv6 traffic when IPv6 is used in an enclave environment.

**Vulnerability Discussion** During MO2 the enclave is in a test period. IPv6 traffic must be controlled and prevented from leaving the enclave.

---

**Checks**

**NET IPv6 filter**

If the enclave is in MO2 running IPv6, ensure the IPv6 protocol is filtered on non-IPv6 interfaces to isolate the protocol.

---

**Default Finding Details** IPv6 must be filtered on non IPv6 interfaces.

---

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

**Fixes**

**NET IPv6 filter**

Block IPv6 on non-IPv6 interfaces

Notes:

**NET1945**

**V0015285 CAT II**

**Tunnels for IPv6 transition must filter 41**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure tunnels used for IPv6 transition are filtered by protocol 41 and the endpoints are explicitly defined on the permit filter.

**Vulnerability Discussion** The DoD IPv6 Transition Office (DITO) Milestone Objective 2 (MO2) introduced the Dual Stack as an approved architecture. The major objective for the MO2 time period beginning September 30, 2006 is to prevent any IPv6 traffic from leaking into non-participating domains or core networks. This version of the Network STIG will provide security guidance for MO2 to meet these requirements.

In the Dual Stack environment the Customer Edge (CE) router facing the DISN Core (PE) can become Dual Stack. In the Dual Stack environment all devices downstream into the enclave can support IPv4, IPv6 or both. Depending on the conversion effort to the DISN Core, the function of the CE could be performed at the NIPRNet or SIPRNet hub router. In this legacy architecture the hub router can process and transfer IPv4 and IPv6 datagrams within a DoD network in a Dual Stack environment similar to the DISN Core architecture CE router.

---

**Checks**

**NET IPv6 41 filter**

Base Procedure: Review the interface supporting the IPv6 tunnel endpoint and verify a filter is in place that does not allow protocol 41.

**NET IPv6 41 filter IOS**

```
interface Ethernet0
description IPv4 uplink
ip address 192.168.99.1 255.255.255.0
ip access-group 101 out
```

```
!
access-list 101 remark deny protocol 41 leaving the enclave
access-list 101 deny 41 any any log
```

---

**Default Finding Details** Tunnels used for IPv6 transition must be filtered by protocol 41

---

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

**Fixes**

**NET IPv6 41 filter**

Add a filter on the interface that supports the tunnel. The filter should not allow protocol 41 traffic.

Notes:

---

---

**NET1950**

**V0015287 CAT I**

**ISATAP tunnels must not breach the perimeter**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure ISATAP tunnels do not breach the perimeter boundary.

**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 tunnel 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 bypass Perimeter**

Base Procedure: Specifying the IPv4 address of the 6to4 relay on the 6to4 router can mitigate these vulnerabilities.

---

**Default Finding Details** ISATAP tunnels must not breach the perimeter boundary

---

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

**Fixes**

**NET ISATAP bypass Perimeter**

Specify the IPv4 address of the 6to4 relay on the 6to4 router.

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:

**NET1954                      V0015289   CAT II                      ISATAP enclave has other IPv6 Mechanisms**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure in ISATAP architectures, the enclave boundary does not have any other IPv6 Transition Mechanisms implemented.

**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 policy**

If IPv6 is found in the infrastructure, interview the IAO and Router Administrator to see to identify what transition mechanisms are being used in the enclave.

---

**Default Finding Details** ISATAP architectures must not have other IPv6 Transition Mechanisms implemented.

---

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

**Fixes**

**NET ISATAP policy**

If ISATAP is implemented in the enclave remove all other transition mechanisms.

Notes:

**NET1965**

**V0015293 CAT II**

**Ingress filter does not filter protocol 41**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure the ingress filter drops unexpected protocol 41 packets at the 6to4 site router before sensor inspection.

**Vulnerability Discussion** 6to4 is an automated tunneling mechanism that provides v6 capability to a dual-stack node or v6 capable site that has only IPv4 connectivity to the site. One key difference between automatic 6to4 tunnels and manually configured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. Basic 6to4 implementation can be used to connect single nodes too. In 6to4 tunnel implementations, tunnels are not defined in pairs as in manual tunnels. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:IPv4-address in hex::/48. 6to4 traffic takes an asymmetric routing path, outbound traffic and return traffic may take different paths. Although the 6to4 site can select the relay it wants to use, it has no control of the return relay used. See diagram in the STIG. Ensuring reliable operations from relays and knowing who is managing the relay are important and are concerns to preventing against denial of service attacks. 6to4 site routers are not capable of identifying bogus traffic injected from malicious 6to4 relay manufacturing packets. Specifying the exact IPv4 address of the 6to4 relay on the 6to4 router can mitigate these vulnerabilities.

6to4 tunnels are required to discard unexpected protocol 41 packets and inspect IPv6 traffic at the decapsulator end-point.

---

**Checks**

**NET 6to4 filter**

Base Procedure: Specifying the IPv4 address of the 6to4 relay on the 6to4 router can mitigate these vulnerabilities.

**NET 6to4 filter IOS**

```
interface Ethernet0
description IPv4 uplink
ip address 192.168.99.1 255.255.255.0
ip access-group 101 in
.
!
interface Ethernet1
description IPv6 local network 1
ipv6 address 2002:c0a8:6301:1::1/64
!
interface Ethernet2
description IPv6 local network 2
ipv6 address 2002:c0a8:6301:2::1/64
!
interface Tunnel0
description IPv6 uplink
no ip address
ipv6 address 2002:c0a8:6301::1/64
tunnel source Ethernet 0
tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 tunnel 0
!
access-list 101 remark Permit protocol 41 from trusted IPv4 6to4 relay address to destination of IPv4 infrastructure
access-list 101 permit 41 [trusted 6to4 relay addr] [infrastructure IPs] log
access-list 101 deny 41 any any log
```

---

**Default Finding** The ingress filter does not drop unexpected protocol 41 packets at the 6to4 site router.

**Details**

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

**Fixes**

**NET 6to4 filter**

Define a filter that allows 6to4 tunneling from trusted 6to4 relays.

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:

# NET1990                      V0015296   CAT II                      IPv4 Interfaces in NAT-PT receive IPv6

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure interfaces supporting IPv4 in NAT-PT Architecture do not receive IPv6 traffic.

**Vulnerability Discussion** Network Address Translation with Protocol Translation (NAT-PT), defined in [RFC2766], is a service that can be used to translate data sent between IP-heterogeneous nodes. NAT-PT translates a IPv4 datagram into a semantically equivalent IPv6 datagram or vice versa. For this service to work it has to be located in the connection point between the IPv4 network and the IPv6 network. The PT-part of the NAT-PT handles the interpretation and translation of the semantically equivalent IP header, either from IPv4 to IPv6 or from IPv6 to IPv4. Like NAT, NATPT also uses a pool of addresses which it dynamically assigns to the translated datagrams.

The NAT-PT architecture is not one of the preferred DoD IPv6 transition paradigms due to the deprecation of NAT-PT within the DoD community. However, as described in the "DoD IPv6 Guidance for Information Assurance (IA) Milestone Objective 3 (MO3) Requirements, some services/agencies may chose to implement this transition mechanism within an enclave. The following subsections provide guidelines for the use of NAT-PT within a controlled enclave.

In addition to the single point of failure, the reduced performance of an application level gateway, coupled with limitations on the kinds of applications that work, decreases the overall value and utility of the network. NAT-PT also inhibits the ability to deploy security at the IP layer.

## Checks

### NET NAT-PT IPv4

Base Procedure: Review network diagram in the STIG and ensure the architecture is designed correctly. The interface facing the IPv4 LAN network must not receive IPv6 traffic. This can be accomplished by not having IPv6 on the interface supporting the IPv4 network. In addition a filter can be added to deny IPv6 at this interface.

### NET NAT-PT IPv4 IOS

IOS Procedure: NAT/PT can be identified by the commands in the following example:

```
interface ethernet-1
ipv6 address 2001:2::10/64
ipv6 nat prefix 2010::/96
ipv6 nat
!
interface ethernet-2
ip address 192.168.1.1 255.255.255.0
ipv6 nat
!
ipv6 nat v4v6 source 192.168.1.100 2010::1
!
ipv6 nat v6v4 source route-map map1 pool v4pool1
ipv6 nat v6v4 pool v4pool1 192.168.2.1 192.168.2.10
prefix-length 24
!
route-map map1 permit 10
match interface Ethernet-1
```

**Default Finding Details** Interfaces supporting IPv4 in NAT-PT must not receive IPv6 traffic.

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

## Fixes

### NET NAT-PT IPv4

This can be accomplished by not having IPv6 enabled on the interface supporting the IPv4 network. In addition a filter can be added to deny IPv6 at the interface.

Notes:

**NET1992**

**V0015295 CAT II**

**Tunneled IPv4 in IPv6 traffic in NAT-PT**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure in NAT-PT architecture there is no tunneled IPv4 in IPv6 traffic.

**Vulnerability Discussion** Network Address Translation with Protocol Translation (NAT-PT), defined in [RFC2766], is a service that can be used to translate data sent between IP-heterogeneous nodes. NAT-PT translates a IPv4 datagram into a semantically equivalent IPv6 datagram or vice versa. For this service to work it has to be located in the connection point between the IPv4 network and the IPv6 network. The PT-part of the NAT-PT handles the interpretation and translation of the semantically equivalent IP header, either from IPv4 to IPv6 or from IPv6 to IPv4. Like NAT, NATPT also uses a pool of addresses which it dynamically assigns to the translated datagrams.

The NAT-PT architecture is not one of the preferred DoD IPv6 transition paradigms due to the deprecation of NAT-PT within the DoD community. However, as described in the "DoD IPv6 Guidance for Information Assurance (IA) Milestone Objective 3 (MO3) Requirements, some services/agencies may chose to implement this transition mechanism within an enclave. The following sub-sections provide guidelines for the use of NAT-PT within a controlled enclave.

In addition to the single point of failure, the reduced performance of an application level gateway, coupled with limitations on the kinds of applications that work, decreases the overall value and utility of the network. NAT-PT also inhibits the ability to deploy security at the IP layer.

---

**Checks**

**NET NAT-PT Tunnel**

Base Procedure: Review network diagram in the STIG and ensure the architecture is designed correctly. The interface adjacent to the IPv4 LAN interface must not deploy IPv6 over IPv4. The techniques include using manually configured tunnels, generic routing encapsulation (GRE) tunnels, semiautomatic tunnel mechanisms such as tunnel broker services, and fully automatic tunnel mechanisms such as 6to4 for the WAN and intra-site automatic tunnel addressing protocol (ISATAP).

**NET NAT-PT Tunnel IOS**

IOS Procedure: NAT/PT can be identified by the commands in the following example:

```
interface ethernet-1
ipv6 address 2001:2::10/64
ipv6 nat prefix 2010::/96
ipv6 nat
!
interface ethernet-2
ip address 192.168.1.1 255.255.255.0
ipv6 nat
!
ipv6 nat v4v6 source 192.168.1.100 2010::1
!
ipv6 nat v6v4 source route-map map1 pool v4pool1
ipv6 nat v6v4 pool v4pool1 192.168.2.1 192.168.2.10
prefix-length 24
!
route-map map1 permit 10
match interface Ethernet-1
```

---

**Default Finding** Tunneled IPv4 in IPv6 traffic must not be in NAT-PT architecture.

**Details**

---

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

**Fixes**

**NET NAT-PT Tunnel**

If NAT/PT is required the tunnel needs to be removed.

Notes: