



# Network Security Checklist - General Infrastructure 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				

**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:

**NET0240**                      **V0003143**   **CAT I**                      **Devices exist that have standard default passwords**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

**Checks**

**NET Password Protection**

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

**Default Finding Details**

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

**Fixes**

**NET Password Protection**

Ensure all communication devices are in compliance with password policy.

Notes:

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

8500.2 IA Control: ECWM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.

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

**Checks**

**NET Warning Banners**

Have the network administrators sign onto each managed network device to ensure the DoD approved warning banners are displayed before the password prompt and after a correct login.

**Default Finding Details** DOD approved warning banners, adhering to Appendix C of the Network Infrastructure STIG, are not displayed on network managed devices.

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

**Fixes**

**NET Warning Banner**

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

Notes:

**NET0400**

**V0003034 CAT II**

**Interior routing protocols are not authenticated**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

---

**Checks**

**NET MD5 Authentication**

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

---

**Default Finding Details** MD5 or IPSec is not used to authenticate routing protocol neighbors.

---

**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:

---

---

**NET0402**

**V0014664 CAT II**

**OSPFv3 routing protocol is not authenticated**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

**Vulnerability** The IAO/NSO will ensure neighbor authentication is implemented between OSPFv3 peer routers within the same or between autonomous systems (AS) using IPSec

**Vulnerability Discussion** OSPFv3 for IPv6 is a completely independent routing protocol than OSPFv2 for IPv4. Securing OSPFv2 in a dual stack environment will not protect OSPFv3 protocol or the OSPFv3 routing table. They are ships-in-the-night routing protocols that do not interoperate. The routing updates and routing tables are completely separate.

Generally, the point of an attack against a routing system falls into one of two categories: disrupting peering and falsifying routing information. To ensure that OSPF for IPv6 packets are not altered and re-sent to the router, OSPF for IPv6 packets must be authenticated.

---

**Checks**

**NET OSPFv3 authentication**

Base Procedure:

The authentication fields found in OSPFv2 have been removed from OSPFv3 packet for IPv6 thus no longer making MD5 an authentication option. OSPF relies on the IP Authentication Header and the IP Encapsulating Security Payload to ensure integrity, authentication and confidentiality of routing exchanges. Defining IPSec on the interface provides stronger security than a definition for an OSPF area. Review the configuration for protocol authentication.

---

**Default Finding Details** OSPFv3 routing protocol is not authenticated among peers.

---

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

**Fixes**

**NET OSPFv3**

The router administrator will configure the routers to use IPSec for routing peer authentication among 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.

---

**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:

---

---

**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:

---

---

**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-id 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.

---

**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:

---

---

**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.

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

**Discussion**

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

**Details**

**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.

---

**Default Finding Details** IOS version 12.3 has not been implemented on all Cisco routers. In some cases IOS version 12.2 is the highest release train. This is typically found on the CAT IOS 6000 series.

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:

**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.

---

**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:

---

**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.

---

**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.

**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:

**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.

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

**Details**

**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:

**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.

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

- 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 ensue no ip unreachable, no ip redirects and no ip mask-reply are enabled in the OS.

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 IA/O/NSO will ensure that the premise router is acting as an NTP server for only internal clients.

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

**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 Details** The NTP server is defined to service external clients.

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

**Fixes**

**NET NTP Internal Clients Only**

Install the server to service internal clients only.

Notes:

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

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

**Checks**

**NET NTP Client use Premise**

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

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

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

**Fixes**

**NET NTP Client use Premise**

Implement a secure NTP process using a local NTP server.

Notes:

**NET0813**                      **V0014671**   **CAT II**                      **MD5 authentication not used for NTP**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

**Checks**

**NET NTP MD5 use**

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

**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.

**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.

**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:

**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.

**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.

**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.

---

**Default Finding Details** Syslog traffic is not using loopback address.

---

**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.

---

**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.

**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.

**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.

---

**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.

---

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

---

**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:

**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:

**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.

**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.

---

**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 IA/O/NSO will configure all devices to log severity levels 0 through 7 and send log data to a syslog server.

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

---

**Checks**

**NET Log Severity Levels**

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

---

**Default Finding Details** The router is not configured to log message severity levels 0-6 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.

---

**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 OOB network are restricted by passwords.

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

**Details**

**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.

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

**Details**

**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.

**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 IAQ/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.

**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.

-----  
**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.

-----  
**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.

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

**Details**

**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.

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

**Details**

**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.

**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.

**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.

---

**Default Finding** SSH version 2 is not implemented.

**Details**

---

**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:

**NET1930**

**V0015266 CAT II**

**Egress interface is not the only accepting IPv6**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

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

**Checks**

**NET Security Zone Egress**

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

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

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

**Fixes**

**NET Security Zone Egress**

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

Notes:

**NET1931**

**V0015269 CAT II**

**Ingress interfaces must not allow native IPv6**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

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

---

**Checks**

**NET Security Zone Ingress**

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

---

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

---

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

**Fixes**

**NET Security Zone Ingress**

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

Notes:

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

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL  
IMPLEMENTATION GUIDE

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

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

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

**Checks**

**NET Security Zone NLRI**

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

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

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

**Fixes**

**NET Security Zone NLRI**

Remove BGP IPv6 statements from the internal router.

Notes:

**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:

**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:

**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.

---

**Default Finding** ISATAP tunnels must terminate at interior router  
**Details**

---

**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: