



Network Security Checklist - Network Policy

Version 7, Release 1.1

20 November 2007

Developed by DISA for the DOD

UNCLASSIFIED

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

NET0090

V0008046 CAT II

Network infrastructure is not properly documented.

8500.2 IA Control: DCHW-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will maintain a current drawing of the site's network topology that includes all external and internal links, subnets, and all network equipment.

Vulnerability Discussion To assist in the management, auditing, and security of the network infrastructure facility drawings and topology maps are a necessity. Topology maps are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks (wire taps) could take place.

Checks

NET Diagram

Validate the network diagram by correlating this information with all router and layer-3 switch configurations. Ensure that all subnets have been documented accordingly. To validate the connectivity as documented on the diagram, physically examine the cable connections for the downstream and upstream links as well as connections for major network components (JIDS, firewall, IDS, etc).

Default Finding Details

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

Fixes

NET Diagram

The NSO will maintain current up-to-date infrastructure and dataflow diagrams of the network under the NSOÆs control. The diagrams will include all remote connections, all local connections to domains not under site control, and all internal connections to PCs/workstations, servers, routers, bridges, and hubs or switches. This will help to show what the security, traffic, and physical impact of adding a new user(s) will be on the LAN. These diagrams will be based on a physical and if available an automated inspection of the network wiring plant. Special circumstances concerning the installation, such as a path that leaves a secure controlled environment, will be noted.

Notes:

NET0130

V0008047 CAT III

Network connections exist without approval

8500.2 IA Control: EBCR-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all external connections are validated and approved by the CAP and DAA, SNAP or SCAO requirements have been met, and MOA and MOU is established between enclaves, prior to connections.

Vulnerability Discussion Every site must have a security policy to address filtering of the traffic to and from those connections. This documentation along with diagrams of the network topology is required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet.

SIPRNet connections must also comply with the documentation required by the SIPRNet Connection Approval Office (SCAO) to receive the SIPRNet Interim Approval to Connect (IATC) or final Approval to Connect (ATC). Also any additional requirements must be met as outlined in the Interim Authority to Operate (IATO) or Authority to Operate (ATO) forms signed by the Designated Approving Authority (DAA).

Prior to establishing a connection with another activity, a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) must be established between the two sites prior to connecting with each other. This documentation along with diagrams of the network topology is required to be submitted to the CAP for approval to connect to the NIPRNet or SIPRNet. The policy must ensure that all connections to external networks should conform equally.

Checks

NET Circuit Apprv

Interview the IAM to verify that each external connection to the site's internal network is secured such that it does not introduce any unacceptable risk to the network.

Default Finding Details Network connections exist without approval

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

Fixes

NET Circuit Apprv

All external connections will be validated and approved prior to connection. Interview the IAM to verify that all connections have a mission requirement and that the DAA is aware of the requirement.

Notes:

NET0135 V0008048 CAT II Unmanaged backdoor connections.

8500.2 IA Control: EBCR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will review all connection requirements on a semi-annual basis to ensure the need remains current, as well as evaluate all undocumented network connections discovered during inspections.

Vulnerability Discussion A network is only as secure as its weakest link. It is imperative that all external connections be reviewed and kept to a minimum needed for operations. All external connections should be treated as untrusted networks. Reviewing who or what the network is connected to empowers the security manager to make sound judgements and security recommendations. Minimizing backdoor circuits and connections reduces the risk for unauthorized access to network resources.

Checks

NET Circuit Review

Verify that the IAO/NSO is aware of all connections and has documented their reviews.

**Default Finding
Details**

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

Fixes

NET Circuit Review

Verify the NSO is aware of all connections, and that all self-assessments require the NSO to verify the need for all connections.

Notes:

NET0140 V0008049 CAT III Circuit location is not secure.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the connection between the CSU/DSU and the local exchange carrier's (LEC) data service jack (i.e., demarc) is in a secured environment.

Vulnerability Discussion DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore unauthorized access must be restricted. Inadequate cable protection can lead to damage and denial of service attacks against the site and the LAN infrastructure.

Checks

NET Comm Closet

The IAO/NSO will ensure the physical network components are in a secure environment.

**Default Finding
Details**

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

Fixes

NET Comm Closet

The IAO will ensure all critical communications are in a controlled access areas. Controlled access area in this case means controlled restriction to authorize site personnel, i.e., dedicated communications rooms or locked cabinets. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the network from unauthorized personnel. The keys to the locked cabinets and dedicated communications rooms will be controlled and only provided to authorized network/network security individuals.

Notes:

NET0141 **V0008050** **CAT III** **The CSU\DSU modems are not disconnected.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the network management modems connected to all Channel Service Units (CSUs)/Data Service Units (DSUs) are disabled or disconnected when not in use.

Vulnerability Discussion DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore: unauthorized access must be restricted. Inadequate cable protection can lead to damage and denial of service attacks against the site and the LAN infrastructure.

Checks

NET CSU/DSU

Visually inspect the CSU\DSU to verify compliance.

Default Finding Details The CSU\DSU modems are not disconnected.

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

Fixes

NET CSU/DSU

The IAO/NSO will ensure that network management modems connected to all Channel Service Units (CSUs)/Data Service Unite (DSUs) will be disabled or disconnecting when not in use.

Notes:

NET0160 **V0008051** **CAT I** **A ISP connection exists without written approval.**

8500.2 IA Control: EBCR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure that written approval is obtained from the GIG Waiver Panel or the Assistant Secretary of Defense (AS-NII) prior to establishing an ISP connection.

Vulnerability Discussion Direct ISP connections are prohibited unless written approval is obtained from the Global Information Grid (GIG) Waiver Panel or the Assistant Secretary of Defense for Networks & Information Integration (AS-NII) who acts as the DOD CIO as well as the chair for the GIG Panel.

Checks

Net ISP Unauthorized

Have the IAM provide a copy of the approval letter and then verify obtained from the GIG Waiver Panel or the Assistant Secretary of Defense (NII).

Default Finding Details The site has an unauthorized connection to an ISP.

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

Fixes

NET ISP Unauthorized

Have the IAM provide a copy of the DAA written approval letter and then verify the mission need is still valid.

Notes:

NET0168

V0014634 CAT II

External IDS must be installed in AG architecture

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If the site has a non-DoD external connection (Approved Gateway), the IAO/NSO will ensure that the external NIDS is located between the site's Approved Gateway (Service Delivery Router) and the premise router.

Vulnerability Discussion The incorrect placement of the external NIDS may allow unauthorized access to go undetected and limit the ability of security personnel to stop malicious or unauthorized use of the network. In order to ensure that an attempted or existing attack goes unnoticed, the data from the sensors must be monitored continuously.

Checks

NET AG PPS policy

Inspect the network topology and physical connectivity to verify compliance.

Default Finding Details An external IDS is not installed in a AG architecture

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

Fixes

NET AG PPS policy

Locate the external NIDS is located between the site's Approved Gateway (Service Delivery Router) and the premise router.

Notes:

NET0170 V0008052 CAT II Backdoor network connections bypasses perimeter.

8500.2 IA Control: EBCR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that no backdoor connections exist between the site's secured private network and the Internet, NIPRNet, SIPRNet, or other external networks unless approved by the DAA.

Vulnerability Discussion The term "backdoor connection" is used to refer to a connection between two customer sites (DOD Enclaves) that do not traverse the provider's network, in this case, the Defense Information System Network (DISN). Routes over this connection are called "backdoor routes." Without taking the proper safeguard steps, this connection could impose security risks to either site. For example, as a result of connection availability or routing protocol administrative distances (i.e., the backdoor route is more favorable), it is possible that traffic destined for other networks from site B's network and vice versa could pass through Site A's premise router. It is also possible that traffic from Site B's network could be destined for Site A's network. In either case, the premise router external interface providing the backdoor connection must have the same ingress filtering applied as an external interface providing a connection to the NIPRNet, SIPRNet, or ISP. Though both networks consider each other a trusted network, the risk becomes evident when one of the networks has been breached, leaving the other in a vulnerable position. Backdoor connections bypassing the network's perimeter (i.e., premise or screening router, firewall, IDS, etc.) are prohibited unless the connection is mission critical and approved by the DAA.

Checks

NET Backdoor protection

Interview the IAM to verify that all connections have a mission requirement and that the DAA is aware of the requirement.

Default Finding Site has a backdoor connection that bypass the Enclave Security Architecture and it has not been reviewed and approved by the CIO
Details and GO42.

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

Fixes

NET Backdoor Protection

Backdoor connections that are not validated and approved by the CIO will be reported to the CIO for disposition.

Notes:

NET0175

V0008053 CAT II

The site is using IPv6 without DAA approval.

8500.2 IA Control: EBCR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that IPv6 implemented on any DOD network that transports production or operations traffic is approved by the DAA.

Vulnerability Discussion As part of the GIG integrated architecture strategy, the migration to IPv6 across DoD networks will consider operational requirements, risks, and costs, while maintaining interoperability within the DoD, across the Federal Government. Due to the level of risks associated with improper implementations, protocol version 6 must be approved by the DAA.

Checks

NET IPv6 Approval

Review all router configurations to determine if they have been enabled to forward IPv6 unicast datagrams and if any IPv6 addresses have been assigned to any interfaces.

Default Finding Details The site is using IPv6 without DAA approval.

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

Fixes

NET IPv6 Approval

Ensure that all IPv6 migrations plans are approved by the DAA prior to implementation on production or operational networks.

Notes:

NET0196 **V0014636** **CAT III** **IPv6 Address Privacy**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that a devised hard to guess IPv6 scheme is implemented through out the infrastructure.

Vulnerability Discussion The IPv6 address, as currently defined, consists of 64 bits of network number and 64 bits of host number. The large address space of IPv6 makes scanning impractical, but attackers can guess important router addresses by assuming that you've chosen obvious addresses. Avoid assigning easy guessed addresses such as 2001:db8::1, ::2, ::10, ::20, ::30, and etc for network device interfaces. It is recommended that you devise a scheme for assigning hard to guess addresses for the enclave network devices. Those concerned with privacy issues should note that 64 bits makes a large enough field to maintain excellent privacy for the enclave.

Checks

NET NAT requirement

Review the IPv6 scheme and determine if the host, and nodes are using an easily guessed IP assignment. Avoid assigning easy guessed addresses such as 2001:db8::1, ::2, ::10, ::20, ::30, and etc for network device interfaces.

Default Finding Details A devised hard to guess IPv6 scheme is not implemented through out the infrastructure.

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

Fixes

NET NAT Requirement

Implement a random IPv6 scheme that takes advantage of the large network range that is available. IETF's IPNG working group has recommended that the address block given to a single edge network, which may be recursively, subnetted be a 48-bit prefix. This gives each such network 2¹⁶ (65,536) subnet numbers to use in routing. A /48 prefix under the 001 Global Unicast Address prefix contains 45 variable bits. That is, the number of available prefixes is 2 to the power 45 or about 35 trillion (35,184,372,088,832).

Notes:

NET0198 **V0008099** **CAT III** **The DHCP server is not configured to log hostnames**

8500.2 IA Control: DCBP-1, ECAR-1, ECAR-2, ECAR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the DHCP server is configured to log hostnames or MAC addresses for all clients and all logs are stored online for 30 days and offline for one year.

Vulnerability Discussion In order to identify and combat IP address spoofing, it is highly recommended that the DHCP server logs MAC addresses or hostnames on the DHCP server.

Checks

NET DHCP Logging

Have the DHCP administrator display the log files for visual inspection. Verify retention of log files.

Default Finding Details The DHCP server is not configured to log hostnames or MAC addresses for all clients.

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

Fixes

NET DHCP Logging

The IAO will ensure that the DHCP server is configured to log hostnames or MAC addresses.

Notes:

NET0199 **V0008100** **CAT III** **DHCP lease duration is less than 30 days on SIPR.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that any DHCP server used within SIPRNet infrastructure is configured with a lease duration time of 30 days or more.

Vulnerability Discussion In order to trace, audit, and investigate suspicious activity, DHCP servers within the SIPRNet infrastructure must have the minimum lease duration time configured to 30 or more days.

Checks

NET DHCP Lease Duration

Review the DHCP configuration.

Default Finding Details A DHCP server used within SIPRNet infrastructure is not configured with a minimum lease duration time of 30 or more days.

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

Fixes

NET DHCP Lease Duration

The IAO will ensure that any DHCP server used within SIPRNet infrastructure is configured with a minimum duration time of the lease to 30 or more days.

Notes:

NET0210 **V0008054** **CAT II** **Network devices are not stored in secure Comm room**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all network devices (i.e., IDS, routers, RAS, NAS, firewalls, etc.) are located in a secure room with limited access.

Vulnerability Discussion If all communications devices are not installed within controlled access areas, risk of unauthorized access and equipment failure exists, which could result in denial of service or security compromise. It is not sufficient to limit access to only the outside world or non-site personnel. Not everyone with the site has the need-to-know or the need-for-access to communication devices.

Checks

NET Comm Closet

The IAO/NSO will ensure the physical network components are in a secure environment.

Default Finding Details Communications devices are not stored in a secure location.

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

Fixes

NET Comm Closet

The IAO will ensure all critical communications are in a controlled access areas. Controlled access area in this case means controlled restriction to authorize site personnel, i.e., dedicated communications rooms or locked cabinets. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the network from unauthorized personnel. The keys to the locked cabinets and dedicated communications rooms will be controlled and only provided to authorized network/network security individuals.

Notes:

NET0260

V0008055 CAT II

Accepted password generation schemes are not used.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all passwords are created and maintained in accordance with the rules outlined in DODI 8500.2, IAIA-1, and IAIA-2. <http://www.dtic.mil/whs/directives/corres/html/85002.htm>.

Vulnerability Discussion Devices protected with weak password schemes provide the opportunity for anyone to crack the password, gaining access to the device and causing network, device, or information damage or denial of service.

Checks

NET Password Protection

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

Default Finding Details Accepted password generation schemes are not being employed on all network devices.

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

Fixes

NET Password Protection

Ensure all communication devices are in compliance with password policy.

Notes:

NET0270

V0008056 CAT II

Passwords are not recorded and stored properly.

8500.2 IA Control: DCBP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will record the locally configured passwords used on communications devices and store them in a secured manner.

Vulnerability Discussion Passwords should be recorded and stored in a secure location for emergency use. This helps prevent time consuming password recovery techniques and denial of administrator access, in the event a password is forgotten or the individual with the access is incapacitated. Router configurations contain passwords in clear text. This must be encrypted for use in areas where this can be compromised.

Checks

NET PSWD Recorded/Stored

Passwords need to be recorded and stored in a secure manner.

Default Finding Details Passwords used on communications devices are not recorded and stored in a secure or controlled manner.

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

Fixes

NET PSWD Recorded/Stored

The IAO will record the passwords used on communications devices and store them in a secure or controlled manner.

Notes:

NET0345 **V0008065** **CAT II** **Firewalls must meet EAL4 evaluation rating.**

8500.2 IA Control: DCAS-1, DCSR-1, DCSR-2, DCSR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IA/O will ensure only firewalls that have obtained the DoD Application-Level for Medium Robustness Environments Protection Profile (PP) are placed in the network infrastructure meeting a Common Criteria PP of EAL 4 or greater.

Vulnerability Discussion With the massive amount of firewall vendors on the market, the only assurance that the firewall meets or exceeds the minimum security requirements obtained in the Enclave Security Policy and the Network Infrastructure STIG is the Common Criteria EAL4 rating.

Checks

Firewall EAL4 by NIST

Have the firewall or network administrator provide a copy of the common criteria award provided from the vendor.

Search http://niap.nist.gov/cc-scheme/vpl/vpl_type.html for current ratings.

Default Finding Details Sites firewall has not been evaluated to the Common Criteria EAL4 rating.

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

Fixes

Firewall EAL4 by NIST

The NSO needs to incorporate a Common Criteria EAL4 rated firewall into the perimeter defenses.

Notes:

NET0346 **V0014638** **CAT II** **A DMZ architecture is not implemented.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IA/O/NSO will ensure that DMZ Architecture is implemented, providing boundary protection for classified and sensitive architectures that interconnect enclaves.

Vulnerability Discussion Without a screened subnet (DMZ) architecture traffic that would be normally destined for the DMZ would have to be redirected to the sites internal network. This would allow for a greater opportunity for hackers to exploit.

Checks

NET FW DMZ

A DMZ is defined and required by all medium robust DOD networks as documented in 8500.2. Verify this requirement by inspecting the site network topology and firewall interface configurations.

Default Finding Details A DMZ architecture is not implemented.

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

Fixes

NET FW DMZ

Use the network diagram in the STIG for guidance for services that should be located on DMZ subnets.

Notes:

NET0347 **V0014639** **CAT III** **DIACAP or DITSCAP documents not updated.**

8500.2 IA Control: DCPR-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the Accreditation documentation (e.g. SSAA) will be updated to reflect the installation or modification of the site's firewall.

Vulnerability Discussion A firewall is the first policy enforcement mechanism that the site uses to enforce the Enclave Security Policy. If the configuration cannot be maintained then the security for the site is suspect and may allow for exploits to be utilized gaining access to the network resources.

Checks

NET DIACAP

The enclave or system owner will identify security domain requirements in the System Security Authorization Agreement (SSAA) or the emerging DIACAP process. Procedures outlined in the DOD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), lay out the process for the enclave security architecture as they are applied to specific requirements. Each SSAA will include a description of the architectural implementation of the security requirements identified in this STIG. As the transition to DITSCAP to DIACAP nears completion, new DIACAP requirements will need to be met as replacement of the DITSCAP requirements.

Default Finding Details DIACAP or DITSCAP documents are not current updated.

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

Fixes

NET DIACAP

Verify the SSAA or DIACAP documents reflect changes made to the firewall.

Notes:

NET0348 **V0014640** **CAT II** **Public servers must be in a DMZ.**

8500.2 IA Control: EBPW-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure publicly accessible servers (i.e., web servers) are placed in an enclave DMZ.

Vulnerability Discussion The only way to mediate the flow of traffic between the inside network and the outside connection is to locate the servers with public connectivity into the DMZ. Placement in this manner allows the firewall the ability to screen the content.

Checks

NET DMZ Servers

Review the architecture diagram and other resources available and determine if servers are located in a DMZ.

Default Finding Details Public servers are not in a DMZ.

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

Fixes

NET DMZ Servers

Move publicly accessible servers to the DMZ. If a DMZ has not been built, established a Plan of Action with milestones to accomplish the task.

Notes:

NET0351 **V0008066** **CAT II** **Firewall placement is not IAW the Network STIG.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure, when protecting the boundaries of a network, the firewall is placed between the private network and the perimeter router and the DMZ.

Vulnerability Discussion The only way to mediate the flow of traffic between the inside network, the outside connection, and the DMZ is to place the firewall into the architecture in a manner that allows the firewall the ability to screen content for all three destinations.

Checks

NET Firewall Location

Inspect the network topology diagrams and visually trace the firewall connections.

Default Finding Details Firewall placement is not IAW the Network STIG.

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

Fixes

NET Firewall Location

Move the firewall into the prescribed location to allow for enforcement of the Enclave Security Policy and allow for all traffic to be screened.

Notes:

NET0355 **V0014641** **CAT II** **Integrated Device not IAW STIG**

8500.2 IA Control: EBPW-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure, when protecting the boundaries of a network, the firewall and IDS/IPS are separate components.

Vulnerability Discussion An integrated solution implemented within DoD should not waive from defense in depth practices. Many solutions available have leveraged processors and memory. Once this technology is compromised all security layers of defense are subject to DOS in a single attack. Integrated solutions within DoD require the firewall and the IDS solution to be on separate devices or CPUs that do not shared the same memory.

Checks

NET FW Integration

Review the architecture and validate the firewall and IDS are separate components or the Integrated solution is similar to the diagram in the STIG. The IDS must be on a separate CPUs that do not shared the same memory.

Default Finding Details Public servers must be in a DMZ

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

Fixes

NET FW Integration

Implementation of a new architecture is required. Establish a POA&M.

Notes:

NET0365 **V0014642 CAT I** **No deep packet inspection**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the enclave is protected by providing a firewall that provides full packet awareness as provided by application-level gateways, hybrid firewalls or a non application-level firewall solution using an application-proxy gateway.

Vulnerability Discussion Implementing firewall solutions without full packet awareness and proxy capabilities do not offer very granular application-level control such as blocking file transfers involving filenames ending in .exe. Disadvantages also include no capabilities to enforce user authentication, no hardware or software token authentication, no source address authentication, or biometric authentication.

Checks

NET FW DPI Inspection

Review the firewall specification sheet. The Enclave requirement to place a firewall at the perimeter can be accomplished by multiple scenarios to include the following:

- An application-level firewall at the perimeter to protect the whole Enclave to include the Security Domains.
- A non application-level firewall at the perimeter (e.g., packet-filter, stateful inspection, deep packet inspection) with a dedicated proxy server or application-proxy gateway protecting every Security Domains.
- A Hybrid firewall at the perimeter to protect the whole Enclave to include the Security Domains capable of application-proxy functionality.

Due to technological advances there are devices such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or stateful inspection firewall, in collaboration with application level proxy devices to service all connections identified in the PPS CAL boundaries 7, 8, 11 and 12 is an acceptable alternative.

Default Finding Details A firewall is not implemented to perform deep packet inspection.

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

Fixes

NET FW DPI Inspection

The site architecture needs to deploy a firewall solution as described above in the ôCheckö field.

Notes:

NET0369

V0011796 CAT I

Deny-by-default is not implemented

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the Enclave perimeter is protected via deny by default policy implemented at the perimeter router or at the firewall. This does not negate the firewall requirement.

Vulnerability Discussion Allowing unknown traffic into the enclave can make all devices susceptible within the enclave to an attack. System Administrators need to identify trusted neighbors and define permit rules with known applications (protocols) they require use of. All unknown traffic must be denied at the perimeter.

Checks

Perimeter Protection

The requirement for perimeter protection includes either a firewall implemented to protect the enclave and in deny-by-default posture or the premise router in a deny-by-default posture. One or the other will satisfy the requirement at the enclave boundary.

Default Finding Details Deny by default policy is not implemented.

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

Fixes

Perimeter Protection

The site must have either a firewall to protect the entire facility OR the perimeter router must be configured with a deny-by-default policy.

Notes:

NET0384

V0008067 CAT III

Firewall admin must register with vendor

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.

Vulnerability Discussion Not being on the vendors vulnerability list can lead to the firewall software not being updated when a new release or security patch is released by the vendor.

Checks

NET FW Vendor Mail List

Interview the FA for compliance.

Default Finding Details The Firewall administrator has not subscribed to the vendors vulnerability mailing list.

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

Fixes

NET FW Vendor Mail List

Have the FA subscribe to the vendors vulnerability mailing list.

Notes:

NET0420

V0008058 CAT II

Key management policy has not been implemented

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure a key management policy has been implemented to include key generation, distribution, storage, usage, lifetime duration, and destruction of all keys used for encryption.

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 the site's written procedures to determine if they are compliant with this requirement.

Default Finding Details The NSO does not have written procedures for key management or the procedures do not cover the following critical areas:

Key exchanged every 6 months
Time expiration
Physical storage
Key compromise

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

Fixes

NET MD5 Key Management

Implement a key management policy that includes key generation, distribution, storage, usage, lifetime duration, and destruction of all keys used for encryption within the infrastructure.

Notes:

NET0430

V0014720 CAT II

Authentication server must be used to gain access

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure an authentication server is used to gain administrative access to all network devices.

Vulnerability Discussion AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage. Without AAA, unauthorized users may gain access and possibly control of the routers. If the router network is compromised, large portions of the network could be incapacitated with only a few commands.

Checks

NET Authentication Access

Base Example: Verify that an authentication server is required to access the router by reviewing the running configuration.

CISCO Example:

The aaa new-model statement must be present as it enables AAA. The authentication list-name defined in the aaa authentication statement must be specified for console and vty access via the login statement as shown above. The authentication server must be defined to the router (i.e., tacacs-server, radius-server) and must be reachable; otherwise, the next available authentication method specified in the list-name will be used (i.e. local). You should find an authentication statement similar to the example below:

```
aaa new-model
aaa authentication login list-name tacacs+ local
..
tacacs-server host x.x.x.x
tacacs-server key xxxx
..
line vty 0 4
login authentication list-name
```

Junos Example:

```
[edit system]
authentication-order [radius password];
radius-server {
  7.7.7.5 {
    secret xxxxx;
    timeout 20;
  }
}
```

Note: The timeout parameter is amount of time in seconds that the local router waits to receive a response from a RADIUS or TACACS+ server.

Default Finding Details Authentication server is not used to gain access.

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

Fixes

NET Authentication Access

The router administrator will configure the TACACS+, Radius or Diameter server with standard accounts and user passwords.

Notes:

NET0431

V0014721 CAT III

AAA server does not redirect to two-factor server

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all AAA authentication services are configured to use two-factor authentication during normal operation.

Vulnerability Discussion AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server. Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage. Without AAA, unauthorized users may gain access and possibly control of the routers. If the router network is compromised, large portions of the network could be incapacitated with only a few commands.

Checks

NET Authentication Access

Procedure: The implementation varies and a thorough review is necessary. Have the SA review and discuss their implementation. A typical AAA process includes the network system redirecting user access requests either directly to an ACE/Server or to a CiscoSecure ACS (TACACS+) server which redirects the 'authentication' request to the ACE/Server for strong authentication via user tokens (keyfobs). During the review have the SA point out the calls from the TACACS+ or Radius servers to the authentication server performing the two-factor requirement.

Default Finding Details AAA server does not redirect/call to a two-factor authentication server.

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

Fixes

NET Authentication Access

The administrator will configure the TACACS+, Radius or Diameter server to redirect user request for two factor authentication.

Notes:

NET0432

V0014722 CAT III

AAA server is not configured to use tier groups

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the device is configured to use AAA tiered authorization groups for management authentication.

Vulnerability Discussion The foundation of a good security scheme in the network is the protection of the user interfaces of the networking devices from unauthorized access. Protecting access to the user interfaces on your network devices prevents unauthorized users from making configuration changes that can disrupt the stability of your network or compromise your network security.

Checks

NET Authentication Access

Procedure: Review the AAA server implemented and determine if user profiles are members of a group. Determine if the groups have different privileges and the users are in the appropriate groups. In the following TACACS example the user (rtr-test) is a member of the group "rtr-basic".

```
<CSUser>$/opt/ciscosecure/CLI/ViewProfile -p 9900 -u rtr_test
User Profile Information
user = rtr_test{
  profile_id = 66
  profile_cycle = 1
  member = rtr_basic
  password = des "*****"
}
```

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

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

Default Finding Details AAA server is not configured to use tier authorization groups.

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

Fixes

NET Authentication Access

The SA will configure the TACACS+, Radius or Diameter server with standard accounts and assign them to privilege levels that meet their job description.

Notes:

NET0445

V0014723 CAT II

Two-factor authentication is not implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure device management is restricted by two-factor authentication (e.g., Secure ID, DoD PKI, or alternate token logon).

Vulnerability Discussion Without secure management implemented with authenticated access controls, strong two-factor authentication, encryption of the management session and audit logs, unauthorized users may gain access to network managed devices compromised, large parts of the network could be incapacitated with only a few commands.

Checks

Net Two-factor Authentication

First review the device configuration to ensure that an authentication server is being used. Then verify that a 2-factor authentication method has been implemented. In most cases a two-factor implementation is called by a Radius or TACACS Server.

Default Finding Details Two-factor authentication is not implemented.

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

Fixes

NET Two-factor Authentication

The network administrator will ensure strong two-factor authentication is being incorporated in the access scheme.

Notes:

NET1022

V0014724 CAT III

The syslog server is not located on management LAN

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the syslog server is only connected to the management network.

Vulnerability Discussion A syslog server provides the network administrator the ability to configure all of the communication devices on a network to send log messages to a centralized host for review, correlation, reporting, and storage. This implementation provides for easier management of network events and is an effective facility for monitoring and the automatic generation of alert notification. The repository of messages facilitates troubleshooting functions when problems are encountered and can assist in performing root cause analysis.

A malicious user or intruder could attempt to cover his tracks by polluting the syslog data or even force the server to crash. Disabling the syslog server would eliminate visibility of the network infrastructure that security analysts depend on. The first line of defense is to ensure that the syslog server will only accept syslog packets from known managed devices and administrative access from trusted management workstations. Because syslog messages are sent from managed devices to the syslog server in clear text an attacker on the network can easily sniff the messages. Furthermore, the syslog protocol uses UDP; thereby, making it relatively easy to spoof a managed device. Placing the syslog server on a separate subnet such as the management network isolated from general access and transient traffic will assist in reducing these risks.

Checks

NET Syslog Mgt LAN

Physically inspect the syslog server and its LAN connection as well as review the network topology diagram to verify compliance.

Default Finding Details The syslog server is not located on management LAN

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

Fixes

NET Syslog Mgt LAN

Ensure the syslog server is only connected to the management network

Notes:

NET1023

V0014725 CAT II

The syslog server is not compliant with OS STIG

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the syslog servers are configured IAW the appropriate OS STIG.

Vulnerability Discussion A syslog server provides the network administrator the ability to configure all of the communication devices on a network to send log messages to a centralized host for review, correlation, reporting, and storage. This implementation provides for easier management of network events and is an effective facility for monitoring and the automatic generation of alert notification. The repository of messages facilitates troubleshooting functions when problems are encountered and can assist in performing root cause analysis.

A malicious user or intruder could attempt to cover his tracks by polluting the syslog data or even force the server to crash. Disabling the syslog server would eliminate visibility of the network infrastructure that security analysts depend on. The first line of defense is to ensure that the syslog server will only accept syslog packets from known managed devices and administrative access from trusted management workstations. Because syslog messages are sent from managed devices to the syslog server in clear text an attacker on the network can easily sniff the messages. Furthermore, the syslog protocol uses UDP; thereby, making it relatively easy to spoof a managed device. A major step to securing the server is to ensure that it is compliant with the respective OS STIG.

Checks

NET Syslog Mgt LAN

Interview the IAO and syslog administrator to determine if the server is compliant with respective OS STIG.

Default Finding Details The syslog server is not compliant with OS STIG

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

Fixes

NET Syslog Mgt LAN

Ensure the syslog servers is configured IAW the respective OS STIG.

Notes:

NET1025 **V0008060** **CAT III** **A centralized syslog server has not been deployed.**

8500.2 IA Control: ECSC-1, ECTB-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure a centralized syslog server is deployed and configured by the syslog administrator to store all syslog messages for a minimum of 30 days online and then stored offline for one year.

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.

Checks

NET Syslog SRV Log Retention

Examine the syslog server to verify that it is configured to store messages for at least 30 days. Have the administrator show you the syslog files stored offline for one year.

Default Finding Details The syslog server is not configured to store syslog messages for 30 days on-line and/or syslog messages are not stored off-line for one (1) year.

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

Fixes

NET Syslog SRV Log Retention

The router administrator will configure the syslog server to store messages for at least 30 days on-line. The router administrator will establish a syslog storage strategy for storing the logs off-line for minimum of 1 year.

Notes:

NET1040 **V0008061** **CAT III** **Configurations must be stored in a secure location**

8500.2 IA Control: COBR-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.

Vulnerability Discussion If the router, as well as, volatile and non-volatile memory are lost without a recent configuration stored in an offline location, it may take time to recover that segment of the network. Subscribers connected directly to that router may be without service for a longer than acceptable time.

Checks

NET Backup Configurations

IOS Procedure: Have the router administrator show you the stored configuration files. At a minimum, a copy of the current and previous router configurations must be saved.

JUNOS Procedure: With Juniper, this is built in and would never be a finding. Previously committed configurations 0 – 4 are saved on flash and configurations 5 – 9 are saved on the router's hard drive. Any one of these can be used for recovery via a rollback command.

Default Finding Details The current and previous router configurations are not stored in a secure location.

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

Fixes

NET Backup Configurations

The router administrator will store the current and previous router configurations in a secure location.

Notes:

NET1060

V0008062 CAT I

Unencrypted passwords are stored offline

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The router administrator will not store unencrypted router passwords in an offline configuration file.

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 Password Storage

Review the stored router configuration files to ensure passwords are not stored in plain-text format.

Default Finding Details Unencrypted passwords are stored in plain text in the routers off-line configuration.

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

Fixes

NET Password Storage

The router administrator will ensure that any router passwords that are stored, are encrypted. Delete any un-encrypted passwords that are currently stored as part of a router configuration file. Incorporate the storage of encrypted passwords as part of the router SOP.

Notes:

NET1070

V0008063 CAT II

TFTP used without written approval.

8500.2 IA Control: DCBP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will authorize and maintain justification for all TFTP implementations.

Vulnerability TFTP requires no password.

Discussion

Checks

NET TFTP Authorization

Base Procedure Verify written authorization is with the IAO. Review and recommend the procedures defined below:

IOS Procedure: Interview the router administrator to see how they transfer the router configuration files to and from the router. Verify that the running configuration for all Cisco routers have statements similar to the following:

```
ip ftp username xxxxxxxxx  
ip ftp password 7 xxxxxxxxxxxxxxxxxxx
```

Following are some alternative approaches that are actually more secured than using FTP:

1. If the router is equipped with PCMCIA Flash Memory Cards, you can copy IOS images as well as configurations to these cards (i.e., slot0, slot1).
2. Copy and paste from a show run while in a SSH session or HyperTerminal (i.e., Capture Text) console connection. The file can then be saved onto a floppy disk and stored in a secured location. Defaults will not be included since most of the IOS defaults are not displayed on a show run command.
3. Secure Copy Protocol (SCP)

Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the Cisco router. SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level. SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the copy command. An authorized administrator may also perform this action from a workstation.

An example configuration would look as follows:

```
! AAA authentication and authorization must be configured for SCP to work.  
aaa new-model  
aaa authentication login default group tacacs+  
aaa authorization exec default group tacacs+  
.....  
! SSH must be configured.  
ip ssh time-out 120  
ip ssh authentication-retries 3  
ip scp server enable
```

Junos Procedure: Configuration files can be copied to and from the router using the file copy command in operational mode or save command while in configuration mode. The destination address is specified on the command line—never preconfigured. Destinations can be the router's flash (path/filename), hard drive (/var/filename), removable media (a:filename), FTP server (ftp://hostname/path/filename), TFTP server (tftp://hostname/path/filename), HTTP server (http://hostname/path/file), or an Secure Copy Protocol (SCP) client (scp://hostname/path/filename).

Unless TFTP, FTP, or HTTP is specified in the command string, both the save and file copy commands will utilize Secure Copy Protocol, which uses the SSH authentication and encryption framework, to securely copy files to and from a remote host. Interview the router administrator to determine what method is used. If the site uses TFTP or HTTP with the save or file copy command, this is a finding.

Default Finding TFTP is being used to transfer the router configuration and image files to and from the routers.

Details

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

Fixes

NET TFTP Authorization

The router administrator will ensure that FTP is used to transfer router configuration files to and from the router if TFTP has not been authorized by the IAO.. Change the routers configuration to include FTP setup information as follows: Address or name of remote host [?] x.x.x.x; Source file name [?] path/filename; Destination filename [?] path/filename.

Notes:

NET1110 V0008064 CAT II Configuration Mgt procedures are not in place

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all changes and updates are documented in a manner suitable for review and audit.

Vulnerability Discussion Change management is the formal review process that ensures that all changes made to a system receive formal review and approval. Change management reduces impacts from proposed changes that could possibly have interruptions to the services provided. Recording all changes in the network will be accomplished by a configuration management policy. The configuration management policy will capture the actual changes to software code and anything else affected by the change.

Checks

NET CM Process not Controlled

Interview IAO/NSO to verify a Change Management policy is in compliance. Changes and Updates should be suitable for the audit.

Default Finding Details All router changes and updates are not documented in a manner suitable for review.

Request forms are not used to aid in recording the audit trail of router changes requested.

Changes and modifications to routers are not audited so that they can be reviewed.

Paper or electronic copies of router configurations are not maintained in a secure location.

Unauthorized personnel are allowed to request changes to routing tables or service parameters.

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

Fixes

CM Process not Controlled

Implement a Change Management policy that ensures review of scheduled and documented changes. Record configuration changes and review periodically. Develop and use a form or tracking mechanism to aid in the audit trail of any router changes requested of the NSO.

Notes:

NET1111 V0014718 CAT II Configuration Mgt forms are not being used

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure request forms are used to aid in recording the audit trail.

Vulnerability Discussion Change management is the formal review process that ensures that all changes made to a system receive formal review and approval. Change management reduces impacts from proposed changes that could possibly have interruptions to the services provided. Recording all changes in the network will be accomplished by a configuration management policy. The configuration management policy will capture the actual changes to software code and anything else affected by the change.

Checks

NET CM Process not Controlled

Have the IAO/NSO provide copies of change request forms for visual inspection.

Default Finding Details Configuration Mgt forms are not being used.

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

Fixes

NET CM Process not Controlled

Implement a Change Management policy that ensures review of scheduled and documented changes. Record configuration changes and review periodically. Develop and use a form or tracking mechanism to aid in the audit trail of any router changes requested of the NSO.

Notes:

NET1113 V0014719 CAT II Change Mgt documents are not in secure storage

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure current paper or electronic copies of configurations are maintained in a secure location.

Vulnerability Discussion Change management is the formal review process that ensures that all changes made to a system receive formal review and approval. Change management reduces impacts from proposed changes that could possibly have interruptions to the services provided. Recording all changes in the network will be accomplished by a configuration management policy. The configuration management policy will capture the actual changes to software code and anything else affected by the change.

Checks

NET CM Process not Controlled

Have the IAO/NSO identify the secured storage area where Change Mgt documents are stored.

Default Finding Details

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

Fixes

NET CM Process net Controlled

Implement a Change Management policy that ensures review of scheduled and documented changes. Record configuration changes and review periodically. Develop and use a form or tracking mechanism to aid in the audit trail of any router changes requested of the NSO.

Notes:

NET1114 V0015430 CAT II Unauthorized Change Control updates

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.

Vulnerability Discussion Limiting the number of people that can request changes to router tables and service parameters limits the chance of errors and thus limits the chance of creating a denial-of-service vulnerability.

Checks

NET Change Control Integrity

Interview IAO and router administrator to verify compliance.

Default Finding Details Unauthorized personnel are allowed to request changes to routing tables or service parameters.

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

Fixes

NET Change Control Integrity

Have the IAO modify the Change Control Process.

Notes:

NET1280 V0008068 CAT III The firewall logs are not being reviewed daily.

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure there is a review on a daily basis, of the firewall log data by the firewall administrator (FA), or other qualified personnel, to determine if attacks or inappropriate activity has occurred.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis.

Checks

NET FW Review Logs Daily

Review site policy, then interview FW administrator and authorized personnel with FW access to determine compliance.

Default Finding Details Firewall logs are not being reviewed daily.

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

Fixes

NET FW Review Logs Daily

Insure that the NSO or FA reviews the firewall logs daily.

Notes:

NET1281

V0014726 CAT III

An HIDS is not implemented on the syslog server

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the syslog servers are configured IAW the appropriate OS STIG.

Vulnerability Discussion A syslog server provides the network administrator the ability to configure all of the communication devices on a network to send log messages to a centralized host for review, correlation, reporting, and storage. This implementation provides for easier management of network events and is an effective facility for monitoring and the automatic generation of alert notification. The repository of messages facilitate troubleshooting functions when problems are encountered and can assist in performing root cause analysis.

A malicious user or intruder could attempt to cover his tracks by polluting the syslog data or even force the server to crash. Disabling the syslog server would eliminate visibility of the network infrastructure that security analysts depend on. The first line of defense is to ensure that the syslog server will only accept syslog packets from known managed devices and administrative access from trusted management workstations. Because syslog messages are sent from managed devices to the syslog server in clear text an attacker on the network can easily sniff the messages. Furthermore, the syslog protocol uses UDP; thereby, making it relatively easy to spoof a managed device. A host intrusion detection system (HIDS) should also be implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.

Checks

NET Syslog Mgt LAN

Interview the IAO and syslog administrator to determine if the server is compliant. Have the administrator provide a demonstration of the HIDS capability to ensure that it is configured and in operation.

Default Finding Details

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

Fixes

NET Syslog Mgt LAN

Ensure an HIDS is implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.

Notes:

NET1284 **V0008070** **CAT III** **The firewall configuration is not backed up weekly**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the firewall configuration data are backed up weekly and whenever configuration changes occur.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

Checks

NET FW Config BU Weekly

Review site policy and interview FW administrator.

Default Finding Details The firewall configuration data is not backed up weekly and whenever configuration changes occur.

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

Fixes

NET FW Config BU Weekly

Back up firewall configuration data on a weekly basis.

Notes:

NET1286 **V0008071** **CAT III** **The audit logs are not backed up weekly**

8500.2 IA Control: ECSC-1, ECTB-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the audit data is backed up weekly.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

Checks

NET FW Log BU Weekly

Review site policy and interview IAO.

Default Finding Details The firewall logs are not backed up weekly.

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

Fixes

NET FW Log BU Weekly

Backup logs on a weekly basis.

Notes:

NET1287

V0014727 CAT III

The audit logs are not protected

8500.2 IA Control: ECSC-1, ECTB-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the audit logs are protected from deletion.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

Checks

NET FW Log Protected

Review site deletion rights of the audit log file.

Default Finding The audit logs are not protected.

Details

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

Fixes

NET FW Log Protected

Correct access privileges to protect the file.

Notes:

NET1288

V0014728 CAT III

Firewall log must be accurate

8500.2 IA Control: ECSC-1, ECTB-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the audit trail events are stamped with accurate date and time.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

Checks

NET FW Log Protected

Review the active log and verify the date and time of the records is correct.

Default Finding Firewall log must be accurate.

Details

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

Fixes

NET FW Log Protected

Ensure the firewall is receiving time from the same source as other network devices are, such as the perimeter router. Verify the NTP guidance is implemented correctly.

Notes:

NET1289 **V0014729** **CAT III** **FW event records do not include required fields**

8500.2 IA Control: ECSC-1, ECTB-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the audit trail events include source IP, destination IP, protocol used and action taken.

Vulnerability Discussion The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

Checks

NET FW Log Protected

Review the active log and verify the source IP, destination IP, protocol used and action taken are recorded fields in the event record..

Default Finding Details FW event records do not include required fields.

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

Fixes

NET FW Log Protected

Ensure the firewall is receiving source IP, destination IP, protocol used and action taken.

Notes:

NET1299 **V0014730** **CAT III** **FW must have report capabilities**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the firewall provides the ability to perform searches and sorting of audit data, based on (user identity, source identity, destination identity, ranges of one or more: dates, times, user identities, service identifiers, or transport layer protocol, rule identity, and network interfaces).

Vulnerability Discussion Audit data should be capable of being searched and sorted on all criteria. Sorting will provide capabilities to arrange the audit records such that they are "grouped" together for administrative review. For example the Audit Administrator may want all the audit records for a specified source or range of source identities (e.g., IP source address or range of IP source addresses) presented together to facilitate their audit review.

Checks

NET IDS NIAP

Validate the IDS and OS version are NIAP approved and meet EAL 2 standards.

Default Finding Details FW must have report capabilities.

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

Fixes

NET IDS NIAP

Create a POA&M to purchase an approved product.

Notes:

NET1325 V0008072 CAT II An external NIDS has not been implemented.

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If an NID is required by the CNDSP, the IAO/NSO will ensure that an external NIDS is installed and implemented so that all external connections can be monitored.

Vulnerability Discussion The incorrect placement of the external NIDS may allow unauthorized access to go undetected and limit the ability of security personnel to stop malicious or unauthorized use of the network.

Checks

NET IDS CNDSP Required

CAVEAT: If a site does not have a direct link to a NIPRNet or SIPRNet node router—that is, its connection to the NIPRNet or SIPRNet is through an upstream link to another activity's premise router, then this site would not be required to have its own external NIDS, if the upstream activity has an external NIDS that is being monitored by the RCERT or a certified CND Service Provider. However, if this site has other external connections such as an Internet Service Provider, this traffic would need to be monitored by a CND Service Provider using an external NIDS.

Procedure: Inspect the network topology to verify compliance.

Default Finding Details Not all of the external connections are being monitored by the external NIDS.

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

Fixes

NET IDS CNDSP Required

Place the external NIDS on the exterior of the network in front of the premise router so that it can monitor all external connections.

Notes:

NET1326 V0008073 CAT II External NIDS is not being monitored by the CNDSP

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If a NID is required by the CNDSP, the IAO/NSO will ensure that the certified CNDSP is continuously monitoring the data from the external NIDS.

Vulnerability Discussion In order to ensure that an attempted or existing attack doesnt go unnoticed, the data from the sensors must be monitored continuously.

Checks

NET IDS CNDSP Monitoring

Have the IAO/NSO provide the agreement from a certified CND Service Provider outlining their responsibilities.

Default Finding Details The data from the external NIDS is continuously being monitored by the RCERT or a certified CND Service Provider.

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

Fixes

NET IDS CNDSP Monitoring

Insure that the data is continuously being monitored by the CND Service Provider.

Notes:

NET1328

V0008075 CAT III

IDS data is being monitored unauthorized persons.

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the data from the external NIDS is restricted to CNDSP personnel only.

Vulnerability Discussion The external NIDS is monitoring all traffic on the external connections. It is imperative that this traffic is only reviewed and monitored by trusted and authorized personnel with a need to know.

Checks

NET IDS Authorized Reviewers

Have the IAO/NSO provide copies of the authorization letter assigning the reviews.

Default Finding Details The external IDS monitoring is not being performed by the RCERT or a certified CND Service Provider.

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

Fixes

NET IDS Authorized Reviewers

The IAO will ensure that the monitoring of the external IDS will be performed by the RCERT or a certified CND Service Provider.

Notes:

NET1330

V0008272 CAT II

The NIDS is not monitoring traffic

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The Network IDS administrator will ensure a Network IDS is installed and operational with all connections (e.g., LAN and WAN) being monitored.

Vulnerability Discussion Although the firewall has logging functions, the first device dedicated to the detection and response of intruders and malicious activities is the Network Intrusion Detection System (NID). This NID provides the site with near real time alarms using known attack signatures and anomaly detection.

Checks

NET IDS Internal Location

Note: If monitoring is being performed using a switch SPAN port, it is recommended that the IDS is configured in Stealth Mode—the NIC connected to the SPAN port would not have any network protocol stacks bound to it. A second NIC would then be connected to an OOB network. Stealth mode will eliminate the risk of the IDS itself being attacked. Stealth mode would not be applicable if the IDS is monitoring from a network tap solution.

The second NIC is for the IDS sensor to be able to backhaul its data via the out-of-band connection to the IDS manager. The sensors need to talk to the manager, so if your sensors are in stealth mode, there is no way to reach the manager on the in-band network.

Procedure: Review the network topology diagrams and equipment.

Default Finding Details The site has failed to install and implement a NIDS inside the enclave.

The NIDS is not monitoring all traffic entering the network infrastructure.

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

Fixes

NET IDS Internal Location

The NSO needs to incorporate a NID into the site architecture IAW the Network Infrastructure STIG.

Notes:

NET1331 **V0014732 CAT III** **IDS is not NIAP approved**

8500.2 IA Control: DCAS-1, DCSR-1, DCSR-2, DCSR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure only NIAP approved IDS components are placed in the network infrastructure meeting a Common Criteria PP of EAL 2 or greater.

Vulnerability Discussion With the massive amount of IDS vendors on the market, the only assurance that the IDS meets or exceeds the minimum security requirements is the Common Criteria ratings.

Checks

NET IDS NIAP

Validate the IDS and OS version are NIAP approved and meet EAL 2 standards.

Default Finding Details IDS is not NIAP approved .

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

Fixes

NET IDS NIAP

Create a POA&M to purchase an approved product.

Notes:

NET1340 **V0008076 CAT II** **The NSO does not have an incident response policy.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will establish policies outlining procedures to notify JTF GNO when suspicious activity is observed.

Vulnerability Discussion A network intrusion system is a policy enforcement mechanism that the site must sue to enforce the Enclave Security Policy. If a clear policy has not be established for reporting suspicious activity to the RCERT, then the site, and possibly all of DoD, is at a greater risk for exposure.

Checks

NET IDS Internal Policies

Have the IAO/NSO provide a copy of the policy outlining procedures to notify the CERT of suspicious activity.

Default Finding Details The NSO does not have an incident response policy.

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

Fixes

NET IDS Internal Policies

Develop an incident response policy and a procedure to carry out the policy.

Notes:

NET1342 V0008077 CAT II Unauthorized personnel have access to the IDS data

8500.2 IA Control: ECAN-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that authorized reviewers of Network IDS data are identified in writing by the site's IAM.

Vulnerability Discussion To preserve the chain of custody for possible legal action, all reviewers of the NID data must be have an authorization letter from the site commander outlining the individuals need to know.

Checks

NET IDS Internal Auth Users

Have the IAO/NSO provide a copy of the letter identifying authorized reviewers.

Default Finding Reviewers of the NID data have not been authorized by the site commander.

Details

Unauthorized personnel have access to the IDS data

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

Fixes

NET IDS Internal Auth Users

Have the site commander sign a authorization letter for all individuals that are required to review the NID data. Ensure that only authorized personnel have access to the IDS data.

Notes:

NET1344 V0008273 CAT II Unauthorized traffic is not logged.

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that any unauthorized traffic is logged for further investigation.

Vulnerability Discussion Audit logs are necessary to provide a trail of evidence in case the network is compromised. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker. Information supplied by an IDS can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis.

Checks

NET IDS Internal Logging

Have the IAO/NSO display the logging and auditing features of the NID.

Default Finding Unauthorized traffic is not logged for further investigation.

Details

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

Fixes

NET IDS Internal Logging

Configure the IDS to log all unauthorized or suspicious traffic.

Notes:

NET1346 **V0008078** **CAT II** **NSO has not established weekly backup procedures**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will establish weekly data backup procedures for the Network IDS.

Vulnerability Discussion IDS data needs to be backed up to insure that the IDS data is preserved in the event of a hardware failure of the IDS or the IDS could be breached.

Checks

NET IDS Backups

Verify the IAO/NSO has established weekly backup procedures for IDS data.

Default Finding The NSO has not established weekly backup procedures.

Details

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

Fixes

NET IDS Backups

The NSO has not established weekly backup procedures.

Notes:

NET1348 **V0008079** **CAT II** **IDS Anti-virus updates procedures not in SOP**

8500.2 IA Control: ECSC-1, ECVP-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will establish anti-virus update procedures for the Network IDS.

Vulnerability Discussion To preserve the integrity of the IDS information and its operational capability, it is imperative that anti-virus software is kept up to date.

Checks

NET IDS Internal Virus Updates

Verify the IAO/NSO has established anti-virus updates procedures

Default Finding NSO has not established anti-virus updates procedures

Details

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

Fixes

NET IDS Internal Virus Updates

NSO must establish anti-virus updates procedures

Notes:

NET1350

V0008080 CAT III

SA has not subscribed to the vendor notifications.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The Network IDS administrator will subscribe to the vendor's vulnerability mailing list.

The Network IDS administrator will update the Network IDS when software is provided by Field Security Operations for the RealSecure distribution, and for all other Network IDS software distributions when a security-related update is provided by the vendor.

Vulnerability Discussion Keeping the NID software updated with the latest engine and attack signatures will allow for the NID to detect all forms of known attacks. Not maintaining the NID properly could allow for attacks to go unnoticed.

Checks

NET IDS Internal Updates

Have the SA display update notifications that have been received to determine compliance.

Have the NID SA display the build number or patch level, then search the vendor's vulnerability database for current release and patch level.

Default Finding Details The NID administrator has not subscribed to the X-press update notification or similar service offered by the NID vendor.

The NID administrator has not performed the required maintenance upgrades to the NID when notified by FSO or the vendor.

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

Fixes

NET IDS Internal Updates

Have the NID administrator subscribe to the X-press notification or similar service offered by the vendor.

Ensure the NID software is updated when software is available either by FSO or the vendor for security related distributions.

Notes:

NET1351 **V0015424** **CAT III** **IDS software is not kept current**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The Network IDS administrator will update the Network IDS when software is provided by Field Security Operations for the RealSecure distribution, and for all other Network IDS software distributions when a security-related update is provided by the vendor.

Vulnerability Discussion Keeping the NID software updated with the latest engine and attack signatures will allow for the NID to detect all forms of known attacks. Not maintaining the NID properly could allow for attacks to go unnoticed.

Checks

NET IDS patch

Have the NID SA display the build number or patch level, then search the vendor's vulnerability database for current release and patch level.

Default Finding Details IDS software is not kept current.

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

Fixes

NET IDS patch

Upgrade to current signatures posted by the vendor.

Notes:

NET1362 **V0008081** **CAT II** **Switches & cross-connects are not in secure IDF.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all switches and associated cross-connect hardware are kept in a secured IDF or an enclosed cabinet that is kept locked.

Vulnerability Discussion Since the IDF includes all hardware required to connect horizontal wiring to the backbone wiring, it is imperative that all switches and associated cross-connect hardware are kept in a secured IDF or an enclosed cabinet that is kept locked. This will also prevent an attacker from gaining privilege mode access to the switch. Several switch products only require a reboot of the switch in order to reset or recover the password.

Checks

NET SW Location

Visual inspect data closets and verify the closet is locked or if located in an open area that the equipment resides in a secured cabinet.

Default Finding Details

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

Fixes

NET SW Location

The IAO will ensure that all unused data outlets are detached from the network infrastructure or electronically disabled from the network infrastructure in all communications closets.

Notes:

NET1421 V0014733 CAT II SIPRNet port does not have a Hoffman Box

8500.2 IA Control: DCAS-1, DCSR-1, DCSR-2, DCSR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure Port Security implementation without authentication on the SIPRNet will have additional physical controls using a box to enclose the communication port.

Vulnerability Discussion To protect the SIPRNet from MAC address spoofing and comply with Traditional Security requirements an enclosed Communications Box is required on the SIPRNet ports when port authentication has not been implemented.

Checks

NET Hoffman Box

Determine if the site is using 802.1x or a port security implementation that enforces authentication. If the site has not, inspect the wall plates and determine if the SIPRNet communication ports are enclosed by security boxes such as the Hoffman box.

Default Finding Details SIPRNet port does not have a Hoffman Box.

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

Fixes

NET Hoffman Box

If an authentication port security such as 802.1x has not been implemented, purchase Hoffman boxes and use traditional port security.

Notes:

NET1432 V0014734 CAT II Sticky configuration is not fully implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure if Sticky Port Security is implemented, the running and startup configuration files are identical.

Vulnerability Discussion The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If the startup configuration does not mirror the configuration running than the port controls previously used by Sticky will be lost, negating previously approved Sticky ports.

Checks

NET SW Sticky cfg

Compare the startup configuration with the running configuration.

Default Finding Details Sticky configuration is not fully implemented.

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

Fixes

NET SW Sticky cfg

Ensure the configuration are the same.

Notes:

NET1433

V0014735 CAT II

Sticky Connection Approval is not established

8500.2 IA Control: DCAS-1, DCSR-1, DCSR-2, DCSR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure if Sticky Port Security is implemented a security policy is in place where the switch port is not enabled unless there is a connection approval process.

Vulnerability Discussion A process for a Sticky implementation ensures ports remain disabled until requests are approved. The port activation process is such that a switch port does not get enabled unless there is a connection approval for the device at the other end, and that subject device is physically connected to the port, and the switch port links up when the port is activated, and that port security is enabled and the MAC address for the server is configured on that switch port.

Checks

NET SW Sticky Process

Review the procedures in place and ensure a written process is in place.

Default Finding Sticky Connection Approval Process is not established.

Details

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

Fixes

NET SW Sticky Process

Establish Sticky connection procedures with the Change Control Process currently in place.

Notes:

NET1440

V0014736 CAT II

VMPS is used to provide port authentication

8500.2 IA Control: DCAS-1, DCSR-1, DCSR-2, DCSR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure VMPS must not be used to provide port authentication or dynamic VLAN assignment.

Vulnerability Discussion VMPS allows a switch to dynamically assign VLANs to users based on the workstation's MAC address or the user's identity when used with the User Registration Tool. A switch is configured and designated as the VMPS server while the remainder of the switches on the segment acts as VMPS clients. The VMPS server opens a UDP socket to communicate and listen to client requests using VMPS Query Protocol (VQP). When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping. If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port, the host receives an "access denied" response when VMPS is not configured in secure mode or the port is shut down if in secure mode.

VQP is a UDP-based protocol that does not support any form of authentication and the data is transmitted in clear text. This makes its use in security-sensitive environments inadvisable. An attacker who is able to spoof VQP could prevent network logins with a DoS attack to the VMPS server or even join an unauthorized VLAN. Furthermore, a VMPS database configuration file is nothing more than an ASCII text file that is stored on a TFTP server and downloaded to the VMPS server at startup or when VMPS server is first enabled on the switch. As noted in previous sections, a network component should not use TFTP to upload or download configuration files. For these reasons, VMPS must not be used to provide port authentication or dynamic VLAN assignment.

Checks

NET VMPS

Interview the Switch Administrator and verify VMPS statements are not found in the switch configuration.

Default Finding Details VMPS is used to provide port authentication or dynamic VLAN assignment.

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

Fixes

NET VMPS

Use an approved port security implementation.

Notes:

NET1621

V0014715 CAT II

Assets are not registered in VMS

8500.2 IA Control: VIVM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will properly register all network components in VMS.

Vulnerability Discussion Vulnerability Management is the process of ensuring all network assets that are affected by an IAVM notice are addressed and corrected within a time period specified in the IAVM notice. VMS will notify Commands, Services, and Agencies of new and potential security vulnerabilities. VMS meets the DoD mandate to ensure information system vulnerability alert notifications are received and acted on by all system administrators. Keeping the inventory of assets current allows for tracking of network inventory and resources. Asset management supports a successful IAVM process. The ability to track assets improves the effective use of network assets, information assurance auditing efforts, as well as optimizing incident response times.

Checks

NET Registration

Procedure: Ensure that all IA management review items are tracked and reported.

Default Finding Assets are not registered in VMS.

Details

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

Fixes

NET Registration

Register all network assets in VMS.

Notes:

NET1622

V0014716 CAT II

Device management is not using a OOB network.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure an OOB management network is in place for MAC I systems or 24x7 personnel have immediate console access (direct connection method) for communication device management.

Vulnerability Discussion From an architectural point of view, providing Out-Of-Band (OOB) management of network systems is the best first step in any management strategy. No production traffic resides on an out-of-band network. The biggest advantage to implementation of an OOB network is providing support and maintenance to the network that has become degraded or compromised. During an outage or degradation period the inband management link may not be available. The consequences of loss of availability of a MAC I system is unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures. Maintenance support for key IT assets must be available to respond 24 X 7 immediately upon failure.

Checks

NET OOB Management

View each aux port and ensure the auxiliary port is disabled or if enabled determine if a secure modem is implemented to support the DCN network. Review the console port configuration and determine if an OOB network has been defined at this interface using a Terminal Server (illustrated in the STIG). If neither a DCN or Terminal Server OOB network has been built, verify the administration staff is 24x7 and personel have immediate access to the console port locally via an administrative laptop.

Default Finding Details Device management is not using a OOB network.

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

Fixes

NET OOB Management

The network administrator will manage devices through out-of-band or direct connection. If the direct connection method is impractical, the DCN method is the next best alternative.

Notes:

NET1628 V0008059 CAT II Unsecured Modems are connected to console or Aux

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure modems are not connected to the console port.

Vulnerability Discussion Access to the router via a modem is potentially very risky. If an intruder were to gain access to the router via a modem, the potential for denial of service attacks, interception of sensitive information, and other destructive actions is greatly increased.

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.

Checks

NET Modems on Mgt Ports

Physically inspect any local routers to ensure modems are not connected or meet the standards defined in the Network STIG.

Default Finding Details Unsecured modems are connected to console or auxiliary port.

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

Fixes

NET Modems on MGT Ports

The router administrator will ensure that modems connected to the router are disconnected or secured modems providing encryption and authentication are installed.

Notes:

NET1635 V0008096 CAT II Use of in-band management is not limited.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The network administrator will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

Vulnerability Discussion It is imperative that communications used for administrative access to network components is limited to emergency situations or where out-of-band management would hinder daily operational requirements. In-band management introduces the risk of an attacker gaining access to the network internally or even externally.

Checks

NET Inband Mgt not Limited

Interview the IAO/NSO for compliance. Ask to see documentation.

Default Finding Details Use of in-band management is not limited.

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

Fixes

NET In-band Mgt not Limited

Use out-of-band management.

Notes:

NET1670

V0008092 CAT III

SNMP SOP Procedures are not documented

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:

- Community string and username expiration period
- SNMP community string and username distribution including determination of membership

Vulnerability Discussion Without a SOP to manage the SNMP community strings, the chance that these strings will be used to gain access to network managed devices is increased. If an attacker gains access to network devices, denial of service, interception of sensitive information, or other destructive actions could take place.

Checks

NET SNMP SOP

Interview the IAO/NSO to ensure a documented SOP is in place for the management of SNMP community strings and usernames.

Default Finding Details The NSO has not developed an SOP management of SNMP community strings and/or the procedure is developed but has not addressed the following information:

SNMP string expiration
SNMP string compromise
SNMP string creation

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

Fixes

NET SNMP SOP

The NSO will ensure that procedures are included in the documented SOP for the network to manage SNMP community strings. At a minimum, these procedures will include SNMP string expiration, SNMP string compromise, and SNMP string creation.

Notes:

NET1730 **V0008093** **CAT II** **The NMS is not located in a secure environment.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the management workstation is located in a secure environment.

Vulnerability Discussion Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that the NMS be located in a secure area that allows access to authorized personnel only. If unauthorized users gain access to the NMS, they could change device configurations, cause network disruptions, or create denial of service conditions.

Checks

NET NMS Location

Inspect the location of the network management workstations.

Default Finding Details The NMS is not located in a secure environment approved for secret level processing

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

Fixes

NET NMS Location

The NOC will ensure that the NMS is located in a secure environment approved for at least secret level processing.

Notes:

NET1740 **V0008094** **CAT II** **NMS accounts are not properly maintained.**

8500.2 IA Control: ECSC-1, IAAC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that only those accounts necessary for the operation of the system and for access logging are maintained.

Vulnerability Discussion Without proper account maintenance, unauthorized users could gain access to the NMS. If unauthorized users gain access to the NMS through an invalid account they could change device configurations or cause denial of service conditions.

Checks

NET NMS Accounts

Review the configuration of the NMS with the IAO/NSO to verify that proper account administration is being enforced. Review the accounts and the personnel using them to verify that they require access.

Default Finding Details The following NMS accounts exist that are not needed for the operation of the system or for access logging:

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

Fixes

NET NMS Accounts

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

Notes:

NET1802 **V0014737 CAT II** **Gateway VPN is not terminated outside firewall.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure gateway-to-gateway VPNs are terminated outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).

Vulnerability Discussion Allowing a gateway VPN to bypass the firewall opens a remote network and all it's devices to enter the enclave without firewall screening.

Checks

NET GatewayVPN placement

Review the network architecture and ensure the VPN does not terminate inside the firewall.

Default Finding Details Gateway VPN is not terminated outside firewall.

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

Fixes

NET GatewayVPN placement

Move VPN connectivity outside the firewall filtering.

Notes:

NET1810 **V0008274 CAT III** **Site has not maintained oversight of enclave.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure that the site retains administrative oversight and control privileges on the IPSEC/VPN device within their security enclave if access is granted to the local network.

Vulnerability Discussion Without administrative oversight and control privileges on the VPN device, the site would have no way of verifying the security controls placed on the device.

Checks

NET VPN Enclave Oversight

Interview the IAM to determine compliancy.

Default Finding Details The site has not maintained administrative oversight and control privileges on the VPN device placed inside the enclave.

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

Fixes

NET VPN Enclave Oversight

When an agreement to establish a VPN with an outside security enclave/domain, retain administrative oversight and control privileges in the IPSEC/VPN device that is within your security enclave.

Notes:

NET1815 V0012101 CAT II REL LAN environments are not documented in SSAA

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure REL LAN environments are documented in the SSAA.

Vulnerability The IAM will ensure REL LAN environments are documented in the SSAA.

Discussion

Checks

NET REL SSAA documentation

GRE tunnels found on a premise or edge SIPRNet router that have an endpoint within the REL IP address space must be documented in the SSAA.

Default Finding GRE tunnels found on a premise or edge SIPRNet router that have an endpoint within the REL IP address space must be documented in the SSAA.

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

Fixes

NET REL SSAA documentation

Have the IAM document GRE tunnels defined on a premise or edge SIPRNet router that have an endpoint within the REL IP address space.

Notes:

NET1816 V0012102 CAT II Annual reviews are not being performed on REL LAN

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure annual reviews are performed on REL LAN environments.

Vulnerability If a REL LAN environment is present the IAM will ensure REL LAN reviews are performed annually.

Discussion

Checks

NET REL annual review

Have the IAM disclose documentaion that an annual REL LAN review has been performed annually.

Default Finding REL LAN environment is not being reviewed annually.

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

Fixes

NET REL annual review

The IAM will document REL LAN reviews being performed annually.

Notes:

NET1820 V0008275 CAT II IDS does not monitor all the VPN traffic.

8500.2 IA Control: EBVC-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will require the customer to provide a Host Based IDS capability for any gateway-to-host VPN established that bypasses the site's current IDS capability.

Vulnerability Discussion When the site enters into an agreement to allow a connection to bypass the sites IDS capability, the site needs to have a mechanism for detecting attacks or anomalies that transverse that connection.

Checks

NET VPN IDS

Review the network topology diagram to determine compliance.

Default Finding Details The site has not required the customer to provide IDS capabilities for the VPN implementation that bypasses the current site IDS capabilities.

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

Fixes

NET VPN IDS

Have the customer provide IDS capabilities for the VPN implementation.

Notes:

NET1822 V0014738 CAT II Unapproved non-C2 traffic exists.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability Tunneling of non-C2 must be accepted by the Classified Data Service Manager (DISA/GS21) via request expressing the requirement with supporting rationale and must be IAW CJCSI 6211.02B, DISN policy.

Vulnerability Discussion If tunneling of non-C2 is required, contact the Classified Data Service Manager (DISA/GS21) to express the requirements with supporting rationale. If the DISN solution proposed by the DISN Service Manager is accepted, and cryptography is employed (generally Type 1) for data protection, then DISN security criteria in accordance with reference CJCSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes, 31 July 2003 will be presumed to have been satisfied. If the non-DISN solution is in place for more than 365 days the site must comply with the GIG Waiver Policy, reference DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002.

Checks

NET Unapproved non-C2 traffic

Review the network architecture and ensure non-C2 traffic is not tunneled on the NIPRNet without waivers.

Default Finding Details Unapproved non-C2 traffic exists.

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

Fixes

NET Unapproved non-C2 traffic

Use the SIPRNet or follow policies for temporary tunneling.

Notes:

NET1823

V0014739 CAT II

Approved non-C2 traffic exceeds approved dates

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If the non-C2 solution will be in place for more than 365 days, then the SIPRNet must be used or the IAO be in receipt of GIG Waiver Policy, DoDD 8100.1 .

Vulnerability Discussion If tunneling of non-C2 is required, contact the Classified Data Service Manager (DISA/GS21) to express the requirements with supporting rationale. If the DISN solution proposed by the DISN Service Manager is accepted, and cryptography is employed (generally Type 1) for data protection, then DISN security criteria in accordance with reference CJCSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes, 31 July 2003 will be presumed to have been satisfied. If the non-DISN solution is in place for more than 365 days the site must comply with the GIG Waiver Policy, reference DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002.

Checks

NET non-C2 traffic exceeds app

Review the non-C2 waiver and determine expiration of the waiver.

Default Finding Details Approved non-C2 traffic exceeds approved dates .

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

Fixes

NET non-C2 traffic exceeds app

Use the SIPRNet.

Notes:

NET1824

V0014740 CAT I

non-C2 traffic exists on a ISP

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If non-C2 traffic is being tunneled on a commercial ISP it must be approved by the OSD GIG Waiver Panel and the IAO be in receipt of GIG Waiver Policy, DoDD 8100.1 .

Vulnerability Discussion If tunneling of non-C2 is required, contact the Classified Data Service Manager (DISA/GS21) to express the requirements with supporting rationale. If the DISN solution proposed by the DISN Service Manager is accepted, and cryptography is employed (generally Type 1) for data protection, then DISN security criteria in accordance with reference CJCSI 6211.02B, Defense Information System Network (DISN): Policy, Responsibilities and Processes, 31 July 2003 will be presumed to have been satisfied. If the non-DISN solution is in place for more than 365 days the site must comply with the GIG Waiver Policy, reference DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002.

Checks

non-C2 traffic exists on a ISP

Review the non-C2 waiver and determine if waiver documents approval of a ISP.

Default Finding Details non-C2 traffic exists on a ISP

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

Fixes

non-C2 traffic exists on a ISP

Use the SIPRNet.

Notes:

NET1826 **V0014741 CAT I** **Classified circuit terminates in non-DoD facility**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability Leasing of point-to-point circuits that extend classified backside connectivity to any non-DoD, foreign or contractor facility is prohibited unless the termination is government operated in the contractor or foreign government facility.

Vulnerability Discussion Leasing of point-to-point circuits that extend classified backside circuits to non-DoD, foreign or contractor facilities is prohibited unless the termination is government operated in the contractor or foreign government facility.

Checks

NET Classified circuit termina

Review the network and ensure classified circuits are secured in a DOD facility.

Default Finding Details Classified circuit terminates in non-DoD facility.

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

Fixes

NET Classified circuit termina

Terminate all classified networks found in non-DOD facilities that are not government operated.

Notes:

NET1827 **V0014742 CAT II** **SIPRNet exceptions must be documented**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/O/NSO will have all C2 and non-C2 exceptions of SIPRNet use documented in the enclave's accreditation package and an Interim Authority to Connect/Authority to Connect (IATC/ATC) amending the connection approval received, prior to implementation.

Vulnerability Discussion Any exception to use SIPRNet must be documented in an update to the enclave's accreditation package and an Interim Authority to Connect/Authority to Connect (IATC/ATC) amending the connection approval received prior to implementation.

Checks

NET SIPRNet exceptions doc

Review accreditation package and an Interim Authority to Connect/Authority to Connect (IATC/ATC) amending the connection approval received.

Default Finding Details SIPRNet exceptions must be documented.

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

Fixes

NET SIPRNet exceptions doc

Document all SIPRNet connections.

Notes:

NET1829 **V0014743** **CAT II** **non-DISN C2 solution must use type-1 encryption**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If the non-DISN C2 solution proposed by the DISN Service Manager is accepted, Type 1 cryptography will be employed for data protection.

Vulnerability Discussion If the need for classified tunneling across NIPRNet or a commercial IP infrastructure is not C2 related, then on a "case by case" basis such tunneling may be considered. The use of a commercial IP service must be approved by the OSD GIG Waiver Panel. Requirements can be referenced in DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002.

Checks

NET non-DISN C2 - Type 1

Review the approved commercial circuit and ensure type 1 encryption has been implemented.

Default Finding Details Non-DISN C2 solution must use type-1 encryption.

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

Fixes

NET non-DISN C2 - Type 1

Add approved type 1 encryption devices.

Notes:

NET1830 **V0014744** **CAT II** **No controls over the type of data to being moved.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure the controls over the type of data to be moved are described in classification guidance, Executive Orders, or other issuances pertaining to controls over categories of information.

Vulnerability Discussion Controls over the type of data to be moved are described in classification guidance, Executive Orders, or other issuances pertaining to controls over categories of information.

Checks

NET no controls over data

Interview the IAO and determine if in compliance.

Default Finding Details No controls over the type of data to being moved.

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

Fixes

NET no controls over data

The IAO will ensure orders support the level of data traffic on the link are documented.

Notes:

NET1832 **V0014745** **CAT II** **Demarcation point is not authorized for SIPRNet**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure the tunnel demarcation is located in facilities authorized to process classified US government information, classified at the Secret Level (for SIPRNet).

Vulnerability Discussion Tunnel terminus or demarcation point will be in facilities authorized to process classified US government information classified at the Secret level (for SIPRNet).

Checks

NET Demarcation point

Review the demarcation point and verify the area meets the security level required.

Default Finding Details Demarcation point is not authorized for SIPRNet.

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

Fixes

NET Demarcation point

Facility demarcation point must meet approved security level.

Notes:

NET1833 **V0014746** **CAT I** **C2 traffic is not located on the SIPRNet**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability If C2 traffic is being tunneled on the NIPRNet, the IAM will have a plan of action and milestones detailing the effort to move the traffic to the SIPRNet.

Vulnerability Discussion The role of SIPRNet is to support C2 requirements. The network is designed to achieve a high availability to support that use. NIPRNet structure may not have the same availability. Therefore, the DISN DAA's, to meet operationally urgent conditions, and has specifically denied tunneling a C2 or related requirement across the NIPRNet infrastructure. In those circumstances efforts immediately begin to engineer and provision the more reliable SIPRNet transport to replace the temporary NIPRNet or even commercial infrastructure.

Checks

NET C2 traffic location

Review the SIPRNet LAN and ensure the C2 traffic leaving the enclave is on the SIPRNet.

Default Finding Details C2 traffic is not located on the SIPRNet.

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

Fixes

NET C2 traffic location

POA&M will be created to immediately remove the tunnel C2 traffic.

Notes:

NET1834

V0008091 CAT II

Remote Access VPN Gateway terminates behind FW

8500.2 IA Control: EBVC-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that VPN gateways terminate on or outside of the firewall.

Vulnerability The IAO/NSO will ensure Remote Access VPN gateways terminate on or outside of the firewall.

Discussion

Checks

NET VPN Termination

Review the network topology diagram and examine firewall rules to verify that there are no encrypted tunnels (i.e. IPSec) passing through the firewall.

Default Finding The VPN connection does not terminate at or outside of the firewall.

Details

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

Fixes

NET VPN Termination

Ensure that all VPN gateways terminate at or outside the firewall (e.g., between the premise router and the firewall, or connected to an outside interface of the router).

Notes:

NET1835

V0014747 CAT II

Remote Access VPN is using split-tunneling

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure remote access via VPN technology uses tunnel-all mode. Split-tunneling entering or leaving the enclave boundary is prohibited.

Vulnerability Discussion The VPN software on a host can be configured in either of two modes. It can be set to encrypt all IP traffic originating from that host, and send all of that traffic to the remote IP address of the network gateway. This configuration is called "tunnel-all" mode, because all IP traffic from the host must traverse the VPN tunnel to the remote system, where it will either be processed or further forwarded to additional IP addresses after decryption. Alternately, the VPN software can be set only to encrypt traffic that is specifically addressed to an IP at the other end of the VPN tunnel. All other IP traffic bypasses the VPN encryption and routing process, and is handled by the host as if the VPN relationship did not exist. This configuration is called "split-tunnel" mode, because the IP traffic from the host is split between encrypted packets sent across the VPN tunnel and unencrypted packets sent to all other external addresses.

There are security and operational implications in the decision of whether to use split-tunnel or tunnel-all mode. Placing a host in tunnel-all mode makes it appear to the rest of the world as a node on the connected logical (VPN-connected) network. It no longer has an identity to the outside world based on the local physical network. In tunnel-all mode, all traffic between the remote host and any other host can be subject to inspection and processing by the security policy devices of the remote VPN-linked network. This improves the security aspects of the connected network, since it can enforce all security policies on the VPN-connected computer.

Checks

NET VPN split tunnel

Interview the IAO and examine the configuration of a VPN client.

Default Finding Details Remote Access VPN is using split-tunneling

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

Fixes

NET VPN split tunnel

Implement tunnel-all mode.

Notes:

NET1836

V0014748 CAT III

VPN does not comply with JTF Best Practices

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure remote access via VPN technology complies with solutions in JTF-GNO Technical Bulletin 05-015 version 2, Virtual Private Networks (VPN) Implementation Best Practices, dated 19OCT2005.

Vulnerability Discussion The intent of the bulletin is to discuss issues involved in implementing Virtual Private Network (VPN) solutions, in particular the issue of ensuring that access controls at differing infrastructure levels/tiers do not adversely affect VPN solutions for traveling DoD personnel.

Checks

NET VPN best practices

Interview the IAO and examine / review the technical bulletin.

Default Finding Details Remote Access VPN does not comply with JTF Best Practices.

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

Fixes

NET VPN best practices

Follow the guidelines in the bulletin.

Notes:

NET1838

V0014749 CAT II

The VPN connection is using a weak SSL version

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that remote access VPNs using SSL protocol use the approved FIPS TLS protocol, also known as SSL 3.1.

Vulnerability Discussion The SSL protocol allows clients and HTTP servers to communicate over a secure connection. It offers encryption, source authentication, and data integrity as means to protect information exchanged over insecure, public networks. There are several versions of SSL:

- SSL
- TLS / SSL 3.1
- SSL Proxy Servers

SSL 2.0 has security weaknesses and is hardly used today; SSL 3.0 is universally supported; and finally the Transport Layer Security (TLS), which is an improvement on SSL 3.0, has been adopted as an Internet standard and is supported by most recent software implementations. The manner in which the SSL 1.0, 2.0, and 3.0 protocols use approved and non-approved cryptographic algorithms for its operation prohibits its usage.

Checks

NET VPN SSL 3.1

Interview the SA and verify client is using a secure protocol.

Default Finding Details The VPN connection is using a weak SSL version.

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

Fixes

NET VPN SSH 3.1

Ensure that remote access client is using a secure protocol.

Notes:

NET1839

V0014750 CAT II

Remote Access VPN does not authenticate user

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA0/NSO will ensure that Remote Access solution verifies user identity and restricts access to authorized users.

Vulnerability Discussion TLS also known as Secure Sockets Layer (SSL 3.1) enables "application layer" VPNs, which operate at layers four through seven of the OSI networking model, and can be used with or without a client. SSL-based VPNs initiate communication by utilizing the program layer between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL works by securing the HTTP protocol, encrypting the data streams transmitted by HTTP. SSL 3.1 provides a secure "wrapper" to the protect IP packets between the browser and the web server. SSL 3.1 uses a public and private key encryption system from RSA Security Inc., which also includes the use of a digital certificate.

There are some limitations with two-way authentication in SSL that are being addressed by recent developments in the use of TLS reverse proxy servers, commonly referred to as SSL Proxy Servers. Although the TLS proxy server method is well suited to protecting Web-based applications, it is unable to handle non-Web-based applications in the same manner. For detailed discussion on TLS proxy server implementation advantages and disadvantages refer to NIST Special publication 800-77.

Checks

NET VPN authentication

Interview the SA and verify compliance.

Default Finding Details Remote Access VPN does not authenticate users.

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

Fixes

NET VPN authentication

Ensure that remote access via VPN solution provides authentication.

Notes:

NET1840

V0008276 CAT III

VPN implemented using split-tunneling

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The SA and the IAO/NSO will ensure that if VPN technology is used to connect to a DoD network, the VPN client and concentrator are configured to deny the use of split tunneling when the connection originates from outside of the protected enclave.

Vulnerability Discussion To provide the maximum level of security for both the DoD network and the remote corporate enterprise, the contractor will have to exceed the normal protection deployed on DoD workstations. This connection is established as an exclusive connection between the VPN client and the VPN network device; all other connectivity is blocked after establishment of the VPN session, so there is no chance of IP packets being forwarded between the contractor company and the DoD network.

Checks

NET VPN Contractor

Interview the IAO/NSO and examine the configuration of a VPN client. Interview the IAO/NSO to verify compliance. Interview the IAO/NSO to verify compliance.

Default Finding Details The contractor computer was not secured IAW the appropriate operating system STIG.

The site doesn't maintain administrative oversight and control privileges of the computers.

The contractor computer did not employ a FIPS-140-2 approved encryption algorithm.

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

Fixes

NET VPN Contractor

Ensure the contractor machine is secured with the appropriate STIG. Ensure the contractor machine is updated with the latest virus engine and signature files. Ensure the contractor machine employ a DoD-CERT approved firewall. Ensure the contractor machine employ, at a minimum, a FIPS-140-2 encryption algorithm.

Notes:

NET1844

V0014751 CAT III

RAS policies are not in place for contractors

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The remote user will enter into a written agreement with the DoD site that allows the site to maintain administrative oversight and control privileges of the computer.

Vulnerability Discussion To provide the maximum level of security for both the DoD network and the remote corporate enterprise, the contractor will have to exceed the normal protection deployed on DoD workstations.

Checks

NET VPN RAS policies

Ensure the site maintains administrative oversight and control privileges of the computers.

Default Finding Details RAS policies are not in place for contractors.

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

Fixes

NET VPN RAS policies

Define written agreements for contractors and begin maintaining administrative oversight and control privileges.

Notes:

NET1845

V0014752 CAT III

The RAS does not deploy encryption for contractors

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The remote user will ensure all communication to and from the site network employs security using an encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion To provide the maximum level of security for both the DoD network and the remote corporate enterprise, the contractor will have to exceed the normal protection deployed on DoD workstations. This connection is established as an exclusive connection between the VPN client and the VPN network device; all other connectivity is blocked after establishment of the VPN session, so there is no chance of IP packets being forwarded between the contractor company and the DoD network.

Checks

NET VPN RAS encryption

Interview the IAO and determine if the contractor VPN solutions are compliant.

Default Finding Details The RAS does not deploy encryption for contractors.

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

Fixes

NET VPN RAS encryption

Establish procedures, written agreements and begin taking oversight and administrative privileges for contractors.

Notes:

NET1850

V0014753 CAT II

Host-to-host VPNs must not bypass the perimeter

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure host-to-host VPNs do not bypass the enclave perimeter protections.

Vulnerability Discussion Two individual computer hosts can connect directly to each other with an encrypted connection. The most well known example of such a connection is a web client to web server connection using the secure https protocol (TLS/SSL). There are, however, other examples in widespread use, including secure shell (SSH) connections by clients to servers, remote access and remote management programs such as Timbuktu and PC Anywhere, and many others. The security implication of an encrypted host-to-host connection is that neither participating network has an opportunity to inspect the unencrypted traffic and process the traffic in the boundary security services.

Checks

NET VPN host-to-host

Review the network topology diagram, and review VPN concentrators. Determine if VPN solutions bypass the perimeter.

Default Finding Details Host-to-host VPNsbypass the perimeter.

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

Fixes

NET VPN host-to-host

Ensure that remote access via VPN terminates are the perimeter for traffic inspection.

Notes:

NET1908

V0015239 CAT I

IPv6 security policy does not mirror IPv4 policy

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability IAO/NSO will ensure in a dual stack environment the enclave IPv6 security policy mirrors the IPv4 security policy.

Vulnerability Discussion The similarities between IPv4 and IPv6-based threats lead to the conclusion that security measures developed and field proven for IPv4 should be used by IPv6. A first step in securing IPv6 deployments is to match IPv4 security policies with IPv6. Once this is accomplished begin implementing IPv6 specific policies for IPv6 vulnerabilities.

- 1) Address management should be implemented to prevent easily guessed trivial IP addresses.
- 2) Using static neighbors for key systems.
- 3) Stop traffic sourced from the internal addresses (ULA) from exiting the enclave. Filter ICMP, but allow operational functions such as PMTU discovery. Deny IPv6 fragments destined to network elements and drop fragments of packets where the upper layer can not be determined. Implement RFC 2847 to containing spoofing attacks. Block source address that is multicast address. The IPv4 firewalls and filters should block the ports used by tunneling mechanisms not deployed in the network.
- 4) Implement application security at the host and the network with the help of firewalls until IDS functionality becomes available.
- 5) Authenticate BGP and IS-IS routing protocols. Use IPSec for OSPFv3 and RIPng.
- 6) Dual Stack deployments are easier to secure and should be preferred over tunneling. If tunneling is used, static tunnels are preferred over dynamic because they are more secure.

Checks

NET IPv6 Security Policy

Review the IPv4 security policy and verify the IPv6 security policy mirrors the IPv4 policy. Once this has been accomplished begin appending IPv6 specific security policies to mitigate specific IPv6 vulnerabilities.

Default Finding Details

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

Fixes

NET IPv6 Security Policy

Build the IPv6 security policy from IPv4, then begin adding IPv6 specific policies for the new threats inherited by IPv6.

Notes:

NET1937

V0015278 CAT II

IDS is not implemented to inspect IPv6 traffic.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the tunnel between the internal router's ingress interface and the perimeter router's egress interface is accessible to an IDS device capable of analyzing IPv6 in IPv4 traffic.

Vulnerability Discussion IDS/ IPS are currently not capable to handle the multiple levels of encapsulation that is required by the transition architectures.

The Department of Defense IPv6 Transition Office (DITO) made recommendations for the placement of firewalls, IDSs and IPSs within each of the transition architectures. The current capability of perimeter security devices does not include inspection necessary to dissect and analyze layers of tunnel encapsulation and other protocol headers supported by MO2 architectures. Therefore, it is necessary for perimeter security devices to be distributed at each encapsulation point in the network in order to accomplish the required inspection.

Checks

NET Security Zone IDS

Review the architecture and ensure an IDS inspects the traffic prior to being encapsulated. As technology advances IDS inspection may be capable of inspecting the tunneled IPv6 traffic.

Default Finding Details IDS is not implemented to inspect IPv6 traffic.

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

Fixes

NET Security Zone IDS

Ensure an IDS is in the architecture to inspect the traffic.

Notes:

NET1938

V0015280 CAT I

Firewall is not implemented to inspect IPv6

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the tunnel between the internal router's ingress interface and the perimeter router's egress interface is accessible to a firewall device capable of inspecting and filtering IPv6 in IPv4 traffic.

Vulnerability Discussion Currently, there is limited ability to proxy IPv6 connections on firewalls, the ability to do deep packet inspection is non-existent, and IDS/IPS are not able to handle the multiple levels of encapsulation that is required by the transition architectures.

The Department of Defense IPv6 Transition Office (DITO) made recommendations for the placement of firewalls, IDSs and IPSs within each of the transition architectures. The current capability of perimeter security devices does not include the deep packet inspection necessary to dissect and analyze layers of tunnel encapsulation and other protocol headers supported by MO2 architectures. Therefore, it is necessary for perimeter security devices to be distributed at each encapsulation point in the network in order to accomplish the required packet filtering.

Checks

NET Security Zone FW

Review the architecture and ensure a firewall inspects and filters the traffic prior to being encapsulated. As technology advances firewall inspection may be capable of the required packet filtering in the tunnel.

Default Finding Details Firewall is not implemented to inspect and filter IPv6 traffic.

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

Fixes

NET Security Zone FW

Ensure a firewall is in the architecture to inspect the traffic.

Notes:

NET1960

V0015290 CAT I

AG must not have Tunnel Broker solution

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure AG does not have Tunnel Broker solutions implemented for IPv6 transition

Vulnerability Discussion Tunnel brokers (TB) can be seen as virtual IPv6 ISPs, providing IPv6 connectivity to users already connected to the IPv4 Internet. In the emerging IPv6 Internet it is expected that many tunnel brokers will be available so that the user will just have to pick one. TB solutions do provide authentication via IPSec where ISATAP does not. At the time of this writing understanding the TB trust relationships being offered by ISP providers was of unknown, leading to a policy denying the use of TB at an AG boundary.

Checks

NET Tunnel Broker

Interview the IAO and router administrator to see if tunnel broker solutions have been implemented into the enclave. Below is an incomplete list of tunnel brokers.

AARNet
ACADEMIA Sinica Computing Centre
ECS Southampton
Hexago / Freenet6
SixXS
UKERNA
Wanadoo France

Ameri.ca
BT Exact
CERNET
Consulintel / Euro6IX
Dolphins / AS8758
Earthlink R&D
FCCN
Hurricane Electric
IJJ
MANIS
MyTBS
NECTEC
NGNet.It
Nerim
SCC
SingNet
Unix-Servers.de
XS26
XS4All

Default Finding AG must not have Tunnel Broker solutions implemented for IPv6 transition.

Details

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

Fixes

NET Tunnel Broker

Remove the tunnel broker from the enclave.

Notes:

NET1975

V0015291 CAT I

TCP-UDP Relay is implemented in the enclave

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure TCP-UDP Relay is not implemented in the enclave.

Vulnerability Discussion Malicious party may try to use Transport Relay Translator (TRT) systems to circumventing ingress filtering, or to achieve some other improper use. TRT systems should implement access control to prevent such improper usage. A careless TRT implementation may be subject to buffer overflow attack, but this kind of issue is implementation dependent. Use of DNS proxies that modify the resource records RRs will make it impossible for the resolver to verify DNSsec signatures. Refer to RFC 3142 for addition details.

Checks

NET TCP/UDP Relay

If IPv6 has been implemented perform the following check. TRT systems use transport layer (TCP/UDP) relay technique to translate IPv6 traffic to IPv4 traffic. TCP/UDP Relay requires at least one TRT relay server to be operated per site. TRT require mapping between DNS names to temporary IPv4 addresses, thus it requires a specially configured DNS server to run.. Normally users do not want to translate DNS query/reply traffic using the TRT system. Instead, it makes more sense to run standard DNS server, or special DNS server that helps TRT system, somewhere in the site IPv6 network. Interview the DNS Administrator to determine if TRT server has been implemented in the enclave and if so inquire on special DNS configurations to support the TCP/UDP Relay. Most vendors do not support this transition mechanism.

Default Finding Details TCP-UDP Relay must not be implemented in the enclave.

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

Fixes

NET TCP/UDP Relay

Disable TCP/UDP Relay in the enclave.

Notes:

NET1976

V0015292 CAT I

BIS must not be implemented in the enclave.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure Bump-in-the-Stack (BIS) is not implemented in the enclave.

Vulnerability Discussion The Bump in the Stack (BIS) [RFC2767] translation mechanism is similar to taking the NAT-PT approach with Stateless IP/ICMP Translator (SIIT) and moving it to the OS protocol stack within each host. Unlike SIIT however, it assumes an underlying IPv6 infrastructure. This algorithm translates, on a packet-by packet basis, the headers in the IP packet between IPv4 and IPv6, and translates the addresses in the headers between IPv4 and either IPv4-translated or IPv4-mapped IPv6 addresses. Whereas SIIT is a translation interface between IPv6 and IPv4 networks, BIS is a translation interface between IPv4 applications and the underlying IPv6 network (i.e. the network interface driver). The host stack design is based on that of a dual stack host, with the addition of 3 modules, a translator, an extension name resolver, and an address mapper.

The assignment is automatically carried out using DNS protocol, users do not need to know whether target hosts are IPv6. This allows them to communicate with other IPv6 hosts using existing IPv4 applications; thus it seems as if they were dual stack hosts with applications for both IPv4 and IPv6. So they can expand the territory of dual stack hosts.

The translator translates outgoing IPv4 headers into IPv6 headers and incoming IPv6 headers into IPv4 headers (if applicable). It uses the header translation algorithm defined in SIIT. The extension name resolver acts as the DNS-ALG in the NAT-PT mechanism. It snoops IPv4 DNS queries and creates another query asking to resolve both 'A' and 'AAAA' records, sending the returned 'A' record back to the requesting IPv4 application. If only 'AAAA' records are returned, the resolver requests the address mapper to assign an IPv4 address corresponding to the IPv6 address. The address mapper maintains a pool of IPv4 addresses and the associations between IPv4 and IPv6 addresses. The address mapper will also assign an address when the translator receives an IPv6 packet from the network for which there is no mapping entry for the source address.

Hosts can not utilize the security above network layer when they communicate with IPv6 hosts using IPv4 applications via the mechanism. The reason is that when the protocol data with which IP addresses are embedded is encrypted, or when the protocol data is encrypted using IP addresses as keys, it is impossible for the mechanism to translate the IPv4 data into IPv6 and vice versa. Therefore it is highly desirable to upgrade to the applications modified into IPv6 for utilizing the security at communication with IPv6 hosts.

Checks

NET Bump-in-the-Stack

Interview the DNS administrators to determine if BIS is being used.

Default Finding Bump-in-the-Stack (BIS) must not be implemented in the enclave.

Details

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

Fixes

NET Bump-in-the-Stack

Disable BIS in the enclave.

Notes:

NET1977

V0015297 CAT II

DSTM must not be implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure Dual Stack Transition Mechanism (DSTM) is not implemented in the enclave.

Vulnerability Discussion When DSTM is deployed in a network, an IPv4 address is allocated to a dual stack node if the connexion can not be established using IPv6. This allows either IPv6 nodes to communicate with IPv4-only nodes, or IPv4-only applications to run on an IPv6 node without modification. This allocation mechanism is coupled with the ability to perform IPv4-over-IPv6 (4over6) tunnelling, hiding IPv4 packets inside the native IPv6 domain. This simplifies network management: only the IPv6 routing plan is managed inside the network.

The DSTM architecture is composed of an address server (DSTM server), a gateway and a number of nodes (DSTM nodes). The address server is in charge of IPv4 address allocation to client nodes. This allocation is very simple since there is no localization purpose in this address. The DSTM server has just to guarantee the uniqueness of the IPv4 address for a period of time. The gateway, or Tunnel End Point (TEP), can be seen as a border router between the IPv6-only domain and an IPv4 internet or intranet. This node performs encapsulation/decapsulation of packets to assure bi-directional forwarding between both networks. Finally, in order to assure IPv4 connectivity, nodes in the IPv6-only domain should be able to dynamically configure their IPv4 stack (by asking the server for a temporary address) and must be capable to establish 4over6 tunnels towards a Tunnel End Point.

DSTM is an early stage IETF-Draft and is not approved technology in DoD.

Checks

NET DTSM

DTSM will not be found in the enclave due to being in IETF Draft. When implemented, a DTSM Server and a DTSM Gateway will reside in the enclave.

In the absence of an IPv4 routing infrastructure, a DSTM node can not directly send IPv4 packets on the network. It has to encapsulate them into IPv6 packets and send them to a Tunnel End Point (which can be seen as a particular DSTM node) that will decapsulate the packet and forward them into the IPv4 network. On a DSTM node, this encapsulation is done by a 4over6 interface. All IPv4 traffic can be directed to that interface by an IPv4 routing table entry.

When a DSTM Node needs to send an IPv4 packet, it is sent to the 4over6 interface. If the 4over6 interface is not configured (it does not have an IPv4 address), the process SHOULD be blocked and the DSTM Server should be contacted to get a temporary address. Once an address is allocated, it is used as the IPv4 source address for all the packets leaving the interface.

Default Finding Details Dual Stack Transition Mechanism (DSTM) must not be implemented.

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

Fixes

NET DTSM

Not applicable at the time of this writing.

Notes:

NET1979

V0015298 CAT I

SOCKS-Based Gateway must not be implemented.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure SOCKS-Based Gateway is not implemented in the enclave.

Vulnerability Discussion The SOCKS-based IPv6/IPv4 gateway mechanism is for communication between IPv4-only and IPv6-only hosts. It consists of additional functionality in both the end system (client) and the dual-stack gateway (router) to permit a communications environment that relays two terminated IPv4 and IPv6 connections at the application layer. This mechanism is based on the SOCKSv5 protocol, and inherits all the features of that protocol. Existing SOCKSv5 commands are unchanged, and the protocol maintains the end-to-end security between the client and the gateway, and the gateway and the destination. The mechanism uses a feature called DNS Name Resolving Delegation to determine IPv6 addresses, delegating the name resolving to the gateway, thus requiring no change to existing DNSs.

Since the SOCKS-based IPv6/IPv4 gateway mechanism is based on SOCKSv5 protocol, the security feature of the mechanism matches that of SOCKSv5. The mechanism is based on relaying two "terminated" connections at the "application layer". The end-to-end security is maintained at each of the relayed connections (i.e., between Client C and Gateway G, and between Gateway G and Destination D). The mechanism does not provide total end-to-end security relay between the original source (Client C) and the final destination (Destination D).

The security of such application layer traversal is highly dependent on the particular authentication and encapsulation methods provided in a particular implementation, and selected during negotiation between SOCKS client and SOCKS server. The SOCKS service is located on TCP port 1080. Port 1080 has not been reviewed by the PPS CAL at the time of this writing. RFC 1928 and RFC 3089 describe SocksV5 and SOCKS-based IPv6/IPv4 Gateway Mechanism respectively.

Checks

NET SOCKS-Based Gateway

The SOCKS-based gateway mechanism requests socksification of applications (install *Socks Lib*) to accomplish heterogeneous communications. It is not necessary to modify (change source codes and recompile them, etc.) the applications, because typical socksification is done by changing the linking order of dynamic link libraries (specifically, by linking the SOCKS dynamic link library before the dynamic link libraries for normal socket and DNS name resolving APIs). The mechanism does not request modification of the DNS system, because the DNS name resolving procedure at the Client C is delegated to the dual stack node Gateway G (review vulnerability discussion). Review the firewall can help determine if the Socks port is open. Interview the IAO, DNS administrator, and Firewall Administrator to determine if a SOCKS-based Gateway is present in the enclave if port 1080 is open.

Default Finding SOCKS-Based Gateway must not be implemented in the enclave.
Details

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

Fixes

NET SOCKS-Based Gateway

Disable the SOCKS-based Gateway in the enclave.

Notes:

NET1993

V0015299 CAT II

Only one Transition Mechanisms can be implemented

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

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

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

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

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

Checks

NET NAT-PT Transition

Interview the IAO, Network Administrator and the DNS Administrator and determine if additional transition mechanisms are implemented in the enclave.

Default Finding Details No other IPv6 Transition Mechanisms can be implemented when supporting NAT-PT.

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

Fixes

NET NAT-PT Transition

Disable all but one transition mechanism.

Notes: