NETWORK INFRASTRUCTURE

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 6, Release 3

5 July 2005

Developed by DISA for the DOD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

Page

APPENDICES

TABLE OF FIGURES

LIST OF TABLES

This page is intentionally left blank.

SUMMARY OF CHANGES

General Changes:

The previous release was Version 5, Release 2, dated 29 September 2003.

Section Changes:

SECTION 1 – INTRODUCTION

Updated with template.

SECTION 2 – ENCLAVE ARCHITECTURE OVERVIEW

No changes.

SECTION 3 – NETWORK INFRASTRUCTURE

3.1 External Connections

NET0135 - Changed the audit to become more specific. A review on semi-annual basis is now required.

NET0140 – Split PDI into two individual checks creating NET0141.

NET0150 – Deleted, Redundant check. NET0130 accomplishes the requirement.

3.1.2 AG/ISP Connections

NET0162 - Added AG ingress ACL requirement to only permit packets with a destination address belonging to the site's address block.

NET0164 - Ensure there is no routing protocol session with a peer router belonging to an AS (Autonomous System) of the AG service provider.

NET0166 - Restricting AG network service provider IP addresses so they are not redistributed into or advertised to the NIPRNet.

NET0175 – Changed requirement to be allowed if approved by DAA.

3.2.1 IANA Reserved Addresses

Added URL references: www.iana.org/assignments/ipv4-address-space and http://www.iana.org/.

NET0186- Added requirement, prevent all BOGON / Martian, and private IP addresses from traversing the IP WAN. The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.

3.2.3 DHCP

NET0195 – Deleted due to lack of vulnerability and it is common practice.
(NET0195: CAT II) *The NSO will ensure that all routers, firewalls, servers, administrator workstations, printers, and all other communications devices are assigned static IP addresses to the fullest extent possible.*

NET0198 – Modified requirement to include retention period.
Stored online for 30 days and offsite for one year.

NET0199 – Modified for clarity objective.

3.3 General Standards for Communications Devices

NET0200 - Removed requirement for maintaining listing of MAC addresses for all workstations.

3.3.1 Passwords

NET0240 – Modified to remove backdoor accounts do to unachievable objective.

NET0260 – Modified to reference current Instruction 8500.2. Outdated Appendix C removed.

3.3.2 Device Management

NET0290 – Deleted. Do to conflicts with other STIGs this PDI was removed. The image file can be loaded from a console (i.e., XMODEM) or via the FTP or SCP—not TFTP. The IAO/NSO will ensure that if FTP or SCP is being used, connectivity between devices and the FTP or SCP server is secured. At a minimum, this will be accomplished by restricting communication to known authorized IP addresses.

3.3.2.1 Out-of-band(OOB) Management

NET310 – Modified for clarity.

Referred Router and Switch review to *Section 3.4.3* and *3.7.3* respectively.

3.3.2.2 In-band Management

Referred Router and Switch review to *Section 3.4.3* and *3.7.3* respectively.

NET0324 - Modified requirement verbiage to become more specific to the environment.
The number of IP addresses must be equal to or less than the number of network administrators

NET0326 – Modified to meet appropriate guidance. "… or IAW FIPS 140-2 validated encryption."

3.3.3 Warning Banners

NET0340 – Modified to meet appropriate guidance. "… access in accordance with DODI 8500.2 Enclosure C, Appendix C." Outdated Appendix C of this document was removed.

3.4.1 Route Table Integrity

NET0400 – Modified for clarity.

NET0420 – Modified requirement to specify keys need to be changed every six months and changed the category code to CAT II.

NET0425 - Require the lifetime of a MD5 Key expiration is set to never expire.

3.4.2 Router Accounts and Passwords

NET0560 – Combined with NET0600.

NET0620 – Deleted, determined PDI was not capable of reviewing.
(NET0620: CAT II) *The router administrator will never set the SNMP community string or username, RADIUS or TACAC+ keys, or FTP username or password to any other password.*

3.4.3.1 OOB Router Management

NET0630 – Modified PDI for OOB criteria.

NET0640 – Originally NET0310, to cover OoB in its entirety for routers in this section.

NET0650 – Modified timeout requirements from 15 minutes to 10 minutes on console port.

NET0652 – Originally NET0640.

NET0655 – Originally NET0630.

3.4.3.2 In-Band Router Management

NET0664 –Originally NET0320 to cover in-band in its entirety for routers in this section.

NET0681 – New PDI requiring Secure Shell timeout of 60 seconds reducing the broken telnet session.

NET0682 – New PDI restricting Secure Shell invalid logon attempts to 3.

NET0685 – Modified timeout requirements from 15 minutes to 10 minutes on vty ports.

3.4.4 Securing Router Services and Features

NET0705 – Deleted. It has been determined there is not a vulnerability in leaving router interfaces in an up/down status.

NET0710 – Modified requirement to restrict on external interfaces only.

NET0722 – Require PAD services to be disabled.

NET0724 – Require TCP Keep-alives to be enabled.

NET0726 – Require Identification support be disabled.

NET0728 – Require DHCP service to be disabled.

NET0781 – Require Gratuitous ARP to be disabled.

NET0790 – Modified to specify all interfaces.

NET0800 – Modified for clarity by assigning ownership.

NET0811 – Require NTP Servers provide services for internal clients only.

NET0812 – Require NTP clients to peer with local NTP servers.

Modified for clarity. (NET… 0710, 0720, 0730, 0740, 0750, 0760, 0770, 0780, 0820)

NET0892 – Renamed from NET0900.

NET0894 – Renamed from NET0925.

NET0900 – Previously NET0830, has been deleted. The Deny-by-Default policy has been changed to remove the requirement from premise/edge router.

NET0910 – Renamed from NET0840.

NET0920 – Renamed from NET0845 and modified for clarity.

3.4.5.2 Exploits Protection

NET0960 – Modified PDI and included information and method to block the later version of traceroute IAW RFC1913.

Rate limiting TCP SYN packets with JUNOS can be performed by including rate limiting on the ingress firewall filter assigned to external facing interfaces. Rate limiting can be configured to limit the amount of bandwidth consumed as well as the maximum burst size of the TCP SYN traffic.

NET0965 – Require TCP wait time interval and Rate limiting on CISCO and JUNOS respectively to prevent TCP SYN Flood Attack.

NET0966 – Require CISCO Express Forwarding (CEF) on all CISCO routers to help router perform better when under SYN Flood Attack.

NET0980 – Modified, new requirement denies ICMP destination unreachable inbound to support the Ports and Protocols category of being a Red Service.

NET0990 – Modified to allow ICMP type 3, code 4, packet fragmentation.

3.4.5.3 Logging

NET1020 – Renamed from NET0850.
NET1021 – Renamed from NET0860.
NET1025 – Renamed from NET1120.
NET1027 – Renamed from NET1130.
NET1028 – Renamed from NET1150.

3.4.6 Router Configuration Management

Added clarification for secured alternative methods for uploading and downloading router configurations and images.

Discussion on PCMCIA flash memory cards, and Secure Copy Protocol (SCP).

3.5.1 Firewall Architecture

Updated drawing.

NET1170 - NIAP Category II lowered to Category III.

NET1190 – Modified PDI to reference application-level gateways or firewalls to proxy traffic.

Deleted NET1192. It duplicates NET1190 procedure.

NET1163 – Changed the requirement to an Enclave Perimeter Defense check

3.5.2 Firewall Placement

NET1200 – Modified PDI for clarity.

3.5.3 Identification & Authentication

NET1228 – Modified PDI for clarity.

3.5.4 Configuration

NET1254 – Modified PDI for clarity.

Deleted NET1262 and NET1270.

3.5.5 Auditing and Administration

NET1316 – Modified PDI for clarity, "… encryption via SSH, SSL or IAW FIPS 140-2 validated encryption."

3.6 Network Intrusion Detection (NID)\Real Secure

Added guidance indicating Host Intrusion Detection (HID) is not required on an OS-based NID.

NET1325 / NET1326 – Split the PDI (originally NET0100) into two PDIs.

NET1327 – Renamed from NET0110.
NET1328 – Renamed from NET0120.
NET1330 - The Network IDS requirement lowered to a CATII.
NET1342 – Modified PDI for clarity.
NET1350 – Modified PDI for clarity.

3.7 Switches and VLANs

3.7.1 Horizontal Wiring IDF

Collapsed Data Outlets and Switch & Intelligent Hub section, renaming it to "Switches and VLANs." Expanded section significantly.

Deleted (NET1360: CAT II) The IAO/NSO will ensure that all LAN outlets not in use are detached in the communications closet and the switch port is disabled.

NET1362 – Require Switch equipment to be in a secured area.

3.7.2 Switch Accounts and Passwords

NET1364 – Require an Authentication Server for Switch equipment.

NET1365 – Only one Local Account can be defined on the Switch.

NET1366 – Require users to have their own account and password to the Switch.

NET1367 – Ensure the lowest security level is assigned to the userids.

NET1368 – Expired Switch user's logons are removed from the Authentication Server.
NET1369 – Require type 5 encryption on passwords to the Switch.

NET1370 – Deleted. Split NET1370 into 6 PDIs (1364, 1365, 1366, 1367, 1368, 1370).

3.7.3 Switch Administrative Access

NET1380 – Require passwords on all OOB switch connections.

NET1381 – Ensure Switch console port times out after 10 minutes.

NET1382 – Ensure modems are not connected to console or auxiliary ports.

NET1383 – Ensure the Switch's Auxiliary port is disabled.

NET1385 – Require passwords on all Switch In-band ports.

NET1386 – Require Switch In-band to be performed on only authorized IP addresses.

NET1387 – Require SSH for all In-band Switch connections.

NET1388 – Require the Switch SSH timeout value is set at 60 seconds or less.

NET1389 – Limit the amount of unsuccessful logons to the Switch to three or less.

NET1390 – Set the timeout value on the Switch console port to 10 minutes or less.

NET1391 – Log all In-band Management attempts.

3.7.4.1 Management VLAN and VLAN1

NET1410 – Previously Net1375. Split PDI into two PDIs. Rewrote for clarity.

NET1411 – Previously Net1375. Split PDI into two PDIs. Rewrote for clarity.

NET1412 – Renamed from 1376 and modified PDI for clarity.

NET1413 – Renamed from 1377 and modified PDI for clarity.

3.7.4.2 VLAN Trunking

NET1416 – Renamed from 1378. Split PDI into three PDIs. Rewrote for clarity.

NET1417 – Renamed from 1378. Split PDI into three PDIs. Rewrote for clarity.

NET1418 – Renamed from 1378. Split PDI into three PDIs. Rewrote for clarity.

3.7.4.3 VLAN Access Port Authentication

NET1435 – Renamed from 1379 and modified PDI for clarity.

NET1436 – Port Security or 802.1x Authentication must be used.

NET1437 – If Port security is used, require static MAC addresses to be coded.

NET1438 – If Port Authentication is used require ports to come up in an unauthorized state.

NET1439 – If Port Authentication is used require re-authentication every 60 minutes.

SECTION 4 –REMOTE ACCESS

4.1 VLAN Access Port Authentication

NET1440 – Renamed PDI from NET1380 and modified PDI for clarity.

NET1441 – Renamed PDI from NET1400 and modified PDI for clarity.

NET1446 – Renamed PDI from NET1415 and modified PDI for clarity.

4.2 Remote Access Agreement

NET1410 – Deleted PDI.

4.3 Authentication, Authorization, and Accounting (AAA)

Deleted following PDIs (NET … 1418, 1435, 1438).

NET1451 – Renamed PDI from NET1420.

NET1452 – Renamed PDI from NET1425.

NET1453 – Renamed PDI from NET1430.

NET1455 – Renamed PDI from NET1436.

NET1456 – Renamed PDI from NET1420 and changed requirement from daily to weekly.

4.4.1 Modems

NET1470 – Modified PDI as conditional if backup services are not used.

4.4.2 Remote Access Server/Network Access Server

NET1530 – Modified PDI for clarity and changed requirements.

NET1540 – Deleted.

NET1550 – Deleted.

NET1590 – Deleted.

NET1606 – Modified PDI to meet more current standards.

4.5 Remote Client to VPN Gateway

NET1620 – Deleted.

NET1635 – Deleted.

5.1.2 Network Management Security Implications

NET1665 – Split NET1665 into two PDIs (NET1665 & NET1666). Modified to meet current standards.

NET1670 – Modified PDI for clarity.

NET1635 – Deleted.

5.1.3 Network Management Station

NET1762 – Modified PDI to meet current standards.

5.2.1 Site to Site VPN

NET1800 – Modified PDI for clarity.

5.2.2 Contractor to Company Site VPN

NET1840 – Modified PDI, adjusting requirements.

APPENDIX C – REQUIRED FILTERING RULES

Modified. All ports and protocols are following the new policy documented as 8551.1.

The DOD Instruction 8551.1 is now real, dated, published, and available at http://www.dtic.mil/whs/directives/corres/html/85511.htm.

1. INTRODUCTION

A core mission for the Defense Information Systems Agency (DISA) Field Security Operations (FSO) is to aide in securing Department of Defense (DOD) Networks. The processes and procedures outlined in this Security Technical Information Guide (STIG), when applied, will decrease the vulnerability of DOD sensitive information. Network Security is clearly still one of the biggest concerns for our DOD customers (i.e., the warfighter).

The intent of this STIG is to include security considerations at the network level needed to provide an acceptable level of risk for information as it is transmitted throughout an enclave.

1.1 Background

The Network Infrastructure Security Technical Implementation Guide has been developed to enhance the confidentiality, integrity, and availability of sensitive DOD Automated Information Systems (AISs).

Each site network/communications infrastructure must provide secure, available, and reliable data for all customers. This document is designed to supplement the security guidance provided by DOD-specific requirements. This document will assist sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure network operations.

It should be noted that FSO support for the STIGs, Checklists, and Tools is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that “all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines” and tasks DISA to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.” This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

1.3 Scope

The requirements set forth in this document will assist Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), Network Security Officers (NSOs), and System Administrators (SAs) in support of protecting DOD network infrastructures.

The requirements in this document will be employed at the boundary between DOD private LANs and all WAN connections such as the Un-classified (but Sensitive) Internet Protocol Routing Network (NIPRNet), and Secret Internet Protocol Router Network (SIPRNet). The document will also assist in identifying external security exposures created when the site is connected to at least one Information System (IS) outside the site's control.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**," indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is http://iase.disa.mil/.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank.

2. ENCLAVE ARCHITECTURE OVERVIEW

Enclave perimeter security mechanisms are employed at the boundary between a DOD private LAN and a WAN (e.g., Internet, NIPRNet, SIPRNet). These connections are discussed in this document as LAN to WAN connections.

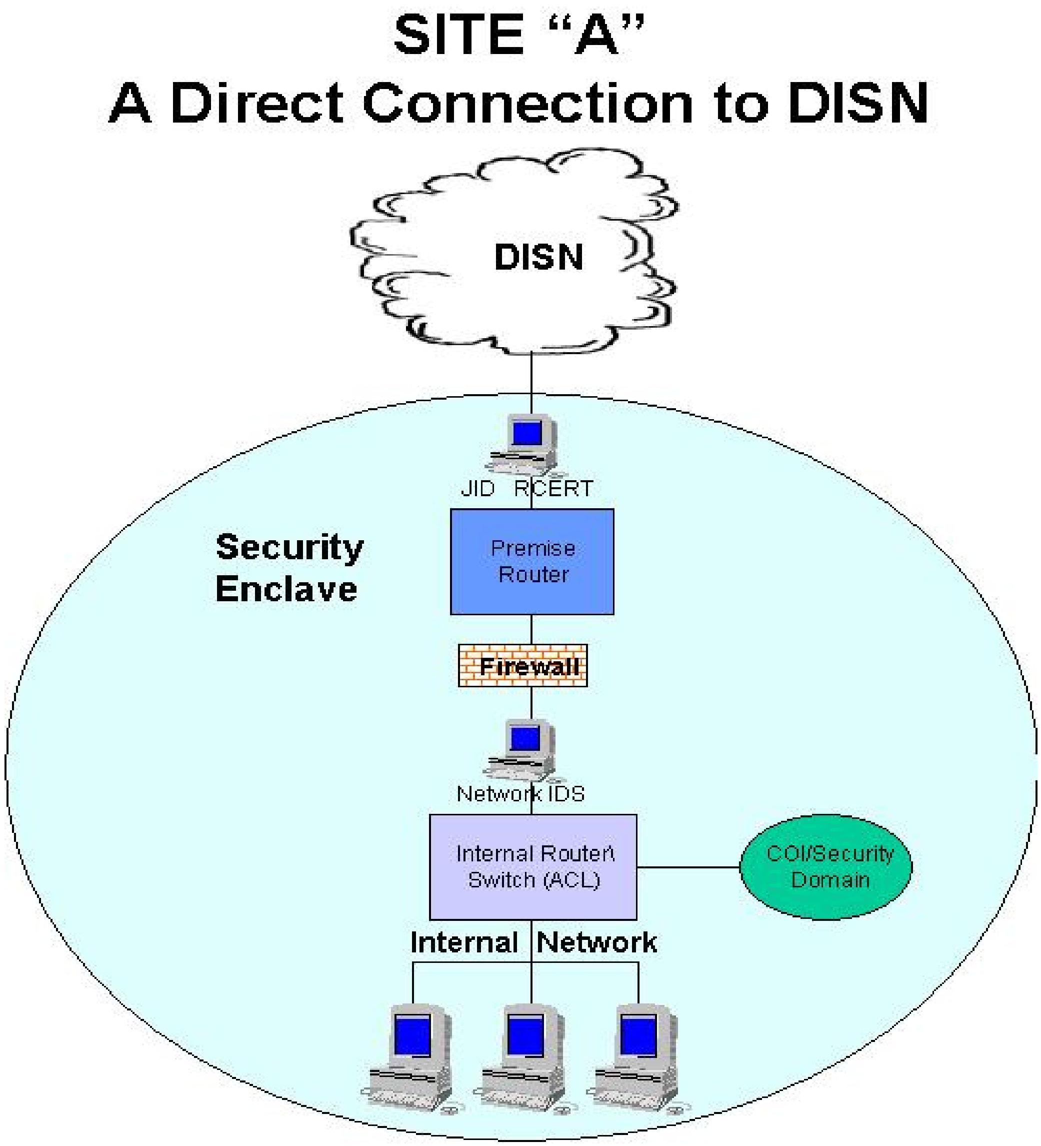

Figure 2-1. Enclave Architecture Overview -Site A

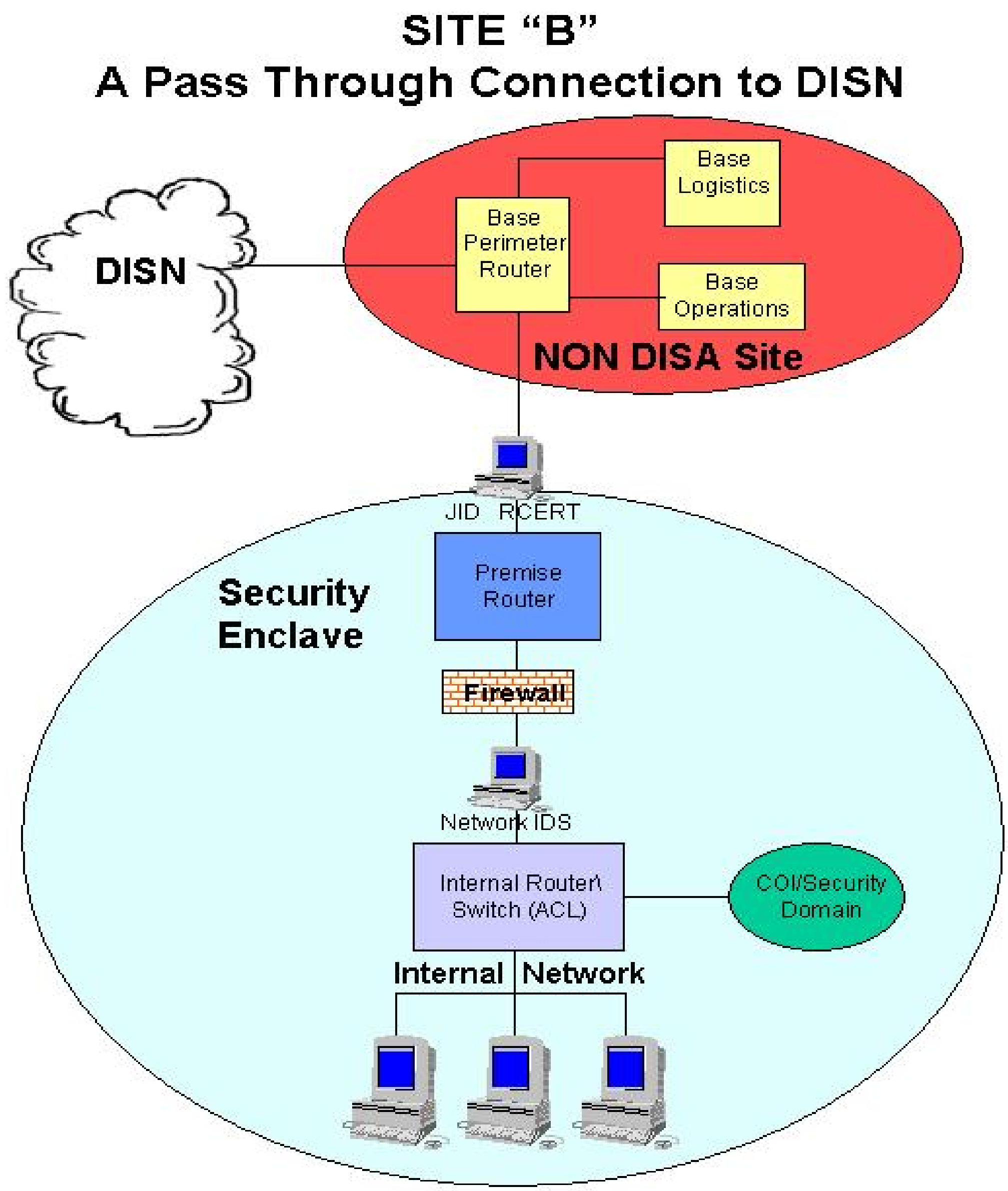

Figure 2-2. Enclave Architecture Overview -Site B

2.1 Enclave Protection Mechanisms

Enclave protection mechanisms are also used to provide security within specific security domains. In general, enclave protection mechanisms are installed as part of an Intranet used to connect networks that have similar security requirements and have a common security domain. A site may have multiple security domains with protection mechanisms tailored to the security requirements of specific customers. There might also be technology-driven security domains for OS/390, Unisys, Tandem, etc. Smaller locations may have a single enclave with a single security domain supporting the entire organization. The enclave or system owner will identify security domain requirements in the System Security Authorization Agreement (SSAA). Procedures outlined in the *DOD Instruction 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97,* 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.

STIGs and the review process provide the specifications, standards, and inspections for each of the key enclave components. In order to comply with the enclave architecture the minimum requirements include the following devices or systems:

- External Network Intrusion Detection System (IDS), anomaly detection, or prevention device if required by the Computer Network Defense Service Provider (CNDSP)
- Router Security with Access Control Lists
- Firewall and application level proxies (May be separate device to proxy applications.)
- Internal Network Intrusion Detection (NID) system
- DMZ, if applicable for publicly accessible services
- Split Domain Name Service (DNS) architecture
- Secure devices and operating systems (i.e., STIG compliant)

The only approved variance to the enclave architecture would be a site that adheres to the Deny by Default rule, does not require access into the Enclave to any user services, or host publicly accessible data (e.g., web servers, ftp servers, etc.). Therefore, the requirement for a DMZ and Split-DNS would not apply to these sites. This does not negate the need for DNS services; therefore, if the site utilizes an internal DNS server it must be configured in accordance with (IAW) the Domain Name System (DNS) STIG, otherwise the use of host files to handle the internal resolution may be an acceptable solution. Either solution would require the utilization of a primary or secondary DNS server, hosted on the NIPRNet, for all external resolution.

This page is intentionally left blank.

3. NETWORK INFRASTRUCTURE

Without current and accurate documentation, any changes to the network infrastructure may jeopardize the network's integrity. To assist in the management, auditing, and security of the network, 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.

- *(NET0090: CAT II) 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.*

3.1 External Connections

Connecting to external networks is one of the most complex areas of designing, implementing, and managing a network. An external network can be the NIPRNet or SIPRNet, as well as a network belonging to another DOD activity, a contractor site, or even the Internet. An external network is connected to the site's internal network via an external connection that can include but is not limited to a dedicated circuit (i.e., DISN Data Services), dial-on-demand Integrated Services Digital Network (ISDN), or an Ethernet upstream link to a neighboring service or activity's network on the same base.

Regardless of technology used, each external connection to the site's internal network must be secured such that it does not introduce any risk to the network. Every site should have a security policy to address filtering of the traffic from those connections. This documentation along with diagrams of the network topology are required to be submitted to the Connection Approval Process (CAP) for approval to connect to the NIPRNet or SIPRNet. Depending on the command, service, or activity, additional approval may be required. SIPRNet connections must also comply with the documentation provided to the SIPRNet Connection Approval Office (SCAO) to receive the SIPRNet Interim Approval to Connect (IATC) or final Approval to Connect (ATC) or as documented in the Interim Authority to Operate (IATO) or Authority to Operate (ATO) signed by the Designated Approving Authority (DAA).

Prior to establishing a connection with another activity, the site's policy will require that a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) 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. A connection to a trusted DOD activity must be treated the same as a connection to the NIPRNet. The security posture of a network is only as good as its weakest link.

- *(NET0130: CAT III) The IAO/NSO will ensure that all external connections are validated and approved prior to connection.*

- *(NET0135: CAT II) 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.*

NOTE: Unjustified and unapproved connections will be disconnected and reported to the IAM.

3.1.1 Leased / Dedicated Lines

DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore unauthorized access must be restricted. Security guidelines concerning leased/dedicated circuits are as follows:

- (*NET0140: CAT III) 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.*

- *(NET0141: CAT III) 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.*

3.1.2 Approved Gateway/Internet Service Provider Connections

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. NIPRNet enclave connections to contractor or non-DOD federal agency networks must be approved by the OSD. Henceforth, an Approved Gateway (AG) is any external connection from a DOD NIPRNet enclave to an ISP, or network owned by a contractor, or non-DOD federal agency that has been approved.

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

The premise router will not use a routing protocol to advertise NIPRNet addresses to the AG. Most ISPs use Border Gateway Protocol (BGP) to share route information with other autonomous systems (AS)—that is, any network under a different administrative control and policy than that of the local site. If BGP is configured on the premise router, no BGP neighbors will be defined as peer routers from an AS belonging to any AG. The only method to be used to reach the AG will be through a static default route. It would also not be feasible to implement Message Digest version5 (MD5) authentication with any BGP neighbors belonging to an AG. Thus, this restriction will ensure that routing information shared by the BGP peers across the NIPRNet will not be corrupted through route updates sent from untrusted routers. Furthermore, by not redistributing NIPRNet routes into the AG, unsolicited traffic that may inadvertently attempt to enter the NIPRNet by traversing the enclave's premise router will be avoided.

- *(NET0160: CAT I) 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.*

- *(NET0162: CAT I) The IAO/NSO will ensure premise router interfaces that connect to an AG (i.e., ISP) are configured with an ingress ACL that only permits packets with destination addresses within the site's address space.*

- *(NET0164: CAT I) The IAO/NSO will ensure the premise router does not have a routing protocol session with a peer router belonging to an AS (Autonomous System) of the AG service provider.*

- *(NET0166: CAT III) The IAO/NSO will ensure the AG network service provider IP addresses are not redistributed into or advertised to the NIPRNet.*

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

3.1.3 Backdoor Connections

The term "backdoor connection" is used to refer to a connection between two customer sites that does not traverse the provider's network (RFC 2764) –in this case, the provider network would be the NIPRNet or SIPRNet. 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 vise 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.

An even greater risk would be a backdoor connection established between two sites' internal routers or layer-3 switches. In this case, the traffic between the two sites is bypassing the perimeter that has been established for each network. 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. This unprotected connection could also be to the Internet, NIPRNet, SIPRNet, or any other DOD or contractor network.

- *(NET0170: CAT II) 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.*

3.2 Network Layer Addressing

IPv6 is the next generation network layer protocol for the Internet as well as the GIG including the NIPRNet and SIPRNet. Implementation of IPv6 is necessary due to the fundamental constraints of IPv4 that render it incapable of meeting long-term requirements of both the commercial community and the DOD. 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, and among business partners in the commercial sector. Henceforth, as of the memo from the ASD (NII) dated June 9, 2003, IPv4 will continue to be the mandated internetworking protocol for DOD. In addition, all references in this document relating to addressing, address blocks, subnets, prefixing, multicasting, and broadcasting will be exclusively within the IPv4 framework.

The first part of an IP address identifies the network on which the host resides, while the second part identifies the particular host on the given network. This creates the two-level addressing hierarchy—subnetting supports a three-level hierarchy. The network-number field has been referred to as the "network-prefix" because the leading portion of each IP address identifies the network number. All hosts on a given network share the same network-prefix but must have a unique host-number.

The DOD Network Information Center (NIC) assigns blocks of network addressees, to local administrators. The local network administrator then assigns individual IP addresses to hosts, servers, printers, and workstations on their LAN.

- *(NET0175: CAT I) The IAO/NSO will ensure that IPv6 implemented on any DOD network that transports production or operations traffic is approved by the DAA.*

3.2.1 Internet Assigned Numbers Authority Reserved Addresses

In the past, it has been typical to assign globally unique addresses to all hosts that use IP. In order to extend the life of the IPv4 address space, address registries are requiring more justification than ever before, making it harder for organizations to acquire additional address space blocks. It is the intent of RFC 1918 to promote a strategy that will provide constraint relief to the available globally unique address space that is rapidly diminishing.

Sites may incorporate the use of private network addresses into the site's NIPRNet architecture using the address spaces defined in this section. A site that uses any of these private addresses can do so without any coordination with Internet Assigned Numbers Authority (IANA) or the NIC. Since these addresses are never injected into the global NIPRNet, SIPRNet, or Internet routing system, the address space can simultaneously be used by every organization.

As documented in RFC 1918 the IANA has reserved the following three blocks of the IP address space that can be used for private networks:

10.0.0.0	- 10.255.255.255	(10/8 prefix)	Class A
172.16.0.0	- 172.31.255.255	(172.16/12 prefix)	Class B
192.168.0.0	- 192.168.255.255	(192.168/16 prefix)	Class C

In addition to the private IP addresses mentioned, all sites need to be aware that IANA has also reserved blocks of IP addresses listed in Appendix C, and the appropriate ACLs need to be applied to filter this traffic. BOGON or Martian addresses are unassigned/reserved by the IANA. The IANA may assign or reserve IP address blocks at any time. It is important to keep the list current in order to limit the impact to the routing or blocking of legitimate IP address spaces. These BOGON / Martian addresses, and the addresses defined by RFC1918 are networks that should never be seen on the IP WAN. The most current IANA listing can be found on the http://www.iana.org web site. The appropriate ACLs need to be applied to filter this traffic.

- *(NET0180: CAT II) The IAO/NSO will ensure all network IP address ranges are properly registered with the .MIL Network Information Center (NIC).*

- *(NET0185: CAT II) The IAO/NSO will ensure that all addresses used within the site's SIPRNet infrastructure are authorized .mil addresses that have been registered and assigned to the activity. RFC1918 addresses are not permitted.*

- *(NET0186: CAT III) The Router Administrator will block all BOGON / Martian, and private IP addresses from traversing the IP WAN. The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.*

3.2.2 Network Address Translation

Using the private addressing scheme in accordance with RFC 1918 will require an organization to also use Network Address Translation (NAT) for global access. Though NAT works well with the implementation of RFC 1918 addressing scheme, it also has the security benefit of hiding real internal addresses. A site's network address infrastructure should be considered proprietary information and should not be advertised. If potential attackers were able to map the network infrastructure by discovering real client addresses, they would be able to identify resources on the network to attack. The external IP address of the firewall or routable addresses from a NAT pool should be the only address visible to the public.

When NAT mapping is implemented, addresses will not bypass egress ACL filtering. A host that is translated must go through an ACL prior to being translated to the public address, or the host must go through a restrictive NAT ACL that only permits authorized hosts to be translated.

- *(NET0190: CAT III) The IAO/NSO will ensure that workstation clients' real addresses are not revealed to the public by implementing NAT on the firewall or the router.*

NOTE: If the site has implemented an application-level firewall, hiding of the clients' real address can also be done by enabling the proxies. Verify that the clients' real source address is replaced with that of the firewall's external IP. This check does not apply to SIPRNet enclaves.

The first scenario would be a site that has configured the firewall with one external IP address and has configured the internal network to use RFC 1918 addresses. It may work for a site that does not allow for external connections into the network, but is the least deployed configuration.

The second scenario would be a site that has multiple external IP addresses configured on the firewall, one primary for the site (workstations, printers, etc.), and the others redirected to individual servers. This is common with sites that host Web and FTP sites. The internal network is configured with the RFC 1918 addresses, including the Web or FTP server, but the server's IP address is mapped one to one with a different external IP.

The last scenario would be a system that requires that its real address be used. For these instances, the site will implement RFC 1918 addresses for the entire network with the exception of those hosts. The site will provide written justification for the exclusion of these hosts from the requirement.

In all of the situations above, the intent is to restrict the source and destination range to the smallest range possible. For servers that are open to the public, or an unmanageable subset of the public range (e.g., .mil, .gov, and .com), the site is configured similar to the second scenario, except the source address for these connections would be "any." If the .com users were only a few users, then restrict to .mil and .gov and configure the small amount of .com addresses. The destination IP should be restricted to a single IP, or in the case of a cluster or server "farm", it could be restricted to a subnet, yet would still implement port restriction.

3.2.3 Dynamic Host Configuration Protocol

With an increase in TCP/IP networks, the ability to assign IP client configurations automatically for a specific time period (called a lease period) has alleviated the time consuming process of IP address management. Network administrators can now automate and control from a central position the assignment of IP address configurations using the Dynamic Host Configuration Protocol (DHCP).

When connected to a network, every computer must be assigned a unique address. In the past, when adding a machine to a network, the assignment and configuration of network IP addresses has required administrator action. The user had to request an IP address, and then the administrator would manually configure the machine. Mistakes in the configuration process are easy to make, and can cause difficulties for both the administrator making the error, as well as users on the network. In order to simplify the process of adding machines to the network and assigning unique IP addresses manually, the site may decide to deploy DHCP.

If DHCP is used to allocate IP addresses for internal devices, a portion of the network IP addresses needs to be excluded or reserved from the DHCP scope for devices that require manual configuration of IP addresses (e.g., servers, routers, firewalls, and administrator workstations, etc.). The DHCP server is required, at a minimum, to log hostnames or MAC addresses for all clients. In order to trace, audit, and investigate suspicious activity, DHCP servers within the SIPRNet infrastructure must have the minimum duration of the lease time configured to 30 days or more.

- *(NET0198: CAT III) 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.*

- *(NET0199: CAT III) 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.*

3.3 General Standards for Communications Devices

The following subsections set security guidance applicable to all communications devices (e.g., routers, switches, firewalls, RAS, NAS, IDS, etc.). This guidance will be adhered to in addition to the requirements set forth in the individual sections that provide detailed security requirements for each device.

NOTE: For the purpose of this document, the term "remote" applies to anything other than direct console access, unless stated otherwise in the following section.

- *(NET0210: CAT II) 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.*

3.3.1 Passwords

- *(NET0230: CAT I) The IAO/NSO will ensure all communications devices are password protected.*

- *(NET0240: CAT I) The IAO/NSO will ensure all default manufacturer passwords are changed.*

- *(NET0260: CAT II) 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*

- *(NET0270: CAT II) The IAO/NSO will record the locally configured passwords used on communications devices and store them in a secured manner.*

3.3.2 Device Management

- *(NET0280: CAT III) The IAO/NSO will ensure that a documented procedure is in place to validate loaded image files image files loaded, and that they are checked on a monthly basis to ensure the file has not been corrupted or altered.*

- *(NET0300: CAT II) The IAO/NSO will disable all network management ports and services except those needed to support the operational commitments of the site.*

3.3.2.1 OOB Management

OOB management consists of accessing the communications device via a dial-up circuit, directly connected terminal device, or local area networks dedicated to managing traffic. With the dial-up method, a modem is attached to the console service port and the administrator connects via a standard phone line. This connection is relatively private, since connect times are random and the circuit is disconnected when not in use. The most secure OOB management method is directly connecting a computer or terminal to the service port. This precludes any intentional or accidental reception of information. *Section 3.4.3, Router Administration*, and *Section 3.7.3, Switch Administration*, covers and expands upon these requirements.

NOTE: Disregard this section for routers and switches.

- *(NET0310: CAT II) The IAO/NSO will ensure all communication. Device management utilizes the OOB or direct connection method for communications device management is used.*

- *(NET0310: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure OOB access enforces the following security restrictions:*

  - *Two-factor authentication (e.g., Secure ID, DOD PKI)*
  - *Encryption of management session (FIPS 140-2 validated encryption)*
  - *Auditing*

NOTE: Two-factor authentication discussion; reference *Section 3.4.3.1*.

3.3.2.2 In-band Management

In-band management is accomplished by establishing a (SSH) session with the device. This method is fast and convenient, but presents some security risks. Accessing the communications device in-band makes the session susceptible to all the monitoring and line sniffing vulnerabilities associated with a distributed LAN. For example, the login or privileged password could be intercepted, providing an attacker the capability to exploit a network device.

In-band management is only to be used in situations where OOB management will hinder operational commitments, and the IAO/NSO has approved, in writing, the use for that specific purpose. If remote access is used to connect to a network component for administrative access, the most stringent security controls will be implemented as specified in *Section 4.1, Levels of Remote Access*. *Section 3.4.3, Router Administration*, and *Section 3.7.3, Switch Administration*, covers and expands these requirements.

NOTE: Disregard this section for routers and switches.

- *(NET0320: CAT II) 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. The IAO/NSO will approve the use of in-band management on a case-by-case documented basis.*

- *(NET0322: CAT II) For in-band management, the IAO/NSO will implement the use of strong two-factor authentication for all access to all communications devices.*

NOTE: Two-factor authentication discussion; reference *Section 3.4.3.1*.

- *(NET0324: CAT II) The IAO/NSO will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses. The number of IP addresses must be equal to or less than the number of network administrator.*

- *(NET0326: CAT II) The IAO/NSO will ensure in-band management access to a network device is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

3.3.3 Warning Banners

- *(NET0340: CAT II) The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.*

3.4 Routers

3.4.1 Route Table Integrity

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

There are two approaches that can be used to safeguard the integrity of a route table: static routes and neighbor router authentication. For obvious reasons, defining static routes is the most secure method and is ideal for small stable networks. When using routing protocols to make route table updates due to changes in network topology and connection states, neighbor router authentication must be used to prevent fraudulent route updates from being received. Authentication occurs when routing updates are exchanged between neighbor routers; thereby, ensuring that a router receives routing information only from a trusted source. Neighbor router authentication is supported by all routing protocols except Routing Information Protocol (RIP) Version 1.

There are two types of neighbor router authentication that can be used: plain text authentication and MD5 authentication. The message digest is created using the key and a message, but the key itself is not sent, preventing it from being read while it is being transmitted. Plain text authentication sends the authenticating key itself over the network. All of the routing protocols support MD5 authentication except RIP Version 1 and Interior Gateway Routing Protocol (IGRP).

NOTE: MD5 for Intermediate System-to-Intermediate System (IS-IS) was introduced in Cisco IOS software version 12.2(13) T and is only supported on limited number platforms.

As with all secret keys and passwords, it is imperative that one closely guards the authentication keys used in neighbor router authentication. The security benefits of this feature are reliant upon keeping all authentication keys confident by using controlled methods for exchanging the keys as well as changing the keys on a regular basis.

NOTE: As of this writing, neighbor router authentication will not be required between the site's premise router and a NIPRNet or SIPRNet subscriber interface on the hub router.

- *(NET0400: CAT II) The router administrator will ensure neighbor authentication with MD5 is implemented for all routing protocols with all peer routers within the same or between autonomous systems (AS).*

- *(NET0410: CAT II) The router administrator will restrict BGP connections to known IP addresses of neighbor routers from a trusted AS.*

- *(NET0420: CAT II) The IAO/NSO will ensure there are written procedures for MD5 key management to include: key exchange, storage, and expiration. Keys will be changed every six months.*

- *(NET0425: CAT I) The IAO/NSO will ensure the lifetime of a MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.*

NOTE: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. This check is in place to ensure keys do not expire creating a DOS due to adjacencies being dropped and routes being aged out. The recommendation is to use two rotating six month keys with a third key set as infinite lifetime. The lifetime key should be changed 7 days after the rotating keys have expired and redefined.

3.4.2 Router Accounts and Passwords

Restricting access to all routers is critical in safeguarding the network. In order to control and authorize access, an authentication server that provides extended user authentication and authority levels will be implemented.

Individual user accounts with passwords will be set up and maintained in accordance with the guidance contained in DODI 8500.2, IAIA-1 and IAIA-2. There are two password protection types provided by Cisco Internetworking Operating System (IOS): Type 7 and Type 5. Type 7 uses the Cisco defined encryption algorithm, which is regarded as weak in the commercial security community. Type 7 encryption can be applied to the enable password, username, and line password commands using the service password-encryption command. Type 5 encryption, which uses a MD5, is considered a stronger mechanism and is used by the enable secret command.

Juniper routers do not have enable or privilege mode passwords, and there is no password prompt to enter edit mode. There is simply a one-time login to access the Command Line Interface (CLI). All privileges are based on the administrator’s account or the class the account belongs to. In addition, all passwords defined in JUNOS are always encrypted when the configuration is displayed.

Some vendors, particularly Juniper, have an additional management port known as a diagnostic port. These ports are for vendor use in troubleshooting when the site administrator requires assistance. It is required that these ports be secured.

- *(NET0430: CAT II) The IAO/NSO will ensure an authentication server is used to gain administrative access to all routers.*

- *(NET0440: CAT II) The IAO/NSO will ensure when an authentication server is used for administrative access to the router, only one account is defined locally on the router for use in an emergency (i.e., authentication server or connection to the server is down).*

- *(NET0460: CAT I) The router administrator will ensure each user has their own account to access the router with username and password.*

- *(NET0465: CAT II) The router administrator will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.*

- *(NET0470: CAT II) The router administrator will immediately remove accounts from the authentication server or router that are no longer required.*

- *(NET0580: CAT III) The router administrator will ensure a password is required to gain access to the router's diagnostics port.*

- *(NET0590: CAT III) The router administrator will ensure the enable secret password does not match any other username password, enable password, or any other enable secret password.*

- *(NET0600: CAT I) The router administrator will ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).*

3.4.3 Router Administrative Access

3.4.3.1 OOB Router Management

From an architectural point of view, providing OOB management of network systems is the best first step in any management strategy. No production traffic traverses an OOB network. Devices should have a direct local connection to such a network.

The console port will be configured to time out, so that if an administrator forgets to log out, the router will log the administrator out automatically. Users should never connect a modem to the auxiliary port as a backup or remote access method to the device.

Two-factor authentication is a security process that confirms user identities using two distinctive factors--something they have and something they know or something they are. By requiring two different forms of electronic identification, the risk of fraud can be reduced. Two-factor authentication does not rely exclusively on something known by a user, but it adds something that they must have. This added factor can be a physical device sometimes referred to as a token. Some two-factor options are smart-tokens, smart cards, and password generation tokens.

A password generation token device is usually a handheld device that is synchronized with an authentication server. The token device generates a password that the authentication server is expecting. This is a one-time password, also called a token. Token devices vary among vendors and are designed as synchronous or asynchronous. Synchronous token devices synchronize with authentication servers using time or events. If the synchronization is time based, the token device and server must have the exact time within their internal clocks. Asynchronous implementations use a challenge and response scheme to authenticate users.

There are two types of smart cards: memory cards and microprocessor cards. A memory card stores information and is read when inserted into a reader device. Memory cards are less expensive than microprocessor cards and rely on the card reader for securing the data on the card. Memory cards tend to be used in lower-security environments because of their inability to perform encryption algorithms. Microprocessor cards offer security independent of the reader device, making it ideal for high-security applications. With microprocessor cards, a user’s private key is securely stored within the smart card and never leaves the card. Using the onboard processor, all cryptographic functions, including digital signatures and decryption of session keys, occur inside the card.

Smart token technologically is similar to smart cards with the exception of the interface. Smart tokens are designed to interface with the Universal Serial Bus (USB) ports. Smart tokens are available in both memory and microprocessor variations also. A main advantage of smart tokens is they do not require a reader, tokens simply plug into USB ports commonly found on most modern computers.

- *(NET0630: CAT II) The IAO/NSO will ensure route management utilizes the OOB or direct connection method for communications device management.*

- *(NET0640: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure OOB access enforces the following security restrictions:*

    - *Two-factor authentication (e.g., Secure ID, DOD PKI)*
    - *Encryption of management session (FIPS 140-2 validated encryption)*
    - *Auditing*

- *(NET0645: CAT I) The IAO/NSO will ensure that all OOB management connections to the router require passwords.*

- *(NET0650: CAT II) The router administrator will ensure the router console port is configured to time out after 10 minutes or less of inactivity.*

- *(NET0652: CAT II) The IAO/NSO will ensure modems are not connected to the console or auxiliary ports.*

- *(NET0655: CAT III) The router administrator will ensure that the router's auxiliary port is disabled.*

3.4.3.2 In-band Router Management

In-band management administration with telnet is dangerous because anyone with a network sniffer and access to the right LAN segment can acquire the router account and password information. Security centers on protecting the paths and sessions used to access the device.

Access lists or filters must be used to limit which hosts may connect to the device using any in-band management application. Additionally, the IP addresses, will be restricted to administrators only and must originate from the internal network.

NOTE: In-band management is only to be used in situations where OOB management has been deemed to hinder operational commitments, and the IAO/NSO has approved in writing the use for that specific purpose.

- *(NET0664: CAT II) 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.*

- *(NET0665: CAT I) The IAO/NSO will ensure that all in-band management connections to the router require passwords.*

- *(NET0667: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure in-band access enforces the following security restrictions:*

- *Two-factor authentication (e.g., Secure ID, DOD PKI)*
- *Encryption of management session (FIPS 140-2 validated encryption)*
- *Auditing*
- *Two-factor authentication discussion; reference Section 3.4.3.1.*

- *(NET0670: CAT II) The router administrator will ensure that the router only allows in-band management sessions from authorized IP addresses from the internal network.*

- *(NET0680: CAT II) The router administrator will ensure in-band management access to the router is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(NET0681: CAT II) The router administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.*

- *(NET0682: CAT II) The router administrator will ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.*

- *(NET0685: CAT II) The router administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.*

- *(NET0690: CAT IV) The router administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*

3.4.4 Securing Router Services and Features

Ensuring each device on the network is as secure as possible dictates that the features and services activated need to be reviewed from a mindset of security. Simple security principles such as, "if you are not using it, do not turn it on," can be applied. The best security practice is to only support the services and protocols needed by the network to meet operational commitments. In most cases the industry recommends turning the service off, and as new operating systems are released they have become turned off by default. If a particular portion of a network needs a service but the rest does not, then the restriction features should be employed to limit the scope of the service.

Operating System

To guard against security weaknesses identified in older versions of the operating system, a current operating system is required.

- *(NET0700: CAT II) The router administrator will implement the latest stable operating system on each router IAW the current Network Infrastructure Security Checklist.*

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is used for some network management functions, but is dangerous in that it allows any system on a directly connected segment to learn that the router is a Cisco device, determine the model number and the Cisco IOS software version being run. This information may in turn be used to design attacks against the router. CDP information should be accessible only by directly connected systems.

- *(NET0710: CAT III) The router administrator will ensure CDP is disabled on all external interfaces on Cisco premise routers.*

Trivial Services

By default, Cisco devices up through IOS version 11.3 offer the "small services:" echo, chargen, and discard. These services, especially their UDP versions, are infrequently used for legitimate purposes, but can be used to launch denial of service and other attacks that would otherwise be prevented by packet filtering. For example, an attacker might send a DNS packet, falsifying the source address to be a DNS server that would otherwise be unreachable, and falsifying the source port to be the DNS service port (port 53). If such a packet were sent to UDP echo port, the result would be the router sending a DNS packet to the server in question. Outgoing access list checks would not be applied to this packet, since it would be considered locally generated by the router itself.

The small services are disabled by default in Cisco IOS 12.0 and later software. In earlier software versions, they may be disabled using the commands no service tcp-small-servers and no service udp-small-servers. In Juniper the defaults have them turned off.

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

Enabling TCP keep-alives on incoming connections can help guard against both malicious attacks and "orphaned" sessions caused by remote system crashes. Enabling the TCP keep-alives causes the router to generate periodic keepalive messages, letting it detect and drop broken Telnet connections.

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

By sending a large packet to the DHCP port, it is possible to freeze the router’s processing engine. DHCP service is enabled by default.

The "finger" service is used to find out which users are logged into a network device. “Finger” is a known security risk on the Internet, due to its divulgence of detailed information of people logged into a system. This is a “need to know” category and an attacker could use the information as a social engineering practice to elicit classified DOD information.

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

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

- *(NET0720: CAT III) The router administrator will ensure TCP & UDP small servers are disabled.*

- *(NET0722: CAT III) The router administrator will ensure PAD services are disabled.*

- *(NET0724: CAT III) The router administrator will ensure TCP Keep-Alives for Telnet Session are enabled.*

- *(NET0726: CAT III) The router administrator will ensure identification support is disabled.*

- *(NET0728: CAT III) The router administrator will ensure DHCP Services are disabled.*

- *(NET0730: CAT III) The router administrator will ensure Finger is disabled.*

- *(NET0740: CAT II) The router administrator will ensure HTTP, FTP, and all BSD r-command servers are disabled.*

Configuration and Image Integrity

Bootp is a UDP that can be used by routers to access copies of software on another router running the Bootp service. In this scenario, one router acts as a software server that can download the software to other routers acting as Bootp clients. In reality, this service is rarely used and can allow an attacker download capability to copy a router's software configuration.

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

- *(NET0750: CAT III) The router administrator will ensure Bootp server is disabled.*

- *(NET0760: CAT II) The router administrator will ensure configuration auto-loading is disabled.*

IP Source Routing

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

- *(NET0770: CAT II) The router administrator will ensure IP source routing is disabled.*

Proxy and Gratuitous ARPs

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

A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used to inform the network about a host's IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, affecting networking performance.

- *(NET0780: CAT II) The router administrator will ensure Proxy ARP is disabled.*

- *(NET0781: CAT II) The router administrator will ensure Gratuitous ARP is disabled.*

Directed Broadcasts

IP directed broadcasts are used in the extremely common and popular smurf, or Denial of Service (DoS), attacks. In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a subnet broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified.

IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the router connected directly to the target subnet can conclusively identify a directed broadcast. Consequently, directed broadcasts must be disabled on all router interfaces.

- *(NET0790: CAT III) The router administrator will ensure IP directed broadcast is disabled on all router interfaces.*

ICMP Exploits

The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. ICMP messages can be used by attackers for DoS attacks and network mapping. An attacker may also use ICMP to identify the operating system that a target system is running. Finally, an attacker may use ICMP to tunnel past perimeter security mechanisms to communicate with an internal host that has previously been compromised. ICMP can be used for a range of nefarious purposes. Network mapping and diagnosis attacks commonly use three ICMP messages: Host unreachable, Redirect, and Mask Reply.

An ICMP redirect message instructs an end node to use a specific router as its path to a particular destination. In a properly functioning IP network, a router will send redirects only to hosts on its local subnets, end nodes will not ever send a redirect, and not redirect will not traversed more than one network hop. However, an attacker may violate these rules; some attacks are based on this. Note that this filtering prevents only redirect attacks launched by remote attackers. It is still possible for attackers to cause significant trouble using redirects if their host is directly connected to the same segment as a host that is under attack.

The ICMP Address Mask Request and mask reply pair can be used to determine the subnet mask on the network allowing ease to network mapping information. When the requesting system issues the Address Mask Request bound for a destination, the destination system responds with an Address Mask Reply message. This condition can sometimes be a part of normal network traffic, but is uncommon on most networks. Suspicion should be aroused when a large number of these packets are found on the network.

Whenever a packet is dropped the router must send an ICMP unreachable packet back to the source. That is mandated by the Internet Standards. The unreachable message can be used to gain network-mapping information. To silently drop denied packets in hardware on the input interface, disable ICMP unreachables.

- *(NET0800: CAT II) The router administrator will ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.*

Logging Integrity - NTP

Accurately correlating information between devices becomes difficult, if not impossible without synchronized time. The ability to successfully compare logs between routers within a network, it will allow the administrator to determine the series of events that resulted in compromising a host or network.

An NTP client is configured to set its clock and stay synchronized with an NTP server. NTP clients can be configured to use multiple servers to set their time and are also able to set preference to the most accurate time sources. An NTP server is configured to synchronize NTP clients, and allow clients update or affect its time settings. NTP peers can provide time synchronization to each other.

Preferred NTP timeservers are provided by the U.S. Naval Observatory. The NIPRNet and SIPRNet accessible NTP servers are identified at http://tycho.usno.navy.mil/ntp.html.

Once a premise router is synchronized with a trusted external timeserver, that router is then capable of providing time synchronization for other NTP clients. Internal routers must be configured to use the premise router as their NTP server, thereby enabling all of the enclave's routers to be in synch. However, it is imperative that the premise router does not act as an NTP server for external clients and the internal clients are restricted by IP addresses.

- *(NET0810: CAT III) The IAO/NSO will ensure that two Network Time Protocol (NTP) servers are defined on the premise router to synchronize its time.*

- *(NET0811: CAT II) The IAO/NSO will ensure that the premise router is acting as an NTP server for only internal clients.*

- *(NET0812: CAT III) The IAO/NSO will ensure that all internal routers are configured to use the premise router to synchronize time.*

Connection Integrity

A router administrator can use a router to establish a Telnet connection with a destination router, switch, or other host using a host name. If the local router is configured as a name resolver and the host name is not in its host lookup table, it will attempt to query a DNS server if one is defined. If there is no DNS server defined, the router will broadcast the DNS query out to all interfaces. If the response to this query is the IP address of a host operated by an attacker, the local router will establish a connection with the attackers host, rather than the intended target.

- *(NET0820: CAT III) The IAO/NSO will ensure that the DNS servers are defined if the router is configured as a client resolver.*

SNMP Service

A router can be configured to act as a client for SNMP. When the SNMP service is enabled on a router, network management tools can use it to gather information about the router configuration, route table, traffic load, and more. SNMP will only be used on the internal network interfaces. SNMPv3 provides the most security, so it should be used if possible.

- *(NET0890: CAT II) The router administrator will restrict SNMP access to the router from only authorized internal IP addresses.*

- *(NET0892: CAT II) The router administrator will ensure SNMP is blocked at all external interfaces.*

- *(NET0894: CAT II) The router administrator will ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.*

3.4.5 Packet Filtering and Logging

Access lists are used to separate data traffic into that which it will route (permitted packets) and that which it will not route (denied packets). Secure configuration of routers makes use of access lists for restricting access to services on the router itself as well as for filtering traffic passing through the router.

Sites will implement router ingress and egress filtering based on a policy meeting security requirements documented in Appendix C and DOD Instruction 8551.1. All ports, protocols, and services (PPSs) required by the site for operational commitments and thus permitted by the ACLs will be configured in accordance with the guidelines contained in DOD Instruction 8551.1. http://www.dtic.mil/whs/directives/corres/html/85511.htm and Appendix C of this document.

The technical guidance lists three levels of blocking protocols at the enclave perimeter:

- Red Ports: Deny. No acceptable mitigation strategy and unacceptable high risk for routine use.

- Yellow Ports: Deny/Conditional/Allow. May have associated risk that can be mitigated to an acceptable level. Yellow is not acceptable under all conditions, but can be brought to an acceptable risk level if required mitigation strategy is implemented and approved by the DAA.

- Green: Deny/Conditional/Allow. May have associated risk that can be mitigated to an acceptable level and considered best security practice and advocated for use in future applications.

The site will enable logging on all statements used to deny any traffic. This feature will provide valuable information about what types of packets are being denied and can be used to enhance the sites intrusion detection capabilities.

- *(NET0910: CAT II) The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in DOD Instruction 8551.1 for all ports and protocols required for operational commitments.*

- *(NET0920: CAT II) The router administrator will bind the ingress ACL filtering packets entering the network to the external interface, and bind the egress ACL filtering packets leaving the network to the internal interface—both on an inbound direction.*

NOTE 1: If the router is in a Deny-by-Default posture, and what is allowed through the router filtering is IAW DOD Instruction 8551.1 and Appendix C, then all requirements related to PPS being blocked would be satisfied. The PPS would be covered under the Deny-by-Default rule as long as a permit rule was not created for them.

NOTE 2: When the site is in an allow-all posture, all filter statements need to be verified for compliance with DOD Instruction 8551.1 and Appendix C, and all PPS that are mandated to be blocked will have a rule created to block these ports.

3.4.5.1 IP Address Spoof Protection

Inbound Traffic

In Software Release 11.1, Cisco introduced the ability to assign inbound access lists to an interface. This allows a network administrator to filter packets before they enter the router instead of as they leave the router. Inbound access lists can be used to prevent some types of IP address spoofing, whereas outbound access lists alone will not provide sufficient security.

- *(NET0940: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network, any local host loop back address (127.0.0.0/8), the link-local IP address range (169.254.0.0/16), IANA unallocated addresses or any reserved private addresses in the source field.*

Outbound Traffic

Egress filtering rules will be applied denying all outbound traffic with an illegitimate address in the source address field. This is to prevent the network from being part of a Distributed Denial of Service (DDoS) attack.

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

- *(NET0950: CAT I) The router administrator will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Reverse Path Forwarding.*

3.4.5.2 Exploits Protection

SYN Flood Attack – Protecting the Network

The first packet in the TCP three-way handshake sets the SYN bit. When a host receives an initial SYN packet requesting a provided service, the host responds with a packet setting the

SYN and ACK bits, and waits for an ACK from the initiator of the connection request. If the initiator never responds to the host, the host will eventually time out the connection. However, while the host is still waiting for the ACK to complete the connection, the half-open connection consumes resources on the host—that is, entries in the connection table.
If there is an attack, the source address in these SYN packets is forged and probably unreachable. In most cases, the source address will either be an unregistered address or the address of a host the attacker knows does not exist. Therefore, the attacked host will never receive a response to its request to complete the initial three-way handshake and must wait to time out thousands of connections. During the wait, the server must ignore legitimate requests since its connection table is full.

In intercept mode, the router responds to the incoming SYN request on the server's behalf with a SYN-ACK and waits for an ACK from the client. If an ACK is received, the original SYN packet is sent to the server, and the router completes the three-way handshake with the server on behalf of the client and joins the two half-connections together transparently. In the case of illegitimate requests, the software's aggressive timeouts on half-open connections and its thresholds on TCP connection requests protect destination servers while still allowing valid requests.

In watch mode, the router allows the SYN requests through to the server. If the session fails to establish itself during a specified period of time, the router sends a reset (RST) to the server to clear the connection. The amount of time the router waits is configurable with the IP TCP intercept watch-timeout command.

By default, the software waits for 30 seconds for a watched connection to reach established state before sending a Reset. To optimize router resources, it is recommended to reduce this to 10 seconds using the following command:

```
ip tcp intercept watch-timeout 10
```

By default, the software still manages a connection for 24 hours after no activity. It is recommended to change this to 60 seconds using the following command:

```
ip tcp intercept connection-timeout 60
```

TCP intercept is available on all Cisco Routers with IOS Version 11.3 or greater. Most firewalls can also provide protection against SYN flood attacks using the similar concept of "proxying" or "watching" the connection until the three-way handshake is complete. SYN flood protection must be implemented on either the premise router or the firewall located on the sites' network perimeter. If the router will be providing the SYN flood protection using the TCP intercept software, it is the site's option to implement this feature in either intercept or watch mode.

JUNOS does not have a similar method to proxy or watch over TCP connection attempts. However, it does have rate limiting mechanisms that can be used to mitigate a SYN flood attack against a network or targeted hosts. Rate limiting TCP SYN packets with JUNOS can be performed by including rate limiting on the ingress firewall filter assigned to external facing interfaces. Rate limiting can be configured to limit the amount of bandwidth consumed as well as the maximum burst size of the TCP SYN traffic. A firewall counter could also be established to sample and count the number of SYN packets and the total number of TCP packets directed towards the network or servers to be protect. The counters can be viewed using a show firewall command. If a SYN flood is underway, the number of SYN packets will be very high (perhaps 50 percent or greater of the total TCP packets).

- *(NET0960: CAT II) The IAO/NSO will implement features provided by the router to protect servers from any TCP SYN flood attacks from an outside network.*

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

SYN Flood Attack – Protecting the Router

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

JUNOS does not have a similar method to control the SYN wait-time interval. However, it does have rate limiting mechanisms that can be used to mitigate a SYN flood attack and prevent a DoS on the routing engine. Rate limiting TCP SYN packets with JUNOS can be performed using either of the following two techniques:

1. Specify the number of allowable connection attempts per minute for each service (i.e., ssh, telnet, ftp) enabled on the router.

2. Create a firewall filter protecting the routing engine that rate limits TCP SYN traffic based on its bandwidth utilization and the maximum burst size.

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

Juniper's FPC (Flexible PIC Concentrator) architecture with the integrated Packet Forwarding Engine provides similar functionality and capabilities and is far superior than the traditional routing cache vulnerable to a DoS attack described above. The forwarding plane on all Juniper M and T Series platforms are built around this architecture and therefore is not configurable.

NOTE: Enabling CEF is required to utilize the Unicast RPF feature previously discussed.

- *(NET0965: CAT II) The router administrator will set the maximum wait interval for establishing a TCP connection request to the router to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.*

- *(NET0966: CAT II) The router administrator will enable CEF to improve router stability during a SYN flood attack to the network.*

ICMP Message Types and Traceroute

There are a variety of ICMP message types. Some are associated with programs (e.g., the ping program works with message types Echo Request and Echo Reply). Others are used for network management and are automatically generated and interpreted by network devices.

With Echo packets an attacker can create a map of the subnets and hosts behind the router. Also, an attacker can perform a denial of service attack by flooding the router or internal hosts with Echo packets. With ICMP Redirect packets, the attacker can cause changes to a host's routing tables. Otherwise, the other ICMP message types should be allowed inbound except message types Echo Request and Redirect.

- *(NET0980: CAT II) The router administrator will block all inbound ICMP messages with the exception of Echo Reply (type 0), and Time Exceeded (type 11). ICMP message number 3, code 4, are permitted inbound with the following exception: Must be denied from external AG addresses, otherwise permitted.*

For outbound ICMP traffic, the router administrator should allow the message types Echo Request, Parameter Problem, and Source Quench, and block all other message types unless needed for operational commitments. With Echo packets, users will be able to ping external hosts. Parameter Problem packets and Source Quench packets improve connections by informing about problems with packet headers and by slowing down traffic when it is necessary.

- *(NET0990: CAT II) The router administrator will block outbound ICMP traffic message types except Echo Request (type 8), Parameter Problem (type 12), and Source Quench (type 4) Destination Unreachable - Fragmentation Needed and Don't Fragment was Set (type3, code 4).*

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

The later version of traceroute initiates a traceroute with the originator sending a packet with a value of 82 in the IP Options field. Each router along the path will respond to the originator with an ICMP traceroute (type 30) message. The premise router will need to block any packets with a value of 82 in the IP Options field.

NOTE: All premise routers will be configured to ensure both methods are being blocked.

- *(NET1000: CAT III) The router administrator will block all inbound traceroutes to prevent network discovery by unauthorized users.*

Distributed Denial of Service (DDoS) Attacks

Several high-profile DDoS attacks have been observed on the Internet. While routers cannot prevent DDoS attacks in general, it is usually sound security practice to discourage the activities of specific DDoS agents (a.k.a., zombies) by adding access list rules that block their particular ports. Sites will utilize automated scanning for DDoS tools on all servers, routers, and other communications devices.

- *(NET1010: CAT I) The router administrator will block known DDoS attack ports in accordance with DOD Instruction 8551.1, Required Filtering Rules.*

The example below shows access list rules for blocking several popular DDoS attack tools.

TRINOO DDoS systems
```
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log
```

Back Orifice systemb
```
access-list 170 deny udp any any eq 31337 log
```

Stacheldraht DDoS system
```
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
```

TrinityV3 system

```
access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
```

T0rn rootkit system

```
access-list 170 deny tcp any any eq 47017 log
```

Subseven DDoS system and some variants

```
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

3.4.5.3 Logging

Logging is a key component of any security architecture and is a critical part of router security. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment. Maintaining an audit trail of system activity logs can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. A syslog server provides the network administrator the ability to send log messages from all of the communication devices on a network to a central host for examination and storage. Syslog levels 0-6 are the levels required to collect the necessary information to help in the recovery process.

Level	Level Name	Description	Example
0	Emergencies	Router becoming unusable	IOS could not load
1	Alerts	Immediate action needed	Temperature too high
2	Critical	Critical condition	Unable to allocate memory
3	Errors	Error condition	Invalid memory size
4	Warnings	Warning condition	Crypto operation failed
5	Notifications	Normal but important event	Interface changed state, up or down
6	Informational	Information message	Packet denied by access list
7	Debugging	Debug message	Appears only when debugging is enabled

Table 3-1. Logging

- *(NET1020: CAT III) The router administrator will ensure that all attempts to any port, protocol, or service that is denied are logged.*

- *(NET1021: CAT III) The router administrator will configure all routers to log severity levels 0 through 6 and send log data to a syslog server.*

- *(NET1025: CAT III) 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.*

- *(NET1027: CAT III) The syslog administrator will configure the syslog sever to collect syslog messages from levels 0 through 6.*

- *(NET1028: CAT III) The syslog administrator will configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).*

3.4.6 Router Configuration Management

3.4.6.1 Logistics for Configuration Loading and Maintenance

There are two basic approaches for configuration loading and maintenance—online editing and offline editing. Each has its advantages and disadvantages. Online editing provides for syntax checking but provides limited editing capability and no comments. Offline editing provides the ability to add comments, allows for the use of better editors, and guarantees all settings will be visible, but provides no syntax checking. It is important to keep the running configuration and the startup configuration synchronized, so that if there is a power failure or some other problem, the router will restart with the correct configuration. If there is a need for old or alternative configurations, they should be stored offline. In this situation, it is only necessary to manage the startup configuration since the running configuration is identical.

If passwords are in an offline configuration file, then they will be stored in the clear and transferred in the clear. Instead, it is best to type the passwords while online and then copy the encrypted strings to the offline configuration. This is especially true for the enable secret password. Obtain the encrypted string by setting the password manually on the router command line interface, then displaying the running configuration, and then copying and pasting the encrypted string into an offline configuration file.

With the configuration files offline, the files must be transferred to the router in a secure method—TFTP is not recommended. FTP is preferred over TFTP, provided that a username and password are required. Following are some alternative approaches that are actually more secure than using FTP:

1. If the router is equipped with PCMCIA Flash Memory Cards, copy images as well as configurations to these cards.

2. Copy and paste output of a displayed configuration 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 secure location.

NOTE: For Cisco IOS, defaults will not be included since most of the IOS defaults are not displayed on a show run command.

3. Secure Copy Protocol (SCP) - The JUNOS software can use SCP with the file copy operational mode command. Before enabling SCP on a Cisco router, one must correctly configure SSH, authentication, and authorization. SCP requires that authentication, authorization, and accounting (AAA) be configured in order for the router to 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 to and from a router by using the copy command.

- *(NET1030: CAT III) The router administrator, when saving and loading configurations will ensure that the running and startup configurations are synchronized.*

- *(NET1040: CAT IV) 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.*

- *(NET1050: CAT III) The IAO/NSO will ensure that on the system where the configuration files are stored, the router administrator uses the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).*

- *(NET1050: CAT III) The IAO/NSO will ensure only authorized router administrators are given access to the stored configuration files.*

- (*NET1060: CAT I) The router administrator will not store unencrypted router passwords in an offline configuration file.*

- *(NET1070: CAT II) The IAO/NSO will authorize and maintain justification for all TFTP implementations.*

- *(NET1071: CAT II) If TFTP implementation is used, the router administrator will ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.*

- *(NET1080: CAT II) The router administrator will ensure the FTP username and password are configured.*

3.4.6.2 Router Change Management

People and organizations are forever moving and changing work locations. Which may facilitate updates to router tables. The point of contact (POC) for each router is usually recorded with the domain registration authority for troubleshooting purposes. However, this can open up the change request process to possible spoofing. A person can impersonate the authorized POC and request updates that can deny or stop services altogether.

- *(NET1110: CAT II) The IAO/NSO will ensure all router changes and updates are documented in a manner suitable for review.*

- *(NET1110: CAT II) The IAO/NSO will ensure request forms are used to aid in recording the audit trail of router change request.*

- *(NET1110: CAT II) The IAO/NSO will ensure changes and modifications to routers are audited so that they can be reviewed.*

- *(NET1110: CAT II) The router administrator will ensure current paper or electronic copies of router configurations are maintained in a secure location.*

- *(NET1110: CAT II) The IAO/NSO will ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.*

3.5 Firewalls

Perimeter filtering rules can be applied to any internal firewall device or router and should be implemented to the fullest extent possible. This is necessary in order to minimize internal threat and protect the enclaves. Allowing only approved IP addresses through the perimeter router will control access to required ports and services. The Enclave firewall rules should be based on applications being used within the internal Enclave; all non-required ports and services will be blocked by the most restrictive rules possible and what is allowed through the firewall will be configured IAW Appendix C and DOD Instruction 8551.1 (*"that which is not expressly allowed is denied"*).

3.5.1 Perimeter Protection

- *(NET1160: CAT II) The IAM will ensure that a firewall has been implemented to protect the entire facility and has been configured with a deny-by-default policy.*

- *(NET1162: CAT II) The IAM will ensure that the firewall policy is in accordance with DOD Instruction 8551.1. http://www.dtic.mil/whs/directives/corres/html/85511.htm and Appendix C of this document.*

- *(NET1163: CAT I) The IAO will ensure that the Enclave perimeter is protected*

NOTE 1: When verifying compliance with the Deny-by-Default requirement, first verify that the filter ends with the deny rule (implied or explicit). Then verify what is permitted by the filtering rules is IAW Appendix C and DOD Instruction 8551.1. http://www.dtic.mil/whs/directives/corres/html/85511.htm. This requirement applies to all internal and external interfaces.

NOTE 2: If the firewall is in a Deny-by-Default posture, and what is allowed through the firewall filtering is IAW DOD Instruction 8551.1 and Appendix C, then all requirements related to PPS being blocked would be satisfied. The PPS would be covered under the Deny-by-Default rule as long as a permit rule was not created for them.

NOTE 3: The requirement for perimeter protection includes either a firewall implemented to protect the enclave or the premise router ACLs are in a deny by default posture. One or the other will satisfy the requirement at the enclave boundary.

3.5.2 Firewall Architecture

The Screened Subnet Firewall Architecture will be used (see *Figure 3-1* below). This firewall implementation is set up as a gateway with multiple network interface cards (NICs)—one connected to the external network through a router, one to the internal network, and one to the DMZ (if applicable). Packet forwarding is disabled on the gateway and information is passed at the application level or the network layer, depending on the type of firewall used. The firewall/gateway can be reached from all sides, but traffic cannot directly flow across it unless that particular traffic is allowed to pass to the requested destination.

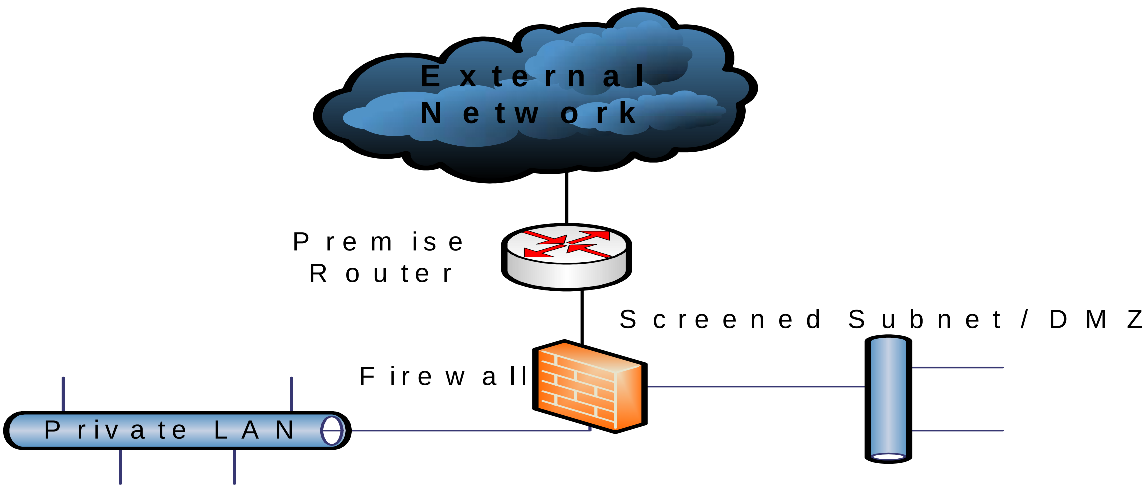

Figure 3- 1. Screened Subnet (DMZ)

- *(NET1170: CAT III) The IAM will ensure that only firewalls that have a Common Criteria Protection Profile evaluation of EAL4 or greater are placed in the network infrastructure.*

- *(NET1180: CAT II) The IAO/NSO will ensure that a Screened Subnet (DMZ) Firewall Architecture is implemented.*

- *(NET1190: CAT II) The IAO/NSO will ensure that all networks use application-level gateways or firewalls to proxy all traffic to external networks. Web proxy services will be provided as a minimum.*

NOTE: 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, is an acceptable alternative.

3.5.3 Firewall Placement

A firewall can be placed at several locations to provide protection from attacks. Each implementation will differ depending on several key factors, including the sensitivity of the networks, the network infrastructure, and the type of network traffic. Firewalls are used primarily to protect the boundaries of a network, although at times they can be used to separate an internal security domain from the rest of an enclave. There are three main points at which a firewall can be implemented within a network—at LAN-to-WAN connections, at LAN-to-LAN connections, and at WAN-to-WAN connections.

The Enclave requirement to place an application-level 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., stateful inspection, hybrid, packet-filter) with an application-level firewall protecting every Security Domain (including the DMZ) with no IP addressable systems or devices operating in the area between the non-application-level firewall and the Security Domain's firewall

- *(NET1200: CAT II) 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.*

3.5.4 Identification & Authentication

Identification and authentication is one of the major functions provided by the firewall. While users on the inside of a firewall are often considered trusted, external users who require access to the internal network must be authenticated. At a minimum, the firewall must support a secure, strong user authentication system (e.g., SecureID, Radius, or TACACS+).

In-band management is only to be used in situations where OOB management has been deemed to hinder operational commitments, and the IAO/NSO has approved in writing the use for that specific purpose.

- *(NET1220: CAT II) The IAO/NSO will ensure the firewall authenticates all administrators using individual accounts before granting access to the firewall's administration interface.*

- *(NET1222: CAT II) The IAO/NSO will ensure all user and administrator accounts are assigned the lowest privilege level that allows them to perform their duties.*

- *(NET1224: CAT II) The IAO/NSO will ensure the firewall is set to lock out accounts after three unsuccessful logon attempts.*

- *(NET1226: CAT II) The IAO/NSO will ensure that only the FA is allowed to remotely access the firewall administration interface.*

- *(NET1228: CAT II) The IAO/NSO will ensure only authorized personnel have permission to change security settings on the firewall.*

3.5.5 Configuration

The firewall must protect the private network from external attacks. The firewall will be maintained with the currently supported version of the firewall software and the Operating System (OS) with all security related patches applied. The firewall administrator (FA) will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.

- *(NET1240: CAT II) The IAO/NSO will ensure that the firewall is configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.*

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

- *(NET1250: CAT II) The FA will ensure the firewall does not utilize or enable any services (DNS, HTTP, etc.) not required by the firewall engine.*

- *(NET1252: CAT II) The FA will use a supported version of the firewall software with all security-related patches applied.*

- *(NET1254: CAT II) The FA will ensure that if the firewall product operates on an OS platform, the host must be STIG compliant prior to the installation of the firewall product.*

NOTE: If an IAVM is issued against the OS any time after the firewall installation and implementation, the FA must contact the firewall vendor, or FSO if deployed by FSO, to determine if the firewall is vulnerable and if there is a patch to be applied to the OS. If the vendor does not recommend installing a patch or upgrade, and has stated that the firewall is not vulnerable, the FA must retain this documentation.

- *(NET1260: CAT III) The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.*

3.5.6 Auditing and Administration

Qualified personnel who are specifically trained in the operation and administration of the firewall must administer the firewall. At least two firewall administrators will be identified for each managed firewall. Follow the auditing and administration rules below:

- *(NET1280: CAT III) 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.*

- *(NET1282: CAT III) The FA will ensure the firewall logs are retained online for a minimum of 30 days and then stored offline for one year.*

- *(NET1284: CAT III) The IAO/NSO will ensure the firewall configuration data are backed up weekly and whenever configuration changes occur.*

- *(NET1286: CAT III) The IAO/NSO will ensure the firewall log data is backed up weekly.*

- *(NET1290: CAT II) The IAO/NSO will ensure the firewall is configured to alert the administrator of a potential attack or system failure.*

- *(NET1300: CAT III) The FA will ensure the following capabilities will be enabled on the firewall:*

  - *Log unsuccessful authentication attempts.*
  - *Stamp audit trail data with the date and time when recorded.*
  - *Record the Source IP, Destination IP, protocol used, and the action taken.*
  - *Log administrator logons, changes to the administrator group, and account lockouts.*
  - *Protect audit logs from deletion and modification.*
  - *The firewall will provide the ability to record a readable audit log of security-related events, with accurate dates and times, with the capability to search and sort the audit log based on relevant attributes.*

- *(NET1310: CAT II) The FA 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.*

NOTE: IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

- *(NET1312: CAT II) For in-band management, the IAO/NSO will implement the use of two-factor authentication.*

NOTE: Two-factor authentication discussion; reference *Section 3.4.3.1*.

- *(NET1314: CAT II) The FA will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses.*

NOTE: The number must be equal to or less than the number of firewall administrators.

- *(NET1316: CAT II) The FA will ensure that all in-band management access to all firewalls is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

3.6 Network Intrusion Detection (NID)\Real Secure

Network intrusion detection systems (NIDS) provide an additional level of control and visibility into the network infrastructure. Implementing a NIDS on the network's exterior can expose unauthorized or malicious traffic that will most likely be blocked by the premise router and firewall as well as traffic from hackers who may be able to thwart the enclave perimeter protection mechanisms. Network intrusion detection systems can also be used to block suspect attacks that are easily recognized. Perhaps the greatest value that network intrusion detection systems provide is the information about the use and usage of the network. This information provides decision support data, can increase the value and efficiency of existing enclave protection mechanisms, and can produce hard evidence and justification for altering the enterprise's security policy.

3.6.1 External Network Intrusion Detection System

As depicted in *Section 2, Enclave Architecture Overview*, an external NIDS must be installed and implemented in front of the premise or border router and must be monitored by the certified CNDSP. Placing the external NIDS on the exterior—that is, between the premise router and the node router—will enable the CNDSP to detect attempted attacks that may otherwise be blocked by the premise router or firewall. A signature-based, anomaly-based, or rules-based NIDS that has been customized to specific NIPRNet or SIPRNet traffic can alert CND Service Provider of suspected threats at the enclave's gateway.

The JID is a suite of software tools that supports the detection, analysis, and gathering of evidence of intrusive behavior occurring on Ethernet or Fiber Distributed Data Interface (FDDI) based networks using IP. In support of these services, JID provides four common operating models:

- Retrospective intrusion analysis
- Near Real-time intrusion detection
- Evidence gathering
- Statistics gathering

- *(NET1325: CAT II) 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.*

- *(NET1326: CAT II) 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.*

NOTE: 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 certified CNDSP. However, if this site has other external connections such as an ISP, this traffic would need to be monitored by a CNDSP using an external NIDS.

- *(NET1327: CAT II) The IAO/NSO will ensure that the external NIDS is located between the site's NIPRNet or SIPRNet Point of Presence (POP) and the premise router.*

- *(NET1328: CAT III) The IAO/NSO will ensure that the data from the external NIDS is restricted to* CNDSP *personnel only.*

3.6.2 Internal Network Intrusion Detection System

All DOD locations will install, maintain, and operate a NIDS inside of their network enclaves. The Enclave NIDS will monitor internal network traffic and provide near real-time alarms for network-based attacks. A host intrusion detection (HID) application is not required on an OS-based NID.

The site may establish a support agreement with the CNDSP for monitoring. The local staff is responsible for initial response to real-time alarms.

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.

- *(NET1330: CAT II) The Network IDS administrator will ensure a Network IDS is installed and operational with all connections (e.g., LAN and WAN) being monitored.*

- *(NET1340: CAT II) The IAO/NSO will establish policies outlining procedures to notify JTF-GNO when suspicious activity is observed.*

- *(NET1342: CAT II) The IAO/NSO will ensure that authorized reviewers of Network IDS data are identified in writing by the site's IAM.*

- *(NET1344: CAT II) The IAO/NSO will ensure that any unauthorized traffic is logged for further investigation.*

- *(NET1346: CAT II) The IAO/NSO will establish weekly data backup procedures for the Network IDS.*

- *(NET1348: CAT II) The IAO/NSO will establish anti-virus update procedures for the Network IDS.*

- *(NET1350: CAT III) The Network IDS administrator will subscribe to the vendor's vulnerability mailing list.*

- *(NET1350: CAT III) 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.*

3.7 Switches and VLANs

3.7.1 Horizontal Wiring

Poor design of horizontal wiring within the physical network infrastructure can invite the connection to the private network by an unauthorized host or even a rogue wireless access point. The horizontal wiring extends from the work area wall plate or LAN outlet to the Intermediate Distribution Frames (IDF)—commonly referred to as the "wiring closet." The path of all horizontal wiring includes the wall plate, the horizontal cable that runs from the wall plate to the IDF, as well as any patch cables used between any cross-connect hardware (i.e., patch panel, distribution frame) and the switch.

Since it would be virtually impossible to monitor all work area wall plates to ensure that only authorized devices are attached, physical LAN access control and security must be maintained within the IDF. This end of the horizontal wiring must be disconnected at the switch port or patch panel if there is no authorized host connected to it in the work area.

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.

- *(NET1362: CAT II) 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.*

3.7.2 Switch Accounts and Passwords

Securing administrative access to all switches is critical to maintaining stability and integrity within the network infrastructure. Administrative access to any switch by unauthorized personnel provides a mechanism to not only disrupt service at the core or access layers, but also break down the security provided between VLANs—including the access to the network's OOB management VLAN. In order to control and authorize administrative access, an authentication server that provides user authentication as well as authority level validation will be implemented. Individual user accounts with passwords will be set up and maintained in accordance with the guidance contained in Appendix B, CJCSM.

- *(NET1364: CAT II) The IAO/NSO will ensure that an authentication server is used to gain administrative access to all switches.*

- *(NET1365: CAT II) The IAO/NSO will ensure that when an authentication server is used for administrative access to the switch, only one account can be defined locally on the switch for use in an emergency (i.e., authentication server or connection to the server is down).*

- *(NET1366: CAT I) The IAO/NSO will ensure that each user has their own account to access the switch with username and password.*

- *(NET1367: CAT II) The IAO/NSO will ensure that all user accounts are assigned the lowest privilege level that allows them to perform their duties.*

- *(NET1368: CAT II) The switch administrator will immediately remove accounts from the authentication server or switch that are no longer required.*

- *(NET1369: CAT II) The IAO/NSO will ensure that passwords are not viewable when displaying the switch configuration.*

3.7.3 Switch Administrative Access

3.7.3.1 OOB Switch Management

Management must be performed OOB via the console port or an OOB management network. The console port will be configured to time out, so that if an administrator forgets to log out, the device will log the administrator out automatically. The auxiliary port will be disabled. Users should never connect a modem to the aux port as a backup or remote access method to the device.

- *(NET1380: CAT I) The IAO/NSO will ensure that all OOB management connections to the switch require passwords.*

- *(NET1381: CAT II) The switch administrator will ensure the switch console port is configured to time out after 10 minutes or less of inactivity.*

- *(NET1382: CAT II) The IAO/NSO will ensure modems are not connected to the console or auxiliary ports.*

- *(NET1383: CAT III) The switch administrator will ensure that the switch's auxiliary port is disabled.*

3.7.3.2 In-band Switch Management

In-band management administration with telnet is dangerous because anyone with a network sniffer and access to the right LAN segment can acquire the device account and password information. Network device security relies upon protecting the paths and sessions used to access the device.

Access lists or filters must be used to limit which hosts may connect to the network device using any in-band management application. Additionally, the IP addresses, which will be restricted to administrators, must originate from the internal network.

In-band management is only to be used in situations where OOB management has been deemed to hinder operational commitments, and the IAO/NSO has approved in writing the use for that specific purpose.

- *(NET1385: CAT I) The IAO/NSO will ensure that all in-band management connections to the switch require passwords.*

- *(NET1386: CAT II) The switch administrator will ensure that the switch only allows in-band management sessions from authorized IP addresses from the internal network.*

- *(NET1387: CAT II) The switch administrator will ensure in-band management access to the switch is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(NET1388: CAT II) The switch administrator will set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds or less.*

- *(NET1389: CAT II) The switch administrator will set the maximum number of unsuccessful SSH login attempts to three before locking access to the switch for the individual account.*

- *(NET1390: CAT II) The IAO/NSO will ensure the timeout for in-band management access is set for no longer than 10 minutes.*

- *(NET1391: CAT IV) The switch administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*

3.7.4 Virtual Local Area Networks (VLANs)

VLAN technology is an efficient way of grouping users into workgroups to share the same network address space regardless of their physical location on the network. Users can be organized into separate VLANs according to their department, location, function, application, physical address, logical address, or protocol. Regardless of organization method used, the goal with any VLAN is to group users into separate communities that share the same resources; thereby, enabling the majority of their traffic to stay within the boundaries of the VLAN.

Network nodes of the same VLAN can communicate with other nodes in the same VLAN using layer-2 switching. In order to communicate with other VLANs, the nodes in one VLAN need to go through a layer 3 device. Broadcast frames are switched only between nodes within the same VLAN. This logical separation of users and traffic results in better performance management (i.e., broadcast and bandwidth utilization control) as well as a reduction in configuration management overhead enabling networks to scale at ease.

3.7.4.1 Management VLAN and VLAN1

By default, all ports—including the internal sc0 interface, are configured to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to transport Layer-2 control plane traffic such as the following:

- Spanning Tree Protocol (STP)
- Cisco Discovery Protocol (CDP)
- Dynamic Trunking Protocol (DTP)
- VLAN Trunking Protocol (VTP)
- Uni-Directional Link Detection (UDLD)
- Port Aggregation Protocol (PAgP)

This is all untagged traffic. As a consequence, VLAN1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly. The risk is even greater if VLAN1 is also used for user VLANs or the management VLAN. In addition, it is unwise to mix management traffic with user traffic making the management VLAN an easier target for exploitation.

- *(NET1410: CAT II) The IAO/NSO will ensure VLAN1 is not used for in-band management traffic. The IAO/NSO will assign a dedicated management VLAN to keep management traffic separate from user data and control plane traffic.*

- *(NET1411: CAT III) The IAO/NSO will ensure the management VLAN is not configured on any trunk or access port that does not require it.*

- *(NET1412: CAT II) The IAO/NSO will ensure VLAN1 is not used for user VLANs.*

- *(NET1413: CAT III) The IAO/NSO will ensure VLAN1 is pruned from all trunk and access ports that do not require it.*

3.7.4.2 VLAN Trunking

There can be several VLANs defined on a single switch, while on the other hand a VLAN can span across multiple switches. VLAN spanning is enabled by trunked links connecting the switches and frame tagging such as IEEE 802.1q or Cisco's Inter-Switch Link (ISL) protocol. Trunk links can carry the traffic of multiple VLANs simultaneously. Therein lies a potential security exposure. Trunk links have a native or default VLAN that is used to negotiate trunk status and exchange VLAN configuration information. Trunking also enables a single port to become part of multiple VLANs—another potential security exposure. Within the switch fabric, switches use frame tagging to direct frames to the appropriate switch and port. Frame tagging assigns a VLAN ID to each frame prior to traversing a trunked link. Each switch the frame traverses must identify the VLAN ID and then determine what to do with the frame based on its filter table. Once the frame reaches the exit to the access link, the VLAN ID is removed and the end device receives the frame. The frame tagging is another technology that can be exploited as a result of a poor VLAN implementation design.
VLAN "hopping" occurs when a tagged frame destined for one VLAN is redirected to a different VLAN, threatening network security. The redirection can be initiated using two methods: "tagging attack" and "double encapsulation." Frame tagging attacks allow a malicious user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port's trunk mode were configured as *auto* (enables a port to become a trunk if the connected switch it is negotiating trunking with has its state set to *on* or *desirable*) and were to receive a fake DTP packet specifying *trunk on* or *desirable*, it would become a trunk port and it could then start accepting traffic destined for all VLANs that belong to that trunk group. The attacker could start communicating with other VLANs through that compromised port—including the management VLAN. Insuring that trunk mode for any non-trunking port is configured as *off* can prevent this type of attack.

Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that is the attacker's VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port. To ensure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

- *(NET1416: CAT II) The IAO/NSO will ensure trunking is disabled on all access ports (do not configure trunk on, desirable, non-negotiate, or auto—only off).*

- *(NET1417 CAT III) The IAO/NSO will ensure when trunking is necessary; a dedicated VLAN is configured for all trunk ports.*

- *(NET1418 CAT III) The IAO/NSO will ensure access ports are not assigned to the dedicated trunk VLAN.*

3.7.4.3 VLAN Access – Port Authentication

Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Unauthorized internal access leads to the possibility of hackers or disgruntled employees gaining control of network resources, eavesdropping, or causing denial-of-service on the network. Simply connecting a workstation or laptop to a wall plate or access point located in the work area enables internal access to the private network.

An initial security best practice for a VLAN-based network is to place all disabled ports into an unused VLAN, thereby thwarting unauthorized VLAN access using both physical and logical barriers.

Once a user has connected to the network, services that the client has access to should be based on individual need—and only if that individual or workstation is authorized. First determining if the individual or workstation is authorized to connect to the network and then ensuring that it is assigned to the appropriate VLAN can restrict this. Restricting VLAN access and authenticating switch port connections can be accomplished using one of the following methods:

1. Port security
2. Port authentication with 802.1X
3. VLAN Management Policy Server (VMPS)

- *(NET1435: CAT III) The IAO/NSO will ensure disabled ports are placed in an unused VLAN (do not use VLAN1).*

- *(NET1436: CAT I) The IAO/NSO will ensure either Port Security or 802.1X Port Authentication is used on all access ports.*

Port Security

The port security feature provided by most switch vendors can be used to block input to the access port when the MAC address of the station attempting to access the port does not match any of the MAC addresses specified for that port—that is, those addresses statically configured or auto-configured (i.e., “learned). The maximum number of MAC addresses that can be configured or learned (or combination of both) is also configurable.

In the event of a security violation, the Link LED for that port turns orange. Configure the port to shut down permanently, shut down for a specified time interval, or drop incoming packets from the unsecured host if a violation occurs. If either of the first two methods is used, a link-down trap is also sent to the Simple Network Management Protocol (SNMP) manager.

If port security is implemented, every switch at the access layer must have port security enabled on every access port that is in use—that is, a switch port configured as enabled and as an access port. Furthermore, the MAC addresses must be statically configured for each port.

- *(NET1437: CAT II) The IAO/NSO will ensure if Port Security has been implemented, the MAC addresses are statically configured on all access ports.*

Port Authentication with 802.1x

While technologies such as MAC filtering and ACLs are used to enhance overall network security, the IEEE 802.1X Port Based Network Access Control specification provides another level of network protection. Authentication through IEEE 802.1X provides the ability to limit network access based on a client profile. A client profile typically contains the client identification and access privileges. Data cannot be passed through the switch and onto the LAN until the client's identification has been verified. There are several benefits gained by implementing 802.1X on all edge or access layer switches. The secure authentication allows a client to be recognized and granted access privileges from the location he or she logs on. It can also account for a client's activity while they are connected to the network.

The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before allowing connectivity. The switch port state determines whether or not the client is granted access to the network. The port starts in the "unauthorized state." While in this state, 802.1X access control only allows Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. The EAPOL traffic facilitates the authentication process between the client and the access servers. When a client is successfully authenticated, the port transitions to the authorized state allowing all traffic for the client to flow normally. Only one client can be connected to the 802.1X-enabled switch port. The switch detects the client when the port link state changes to the up state. If a client leaves or is replaced with another client, the switch changes the port link state to down, and the port returns to the unauthorized state.

EAPOL is a delivery mechanism and does not provide the actual authentication mechanisms for the protocol. When utilizing 802.1X, an Extensible Authentication Protocol (EAP) type must be chosen to define how the authentication is to take place. The specific EAP type resides on the authentication server and within the operating system or application software on the client devices. During negotiation, the switch sends the identity to an authentication server. EAP is defined by the IETF and can be further researched at (http://www.ietf.org). The 802.1X standard describes how to send and receive EAP over IEEE 802 LANs (EAPOL). In order to deploy 802.1X, an authentication method/type must be selected in order to transmit inside this EAPOL envelope. Following are some methods that may be considered.

Transport Layer Security (EAP-TLS)
EAP Tunneled Transport Layer Security (EAP-TTLS)
Protected EAP
Lightweight EAP (LEAP)
EAP-MD5

EAP-TLS uses the Transport Layer Security (TLS) protocol to create an encrypted channel for negotiation and authentication using digital certificates. TLS (the standard version of SSL) provides confidentiality and integrity, therefore, using EAP-TLS is a secure solution.

EAP-TTLS (Tunneled TLS) method provides a means for the Authentication Server to use a certificate to establish the TLS tunnel. Existing client credentials (for example, Windows login/password) can then be transmitted over the encrypted tunnel to authenticate the station. Authentication protocols such as (PAP, CHAP, and EAP) are carried as RADIUS attribute/value pairs over TLS and may be considered secure solutions.

Protected-EAP (PEAP) is conceptually similar to EAP-TTLS, but sends only EAP over the TLS tunnel. Phase 1 PEAP creates the TLS tunnel, then Phase 2 PEAP uses the tunnel to carry out and complete EAP authentication. PEAP can be used with any kind of authentication carried by EAP, including certificate authentication and client-side password authentication. PEAP is considered a secure solution.

Lightweight EAP (LEAP) is a CISCO proprietary protocol providing an easy-to-deploy l password authentication. LEAP is vulnerable to dictionary attacks. A "man in the middle" can capture traffic, identify a password, and then use it to access a WLAN. LEAP is inappropriate and does not provide sufficient security for use on DOD networks.

EAP-MD5 is functionally similar to CHAP and is susceptible to eavesdropping because the password credentials are sent as a hash (not encrypted). In addition, server administrators would be required to store unencrypted passwords on their servers violating other security policies. EAP-MD5 is inappropriate and does not provide sufficient security for use on DOD networks.

EAP methods/types are continually being proposed, however, as of this writing the five indicated above have been evaluated. Of the five, the three being considered secure are EAP-TLS, EAP-TTLS, and PEAP.

If port authentication is implemented, every switch at the access layer must have 802.1X enabled on every access port that is in use. Furthermore, the ports must be configured to start in the unauthorized state and they must re-authenticate the client at regular intervals.

- *(NET1434: CATII) The IAO/NSO will ensure when utilizing 802.1X, a secure EAP type (EAP-TLS, EAP-TTLS or PEAP) resides on the authentication server and within the operating system or application software on the client devices.*

- *(NET1438: CAT I) The IAO/NSO will ensure if 802.1X Port Authentication is implemented, all access ports start in the unauthorized state.*

- *(NET1439: CAT II) The IAO/NSO will ensure if 802.1X Port Authentication is implemented, re-authentication occurs every 60 minutes.*

VLAN Management Policy Server (VMPS)

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 act 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 an 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.

- *(NET1435: CAT III) The IAO/NSO will ensure disabled ports are placed in an unused VLAN (do not use VLAN1).*

- *(NET1436: CAT I) The IAO/NSO will ensure Port Security or 802.1x Port Authentication is used on all access ports.*

- *(NET1437: CAT II) The IAO/NSO will ensure if Port Security has been implemented, the MAC addresses are statically configured on all access ports.*

- *(NET1438: CAT I) The IAO/NSO will ensure if 802.1x Port Authentication is implemented, all access ports must start in the unauthorized state.*

- *(NET1439: CAT II) The IAO/NSO will ensure if 802.1x Port Authentication is implemented, re-authentication must occur every 60 minutes.*

4. REMOTE USER ACCESS

Information security vulnerabilities are inherent in all forms of computer systems, software, architectures, and devices. The goal of information security is to provide data integrity, confidentiality, and availability. In order to provide these services to the DOD community, general security standards for any form of remote access to a DOD network must be in place. These standards are set forth for ease of configuration management and to aid in developing a secure, standardized remote access environment. This section sets the security guidance applicable to all remote access communications methods and access levels. This guidance will be adhered to, in addition to the requirements set forth in the individual sections that provide detailed security requirements for remote access.

4.1 Levels of Remote User Access

There are varying sensitivity levels when initiating remote access to a Department of Defense network and the resources it contains. The following levels are defined to differentiate the types of remote access users. These definitions are used to clarify differing requirements based on the type of access required by the user. If the site so chooses, Administrative and End-User access may be treated the same for configuration management purposes; however, systems will be secured at the Administrative Access Level. If the site allows Administrative or End-User access to a system, the remote device must be controlled or owned by a Government entity to allow for confiscation and review at any time. This requirement allows for the review of security vulnerabilities and STIG requirements, as well as determination of possible spillage or harm to the network infrastructure. These requirements pertain to any system within an Enclave, excluding those resources specifically designed for public access (e.g., resources residing in a DMZ such as a web server).

Administrative Access – Remote users who will be connecting to a DOD core network to perform any system administration duties to include troubleshooting, configuration changes, and reviewing any system or configuration data, regardless of system type. This type of access will require the most stringent security controls and users must use government owned or controlled devices. Administrative access will employ encryption.

End-User Access – Remote users who will be accessing, downloading, or uploading data. The “end-user” remote access level requires that users do not make any system configuration changes or view system configuration information. This type of access will require medium security controls on the remote system and users must use government owned or controlled devices. End-User access includes customers who access, change, or download Government data via Telnet and other clear-text terminal emulators. It is strongly suggested that End-User access employs the use of encryption.

Limited (General) Access – Remote users who are viewing content or sending e-mail, but are not altering or entering official Government data (e.g., viewing e-mail via a web mail application such as Outlook for Web Access [OWA] or accessing a DOD web site). This type of access will require minimum-security controls and users may use personal computers or devices if approved by the local DAA.

As System Administrators perform duties such as configuration changes, troubleshooting application and communications issues, and logging in to a system with privileges to perform maintenance functions, rigorous security measures must be in place to protect the data and communication to and from the system. Administrative access will require the use of encryption on all communication channels between the remote user and the system being accessed. If the system requires the use of a clear-text based terminal emulator such as Telnet or TN3270, which accesses 3270 and 5250 based applications over TCP/IP, the only acceptable methods of connectivity will be an encrypted session, the employment of VPNs, Secure Web Access (SWA) with Secure Socket Layer (SSL), IPSEC, or SSH. Encryption should be used to protect the End-User access level. However, as of this writing, it is not required, but rather it is a suggested practice.

Limited access does not preclude the remote user from using their personal PCs to access services such as a web mail application (e.g., OWA) to send and receive e-mail. Limited Access users are not prohibited from accessing publicly accessible services that reside in a DMZ. While the intent at this time is to allow users to access a Government web mail application from a personal PC, the preferred method is to access e-mail from Government owned or controlled devices via dial-up or VPNs in order to limit the Government's exposure to malicious threats.

To ensure security within a classified environment, strict controls must be in place prior to any remote access to the classified network or resource. DOD has stringent policies on the access, storage, location, and containment of all classified data and processing. Furthermore, it is prohibited to allow non-DOD personnel to obtain remote access capability to any DOD network.

- *(NET1440: CAT III) The IAO/NSO will ensure that end user access is limited and the use of clear text Telnet, TN3270, and other terminal emulator TCP/IP sessions employ encryption to the fullest extent possible.*

NOTE: Refer to the *Enclave STIG* for additional information on FTP and Telnet.

- *(NET1441: CAT I) The IAO/NSO will ensure that an NSA Certified remote access security solution is in place for remote access to a classified network and is only used from an approved location.*

  - *The solution will be used in accordance with all NSA and DOD policy and guidelines.*
  - *The secure solution will support Key Exchange Algorithm (KEA).*
  - *The secure solution will support Palladium Fortezza Modems.*
  - *Each modem will have a valid X.509 V1 Certificate issued.*
  - *The Fortezza card will be kept in the user's possession at all times or stored in accordance with policy applicable to classified storage.*
  - *The modem will be stored separately from the computer when not in use.*

4.2 Remote User Access Agreement

There are numerous places from which a remote user can access a network, such as General Services Administration (GSA) telework centers, hotel rooms, homes, airports, other DOD sites, etc. To remotely access a DOD network or resource, a remote user must complete and sign a computer security checklist and a remote access agreement that is developed by the site. This STIG is intended to secure the site's network regardless of the location the remote user.

- *(NET1446: CAT II) The IAM will develop a policy for secure remote access to the site and an agreement between the site and remote user, to include, but not limited to, the following:*

  - *The signed agreement will contain the type of access required by the user.*

  - *The signed agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of their remote access device.*

  - *Incident handling and reporting procedures will be identified along with a designated point of contact.*

  - *The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.*

  - *The policy will contain general security requirements and practices and will be acknowledged and signed by the remote user.*

  - *If classified devices are used for remote access from an alternative work site, the remote user will adhere to DOD policy in regard to facility clearances, protection, storage, distributing, etc.*

  - *Government owned hardware and software will be used for official duties only. The employee is the only individual authorized to use this equipment.*

4.3 Authentication, Authorization, and Accounting (AAA)

An Authentication, Authorization, and Accounting (AAA) server manages user requests for access to network resources. Restricting access to all network components is critical in safeguarding the enclave. In order to control and authorize access, an authentication server (e.g., Radius, TACACS+, or Kerberos) that provides extended user authentication and authority levels will be implemented.

- *(NET1451: CAT II) The IAO/NSO will ensure that all remote users are required to use a form of two-factor authentication to access the network.*

  - Two-factor authentication discussion; reference *Section 3.4.3.1*.

- *(NET1452: CAT III) The IAO/NSO will ensure that the remote access infrastructure (i.e., authentication server, RAS/NAS device, VPN gateway) logs session connectivity and termination, userid, assigned IP address, and success or failure of all session events.*

Logging is a key component of any security architecture and is a critical part of AAA server security. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment. Maintaining an audit trail of system activity logs can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network.

- *(NET1453: CAT III) The IAO/NSO will ensure that a session that exceeds 30 minutes of inactivity is disconnected.*

- *(NET1455: CAT III) The IAO/NSO will ensure that the audit logs for any remote access server authentication mechanism are maintained for no less than a period of 30 days on-line, and one year off-line.*

- *(NET1456: CAT III) The IAO/NSO will ensure that the audit logs are viewed on a weekly basis.*

4.4 Dial-up Communications

Using either public switched telephone network (PSTN) or Integrated Services Digital Network (ISDN) lines, dial-up remote access is still one of the most cost effective and flexible solutions available today. With boosts in data throughput through increases in modem speeds and gains in data compression algorithms, as well as effective resource sharing though modem pooling, there are a number of applications that are well suited for dial-up communications. This section will focus on opportunities along with the risks associated with the dial-in remote access application that can be implemented within a site’s network infrastructure enabling personnel at remote locations to gain access to its resources.

4.4.1 Modems

Implementing a dial-up technology—whether dialing out or dialing in—introduces additional security concerns for the network infrastructure. Each modem is a potential gateway for uninvited users, either by chance or malicious intent, to gain access to the attached network. Modems can provide an unchecked gateway to sensitive data within the DOD’s computing boundaries. Keeping accurate records of all authorized modems used for both dial-in and dial-out is a good practice that promotes sound configuration management and an awareness of all network access points.

- (*NET1460: CAT III) The IAO/NSO will ensure all modems are physically protected.*

- *(NET1462: CAT III) The IAO/NSO will maintain a listing of all modems, associated phone number, and location.*

- *(NET1470: CAT III) The IAO/NSO will ensure that all modem phone lines are restricted to single-line operation if dial back services are not used (inward dial only or outward dial only) without any special features (e.g., call forwarding).*

4.4.2 Remote Access Server/Network Access Server

A Remote Access Server (RAS) or Network Access Server (NAS) is a device that provides for the initial entry point into a network. The NAS provides all the services that are normally available to a locally connected user (e.g., file and printer sharing, database and web server access, etc.). Permission to dial in to the local network is controlled by the NAS and can be granted to single users, groups, or all users. NAS servers such as Windows RAS, Shiva LanRover, and CISCO AS5200 have interfaces both to the network backbone and to the switched telephone service provider. These servers receive calls from remote clients or hosts that want to access the network using analog dial-up services that can support connections up to 56 Kbps. Access servers (e.g., Ascend Pipeline 4004 and Cisco AS5200) with an ISDN interface, as well as remote access servers with ISDN cards, support connections up to 128 Kbps. NAS and RAS devices can also interface with authentication servers such as RADIUS and TACACS.

Multi-modem adapter cards that plug into Windows servers can provide a low-cost analog alternative to a dedicated remote access server. These cards fit into any Intel-based server and support up to 24 communication ports bound to Windows RAS services. Some multi-modem cards support RSA SecurID for user authentication, which can be used with a RADIUS server to provide user management, session management, and accounting services. Because server cards can be installed on primary or backup domain controllers, a network administrator may inadvertently give all dial-in clients "log on locally" rights to the network. If a few permissions were to be configured improperly, a security breach could be created. Furthermore, some multi-modem cards rely solely on Windows RAS for user authentication, and do not allow for the use of the approved authentication servers.

Callback features are an attempt to protect the network by providing a service that disconnects an incoming call and reestablishes the call, dialing back to a predetermined number. Upon establishment of the callback connection, the communications device will require the user to authenticate to the system.

Configuring a focal point of access is vital to the overall security of a remote access infrastructure. In addition, only services that are absolutely needed for end users to conduct business should be allowed through the firewall from this access point. Hence, a sound approach would be to place dial-in users under the same access policy as those connecting via VPN. This can easily be accomplished by placing the remote access server either in the DMZ or within a screened subnet where the VPN gateway resides. The screened subnet architecture provides a layered defense ensuring only authorized users are permitted access to the internal network while still providing protection for the remote access server.

- *(NET1530: CAT III) The IAO/NSO will maintain ANI logs to provide a call audit trail.*

- *(NET1535: CAT III) The Network Administrator (NA) will ensure that if callback procedures are used, upon establishment of the callback connection, the communications device requires the user to authenticate to the system.*

- *(NET1595: CAT II) The IAO/NSO will ensure that the RAS/NAS device is located in a DMZ or screened subnet, thereby providing protection to the server while enforcing remote user access under the same remote access policy as those connecting by VPN.*

- *(NET1600: CAT II) The IAO/NSO 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. The IAO/NSO will approve the use of in-band management on a case-by-case documented basis.*

- *(NET1602: CAT II) The IAO/NSO will ensure for in-band management, that the site implements the use of strong two-factor authentication.*

NOTE: Two-factor authentication discussion; reference *Section 3.4.3.1*.

- *(NET1604: CAT II) The IAO/NSO will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses. The number of IP addresses must be equal or less than the number of network engineers.*

- *(NET1606: CAT II) The IAO/NSO will ensure that all in-band management access to all remote access servers are secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

4.4.3 Dial-in Connectivity: SLIP and PPP

Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP) are the two communication protocols that enable a remote computer to connect to a network over standard asynchronous serial lines using a modem. Both SLIP and PPP provide the ability to transport TCP/IP traffic over the serial lines; however, PPP can support additional protocols such as IPX and AppleTalk.

The most significant advantage PPP provides is authentication and configuration negotiation. With SLIP, the remote user must configure communication parameters such as MTU (maximum transmission unit) and MRU (maximum receive unit). In addition, SLIP does not support authentication; hence, chat scripts must be used to provide some form of authentication before SLIP is started. On the other hand, PPP negotiates the configuration parameters at the start of the connection to include which authentication method will be used, as well as all required transmission parameters. PPP provides authentication methods such as PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). These protocols are used for authentication at the Data Link Layer—that is, between the remote client and the remote access server. These methods provide the means for the remote client to send logon userid and password information to the remote access server.

Authentication takes place when the remote node attempts to establish a PPP session with a remote access server. The remote access server can be configured to use PAP, SPAP, or CHAP to authenticate the remote node. After the link is established, the remote node is required to send the username and password pair to the remote access server.

PAP transmits the username and password as plain text. NT RAS server supports SPAP to allow remote access to Shiva clients. Unlike PAP, SPAP does send encrypted passwords over the communication link as opposed to clear-text passwords. CHAP offers additional security by using encrypted keys during communication between the remote access server and the remote node. With CHAP, PPP sends a randomly generated challenge string to the client, along with its hostname. The client uses the hostname to look up an appropriate key, combines this with the challenge, and encrypts it with a one-way hashing algorithm. The resulting string is returned to the server, along with the client's hostname. The server performs the same computation as the client on the challenge string. The server will only allow the client to connect if its computation result is identical to that received from the client. DES or MD5 encryption can be chosen when using CHAP. DES is the default option used by CHAP; however, MD5 is recommended. An additional security feature of CHAP is that client authentication is not only required at initial connect time but the server sends challenge strings to the client at regular intervals to detect if the client has not been replaced by an imposter. These two security features working together help to ensure data transfer security in the PPP network.

MS-CHAP is the most secure encryption algorithm that NT supports and is Microsoft's version of the RSA MD4 standard. MS-CHAP uses a one-way hash function to produce a message-digest algorithm. A hash function takes a variable-sized input and returns a fixed-size 128-bit string. This type of algorithm produces a secure checksum for each message, making it almost impossible to change the message if the checksum is unknown. MS-CHAP V2 provides two-way authentication or mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.

- *(NET1610: CAT II) The IAO/NSO will ensure that all remote clients and remote access servers are configured to use PPP instead of SLIP to provide the dial-up communication link.*

- *(NET1610: CAT II) The IAO/NSO will ensure that CHAP with MD5 or MS-CHAP with MD4 encryption is used to authenticate the remote client.*

4.5 Remote Client to VPN Gateway

A VPN is a network secured by encryption and authentication and is layered on existing public networks such as the Internet. A remote client uses the Internet and NIPRNet as the backbone for VPN connectivity to a DOD local area network. There are three tunneling protocols that can be used to create connectivity between a remote client and a VPN gateway:

- Point-to-Point-Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- IPSec

The latter is the most secured and the required method for VPN connectivity between a remote client and a DOD network.

PPTP is Microsoft‘s solution for remote access VPN using RSA RC4 encryption and CHAP or MS-CHAP authentication. Both encryption and authentication are done within PPP. The PPP packets are then encapsulated within IP packets to create the tunnel. PPTP uses an enhanced Generic Routing Encapsulation (GRE) mechanism to provide a flow- and congestion-controlled encapsulated datagram service for carrying PPP packets within IP. With PPTP, a remote user makes a dialup connection to an ISP NAS. The ISP provides a connection through its WAN and the Internet to a PPTP server residing in a DOD LAN. All encryption is done on the PPTP client and the decryption is done on the PPTP server creating a secured tunnel between the PPTP client and the PPTP server. The NAS can act as a PPTP client if the remote client is not PPTP aware; thereby, only providing a PPP session between the remote client and the NAS device at the ISP point of presence. For the obvious reason, the most secured implementation is to use a PPTP-enabled remote client to ensure that there is a secured tunnel between the remote client and the DOD LAN.

Based on Microsoft‘s PPTP and Cisco’s Layer 2 Forwarding Protocol (L2F), an L2TP VPN implementation model is similar to PPTP with one major difference—there is no encryption of the PPP packets so it must depend on IPSec or some other technology for encryption. Authentication is performed within PPP using PAP, CHAP, or Extensible Authentication Protocol (EAP).

IPSec provides two main facilities for creating VPN connections: an authentication-only function referred to as an Authentication Header (AH) and a combined authentication/encryption function called Encapsulating Security Payload (ESP) which can operate either in transport mode or tunnel mode.

In transport mode IPSec encrypts only the data component of the IP packet to be transported; if application headers, TCP/UDP headers, and data are encrypted, the IP headers are readable. The authentication data is calculated on the basis of values in the IP header (and some other things). The original IP header is therefore maintained and an additional IPSec header is appended. The advantage of this mode of operation is that only a few bytes are added to each packet. On the other hand, it is possible for attackers to analyse the data traffic in VPN, since the the IP headers are not modified. The data itself however is encrypted, so one can only determine how much data is being exchanged by which stations, but not what data.

In tunnel mode, the entire IP packet is encrypted and provided with a new IP header and IPSec header. The advantage lies in that those LANs that should be connected to a VPN, a gateway can be configured such that it accepts IP packets, changes them into IPSec packets and then sends them over the Internet to the gateway on the target network, which restores and forwards the original packet. Moreover, attackers can thereby only determine the start- and end point of an IPSec tunnel.

- *(NET1625: CAT II) The IAO/NSO will ensure that VPN gateways terminate on or outside of the firewall.*

- *(NET1630: CAT II) The IAO/NSO will ensure that remote access via VPN uses IPSec ESP in tunnel mode. For legacy support, L2TP may be used if IPSec provides encryption (DAA approval required), or another technology that secures using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

UNCLASSIFIED

This page is intentionally left blank.

5. NETWORK MANAGEMENT AND SUPPORT SERVICES

5.1 Network Management

Managing a network with automated tools is becoming a necessity as networks become more complex. These automated processes can be used to monitor network performance and activity as well as to provide reports about the network. Network management models are built around network elements and are configured to monitor the attributes and functions associated with them. A network management configuration generally involves a managing process that runs on a management workstation. The managing process collects performance and other relevant data about the network or about particular nodes on the network.

Network management is generally implemented as a high-level application, so that the management software uses well-established protocol suites, such as the TCP/IP and the seven-layer OSI Reference Model, to move its information around.

5.1.1 The IP Management Model

The major components within the TCP/IP based model are Structure of Management Information (SMI), Management Information Base (MIB), and SNMP. The SMI specifies how information about managed objects is to be represented. The MIB contains the definitions and values for the managed objects relevant to a particular network. The information for the MIB component is acquired and updated by a management agent, a program whose task is to determine and report the information desired by a management program. Continued expansion of a generic MIB has been abandoned in favor of a scheme that allows extensions for specific networking products to be defined as separate nodes. SNMP is the protocol used to transmit management information.

5.1.2 Network Management Security Implications

This document focuses on the IP management service. SNMP, by virtue of what it is designed to do, can be a large security risk. Because SNMP can obtain device information and set device parameters, unauthorized users can cause damage rather easily.

SNMP has three basic commands that can supply potentially network-damaging information to individuals:

- *GET* *For MIB variable polling, used by the management station to create threshold alarms, provide system settings, and show other device information.*

- *SET* *For altering a variable's value from the management station, possibly triggering an intended side effect such as causing the managed device to reset a counter or to reboot.*

- *TRAP* *For agents to asynchronously notify the management station of a significant event, such as a change in the availability status of a communication link.*

SNMPv2 and later releases support the use of MD5 protocol to ensure sender authenticity and message integrity by creating a hash value of the Protocol Data Unit (PDU). It can also incorporate a time stamp to avoid possible replay attacks. To achieve confidentiality of the PDU transmission, SNMPv2 and later uses Symmetric Privacy Protocol, which currently calls for the messages to be encrypted using the Digital Encryption Standard (DES). The communicating SNMP devices know the same symmetric DES key and can communicate freely across the network.

A would-be attacker can send SNMP GET sequences to routers, bridges, printers, or other devices polling for information. This individual could flood a particular device with so many GETs that all the processing time is used up, causing a denial of service. Using the TRAP, an unauthorized user could send an erroneous PDU to the router signaling that a circuit is down, thus causing packets to be rerouted or not delivered. A router's table or ACL could be overwritten by the SET command, allowing an unauthorized workstation access past the ACL router. On hosts using SNMP to communicate with the management station, commands can be sent to change an ARP cache table or even reboot the machine.

- *(NET1650: CAT II) The IAO/NSO will ensure IPSec is used to secure traffic between the network management workstation on DOD-managed LANs and all monitored devices sent via the Internet, NIPRNet, SIPRNet, or other external network.*

- *(NET1660: CAT I) The IAO/NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) is used across the entire network infrastructure.*

NOTE: If the site is using Version 1 or Version 2 with all of the appropriate patches to mitigate the known security vulnerabilities, this finding can be downgraded to a Category II. If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category III.

- *(NET1665: CAT I) The IAO/NSO will ensure that all SNMP community strings are changed from the default values.*

- *(NET1666: CAT II) The IAO/NSO will ensure that all SNMP community strings and usernames are protected via technology that secures using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(NET1670: CAT III) 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*

- *(NET1675: CAT II) The IAO/NSO will ensure that if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.*

- *(NET1710: CAT III) The IAO/NSO will ensure that security alarms are set up within the managed network's framework. At a minimum, these will include the following:*

  - *Integrity Violation: Indicates that network contents or objects have been illegally modified, deleted, or added.*

  - *Operational Violation: Indicates that a desired object or service could not be used.*

  - *Physical Violation: Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.*

  - *Security Mechanism Violation: Indicates that the network's security system has been compromised or breached.*

  - *Time Domain Violation: Indicates that an event has happened outside its allowed or typical time slot.*

- *(NET1720: CAT III) The IAO/NSO will ensure that alarms are categorized by severity using the following guidelines:*

  - *Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.*

  - *A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.*

  - *A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.*

  - *A warning alarm is used to signal a potential problem that may affect service.*

  - *An indeterminate alarm is one that requires human intervention to decide its severity.*

5.1.3 Network Management Station

At the center of the network management structure is the management station. Applications such as HP's OpenView and Cabletron's Spectrum provide the user interface to the various levels of network management mentioned above. All facets of the management umbrella are controlled from here. Without encrypted in-band management connections, unauthorized users may gain access to the NMS enabling them to change device configurations and SNMP variables that can cause disruptions and even denial of service conditions. It is extremely important that this workstation be protected as follows:

- *(NET1730: CAT II) The IAO/NSO will ensure that the management workstation is located in a secure environment.*

- *(NET1740: CAT II) The IAO/NSO will ensure that only those accounts necessary for the operation of the system and for access logging are maintained.*

- *(NET1750: CAT III) The IAO/NSO will ensure a record is maintained of all logons and transactions processed by the management station.*

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

- *(NET1760: CAT I) The IAO/NSO will ensure access to the NMS is restricted to authorized users with individual userids and passwords.*

- *(NET1762: CAT II) The IAO/NSO will ensure that all in-band sessions to the NMS is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

- *(NET1770: CAT II) The IAO/NSO will ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored.*

- *(NET1780: CAT II) The IAO/NSO will ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.*

5.2 Virtual Private Networks

5.2.1 Site-to-site VPN

A VPN is a distributed collection of networks or systems that are interconnected via a public and/or private network (i.e., the Internet or the NIPRNet) but protect their communications using encryption. In effect, a VPN is a private secure distributed network that is *transported* or *tunneled* across a public and/or private network. Typically, VPN encryption is implemented at the local network entry point (i.e., the firewall or Premise Router), thereby freeing the end systems from having to provide the necessary encryption or communications security functions.

- *(NET1800: CAT II) The IAO/NSO will ensure VPNs are established as tunnel type VPNs, which terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).*

The placement of the VPN is to maintain the security of the enclave and the requirement that all traffic must pass through the Enclave Security Architecture. This is not to say that encrypted data (e.g., SSL, SSH, TSL) that entered the VPN tunnel must also be unencrypted prior to leaving the tunnel. However, the data would still have to pass through the respective application proxy. If a host-to-host VPN is required, it will be established between trusted known hosts.

NOTE: A DOD site that enters into an agreement to establish a VPN with an outside security enclave/domain will retain administrative oversight and control privileges on the IPSEC/VPN device within their security enclave.

- *(NET1810: CAT III) 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.*

- *(NET1820: CAT II) The IAM will require the customer to provide an Intrusion Detection System (IDS) capability (host IDS) for any VPN established that bypasses the site's current IDS capability.*

A VPN solution can be cheaper than conventional networks that run over WAN connections. VPN devices and software provide not only encryption functions but also network access control to secure Internet tunnels between remote sites. A VPN must provide privacy and integrity of data as it traverses the public network. At a minimum it should provide for the following:

- User Authentication — The solution must verify a user's identity and restrict VPN access to authorized users. In addition, the solution must provide audit and accounting records that reflect who, what, and when information was accessed.

- Address Management — The solution must assign a client's address on the private net, and must ensure that private addresses are kept private.

- Data Encryption — Data carried on the public network must be rendered unreadable to unauthorized users on the network. The VPN solution must also generate and refresh encryption keys for the client and server.

5.2.2 Contractor-to-Company Site VPN

The connection established is 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 Internet and the DOD network. Contractors working at DOD locations that require the ability to connect to their company network, using client-side VPN software installed on their government machine, will adhere to the following guidance:

- *(NET1840: CAT III) 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.*

- *(NET1840: CAT III) 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.*

- *(NET1840: CAT III) The remote user will ensure all communication to/from the site network employs security using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

APPENDIX A. RELATED PUBLICATIONS

Government Publications

DOD Directive 8500.1, "Information Assurance (IA)," 10/24/2002

DOD Instruction 8500.2, "Information Assurance (IA) Implementation," 02/06/2003

DOD Instruction 8551.1, "Ports, Protocols, and Services Management (PPSM)," 08/13/2004

DOD CSC-STD-002-85, "DOD Password Management Guideline," 12 April 1985.

CJCSM 6510.01, "Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND) ", 25 Mar 03

DOD CM-400-260-01, “Software Requirements Specification (SRS) for the Network Management (NM) Functional Area Of The Defense Information Infrastructure (DII),” 8 July 1997.

DOD Directive Number 3020.26, Continuity of Operations (COOP) Policy and Planning, May 26, 1995.

DOD Instruction Number 3020.39, Integrated Continuity Planning for Defense Intelligence, ASD (C3I), August 3, 2001.

DOD Directive Number O-8530.1, Computer Network Defense (CND), January 8,2001.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August 1991, and Supplements 1 and 2, not dated.

NSA, "Information Systems Security Products and Services Catalog."

NSA, “Router Security Configuration Guide.”

NSA, “Switch Guide.”

ASD (NII) Memo, “Internet Protocol Version 6” (IPv6), June 9, 2003.

DISA Computing Services Security Handbook

DNS STIG

NIPRNet STIG

Secure Remote Computing STIG

Enclave Security STIG

UNIX STIG

Web Application STIG

Wireless STIG

Commercial and Other Publications

William R. Cheswick and Steven M. Bellovin. Firewalls and Internet Security, Repelling the Wily Hacker. Addison-Wesley Publishing Company, 1994.

World-Wide Web References

Network Information Center (NIC) – http://www.internic.net

Electronic Industry Association/ Telecommunications Industry Association (EIA/TIA) – http://www.eia.org

Global Engineering Documents – http://global.ihs.com

Internet Engineering Task Force (IETF) – http://ww.ietf.org

Internet Assigned Numbers Authority (IANA) – http:///www.iana.org

CISCO – http://www.cisco.com

Foundry Networks – http://www.foundrynet.com

Juniper – http://www.juniper.net

Cisco Channel Interface Processor – http://www.cisco.com

Cisco Field Notices – http://www.cisco.com/warp/public/770/index.shtml

Cisco Security Advisories – http://www.cisco.com/warp/public/707/advisory.html

Cisco White Papers Website – http://www.cisco.com/warp/public/126/index.shtml

JTF-GNO Net Defense home page – http://www.cert.org

CERT Alerts (from 1988) – http://www.cert.org/nav/alerts.html

DOD-CERT Home Page – http://www.cert.mil

NIPRNet Connection Approval Process – http://cap.nipr.mil

This page is intentionally left blank.

APPENDIX B. CJCSM AND DISA COMPUTING SERVICES SECURITY HANDBOOK REFERENCES

The references below are excerpts from *CJCSM 6510.01* and the *DISA Computing Services Security Handbook*, and are **outdated**. This section is slated for deletion do to inaccuracies. Please reference CJCSM 6510.01 and the 8500 IA controls for password and warning banner requirements.

- The following is an excerpt from *Section 3.13, Passwords*, in the *Handbook*. The excerpt is provided as an adjunct to *DISA Computing Services Security Handbook* references.

3.13 Passwords

1. General.

a. Passwords provide the identification and authentication (I&A) function required of a C2 trusted level system. However, passwords become a vulnerability rather than a protection if misused or poorly maintained.

b. Ideally, only the user and the system know a password. The IAO/NSO will issue a temporary password that the user will change on initial access to the system. Temporary passwords will meet password structure requirements and will be varied. If a user forgets a password, the IAO/NSO will have to delete the existing account and reissue a new temporary password.

c. Users must sign a receipt for their initial password. The receipt must contain an acknowledgment that the user understands the responsibility to protect the password and has received guidance on password selection (if user selected). Password receipts must be kept on file for as long as a user has access.

2. Password Structure.

a. Passwords will generally be a minimum of eight characters. The pertinent STIG will be consulted for the requirement of each operating system.

b. No words found in standard dictionaries will be used.

c. At least one upper case letter, lower case letter, numeric, and special character will be used.

d. Repeating, consecutive characters will not be used.

3. Password Maintenance. The following are minimum standards. Refer to the appropriate STIG for standards specific to the operating system.

a. Passwords must be changed every 90 days.

b. Passwords cannot be reused within 10 password changes.

c. Passwords cannot be changed more than once every 24 hours without the intervention of the IAO/NSO.

d. If software allows, set it to enforce the above rules.

e. The password file must be encrypted, if possible, and protected from unauthorized access.

4. Password Classification.

a. Passwords for unclassified but sensitive systems will be marked, "**FOR OFFICIAL USE ONLY**."

b. Passwords for classified systems, operating in the dedicated or systems high mode, will be marked, "**FOR OFFICIAL USE ONLY**."

c. Passwords for classified systems, operating in the multi-level mode, depend on what other security measures are in place. If physical security or COMSEC measures separate the levels of classification, the passwords may be marked, "**FOR OFFICIAL USE ONLY**." However, if the password is the only measure separating the levels of classification, the password must be classified to the level of that user.

5. Password Storage.

a. If it is necessary to maintain a password list, it must be kept under key lock. *Although a list of all passwords for a classified system is FOUO, it is recommended the list be stored as classified.*

b. Users are encouraged not to keep a copy of their written password, but it is often necessary to have it available. It should be protected as follows to prevent loss and to detect a compromise.

(1) Do not store the password where it is easily accessible to your computer.

(2) Do not keep the password and user ID together.

(3) Store the password in a locked drawer or cabinet. However, this is not effective if the same key opens most of the drawers in the office area.

(4) Seal the password in an envelope and sign across the seal to detect tampering.

6. Password Dissemination.

a. Passwords must be given to the user via a secure means. The user ID and password should never be transmitted, together in the clear. There is no one solution, but many possible alternatives. A risk management approach should be used and the less secure the means, the less time the password should remain active before the change. If the user is not able to change passwords, the most secure methods should be employed.

b. The ideal situation would involve the IAO/NSO personally giving the user their initial, one-time password and the user immediately changing that password.

c. Other acceptable solutions include:

(1) Sending the user ID and password by mail.

(2) Giving the user ID and password over a secure phone.

(3) Sending the user ID and password by an encrypted E-mail. The password to unencrypt will be sent by a separate message, without referencing what this password is for.

(4) Centrally managed system may predetermine default password, such as the password of the week or a list of 25 different passwords. These can be mailed to local IAO/NSO ahead of time. When an account is established centrally, the local IAO/NSO will be notified that the password for the week of the 17^{th} was used or password #12. The local IAO/NSO can then personally give the user their one-time password.

d. Other methods of disseminating passwords should be submitted to FSO for approval.

7. Password Vaults.

a. A password vault is a utility program that stores multiple passwords under a master password. This eliminates the problem of users forgetting multiple passwords or having to write them down.

b. The use of a password vault will only be considered if:

(1) Passwords are stored by a minimum of 128-bit encryption.

(2) The vendor provides a Vendor Integrity Statement. *See Section 3.23.*

(3) The IAO/NSO or IAM approves the software and use of this product is reflected in the accreditation.

3.26 CJCSM Warning Banners

1. The purpose of the warning banner is two-fold. First, it warns unauthorized users, surfing the net, that unless they are authorized they should not proceed. It is like an electronic **No Trespassing** sign that allows us to prosecute those who do trespass. Secondly, it warns both authorized and unauthorized users that they are subject to monitoring to detect unauthorized use. This provides the informed consent that again allows us to prosecute those who abuse the system.

2. The requirement for a LOGON Warning Banner was disseminated through DOD-CERT Bulletin 93-17, subject: LOGON Warning Banner for DOD Interest Computer Systems. The bulletin referenced guidance from the Deputy Assistant Secretary of Defense for Security Countermeasures and Counterintelligence (DASD/SCM/CI). Other clarifying guidance has also been distributed.

3. The banner should be installed so that it appears before a LOGON screen or before any identification of the system. An escape should also be provided to allow the individual to end the LOGON attempt (e.g., **PRESS ENTER TO LOG ON TO SYSTEM OR ESCAPE TO ABORT SESSION**). If the banner cannot be installed before the LOGON process due to the configuration of the system, install the banner as soon as possible.

4. Below is the latest version of the warning banner provided by CJCSM 6510.01 dated 15 March 2002. Previously approved versions are acceptable, but should be updated when possible.

> This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including internet access), are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system, may be monitored.
>
> Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

APPENDIX C. REQUIRED FILTERING RULES

The understanding of mutually accepted risk within the NIPRNet community seeks to provide maximum interoperability while maintaining an emphasis on security. The logic is that all participants inside the NIPRNet share a common level of risk to their systems, defined by the protections established at the NIPRNet/Internet boundary, and the minimum level of protection found at all internal enclave boundaries to the NIPRNet backbone. To mitigate this threat, DOD has established a NIPRNet ports and protocols security document. This document establishes the DOD community policy for firewall and router implementations for the NIPRNet. It will provide detailed configuration settings for known identified combinations of ports, protocols, and services (PPS). It will recommend security countermeasures for minimizing the vulnerabilities for use of risky ports, protocols, and services that are used by essential applications.

The DOD Ports and Protocol Technical Guidance is a valuable source that can be utilized in filtering traffic. The publicly accessible data is at http://www.dtic.mil/whs/directives/corres/html/85511.htm; the guide itself can be found at https://pnp.cert.smil.mil/portsandprotocols.

The following table contains guidelines for implementing filtering rules (allow, deny, or conditional) at the Enclave and Security Domain perimeters.

Compatibility with existing applications is not known; therefore, the site should perform testing on a non-production system or network prior to deployment.

A Deny-by-Default (*"deny that which is not expressly permitted")* packet filtering policy is the only approved implementation of firewalls. With this type of policy implemented, all of the services that are vital to the organization must have a filtering rule that allows entry into the network.

KEY TO TABLE ENTRIES	
Allow	Without this service the system may not be fully functional. Allow, if required. Further security controls may be necessary to adhere to local security policy.
Deny	Possible source of entry for exploitation. If absolutely necessary, submit documenting rationale and alternate protection used.
Cond	Conditional. Allow only where service is needed with controls such as source and destination IP addresses, filtering, and strong authentication. Deny if not needed.

SERVICE FILTERING GUIDE				
SERVICE	SECURITY		ACL EXAMPLES	DESCRIPTION/NOTES
	In-Bound	Out-Bound		
0.0.0.0	Deny		access-list 101 deny ip 0.0.0.0 0.255.255.255 any log	Historical Broadcast
255.255.255.255	Deny		access-list 101 deny ip host 255.255.255.255 any log	Broadcast
127.0.0.0	Deny		access-list 101 deny ip 127.0.0.0 0.255.255.255 any log	Local Host
10.0.0.0/8	Deny		access-list 101 deny ip 10.0.0.0 0.255.255.255 any log	Private Network
169.254.0.0/16	Deny		access-list 101 deny ip 169.254.0.0 0.0.255.255 any log	Link Local Networks
192.0.2.0/24	Deny		access-list 101 deny ip 192.0.2.0 0.0.0.255 any log	Test Net
192.168.0.0/16	Deny		access-list 101 deny ip 192.168.0.0 0.0.255.255 any log	Private Network
224.0.0.0/4	Deny		access-list 101 deny ip 224.0.0.0 15.255.255.255 any log	Class D - Reserved 224.0.0.0 - 239.255.255.255
240.0.0.0/5	Deny		access-list 101 deny ip 240.0.0.0 15.255.255.255 any log	Class E - Reserved 240.0.0.0 - 255.255.255.255
172.16.0.0/12	Deny		access-list 101 deny 172.16.0.0 0.15.255.255 any log	Private Network
192.0.0.192	Deny		access-list 101 deny 192.0.0.192 0.0.0.255 any log	HP Printer Default IP Address
192.0.127.0	Deny		access-list 101 deny ip 192.0.127.0 0.0.0.255 any log	IANA NS Lab
192.0.0.0/17	Deny		access-list 101 deny ip 192.0.0.0 0.0.128.0 any log	IANA - Reserved 192.0.0.0 - 192.0.127.255
1.0.0.0	Deny		access-list 101 deny ip 0.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
2.0.0.0	Deny		access-list 101 deny ip 2.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
5.0.0.0	Deny		access-list 101 deny ip 5.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
7.0.0.0	Deny		access-list 101 deny ip 7.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved

SERVICE FILTERING GUIDE				
SERVICE	**SECURITY**		**ACL EXAMPLES**	**DESCRIPTION/NOTES**
	In-Bound	**Out-Bound**		
23.0.0.0	Deny		access-list 101 deny ip 23.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
27.0.0.0	Deny		access-list 101 deny ip 27.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
31.0.0.0	Deny		access-list 101 deny ip 31.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
36.0.0.0	Deny		access-list 101 deny ip 36.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
37.0.0.0	Deny		access-list 101 deny ip 37.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
39.0.0.0	Deny		access-list 101 deny ip 39.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
42.0.0.0	Deny		access-list 101 deny ip 42.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
77.0.0.0	Deny		access-list 101 deny ip 77.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
78.0.0.0	Deny		access-list 101 deny ip 78.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
79.0.0.0	Deny		access-list 101 deny ip 79.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
92.0.0.0	Deny		access-list 101 deny ip 92.0.0.0 31.255.255.255 any log	Unallocated / IANA Reserved 92.0.0.0 - 123.255.255.255
173.0.0.0	Deny		access-list 101 deny ip 173.0.0.0 7.255.255.255 any log	Unallocated / IANA Reserved 173.0.0.0 - 180.255.255.255
180.0.0.0	Deny		access-list 101 deny ip 173.0.0.0 7.255.255.255 any log	Unallocated / IANA Reserved 180.0.0.0 - 187.255.255.255
197.0.0.0	Deny		access-list 101 deny ip 197.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved
223.0.0.0	Deny		access-list 101 deny ip 223.0.0.0 31.255.255.255 any log	Unallocated / IANA Reserved 223.0.0.0 - 254.255.255.255
255.0.0.0	Deny		access-list 101 deny ip 223.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved

BOGON LIST (30 June 2005)

<u>Private Space</u>	**10.0.0.0/8**	**172.16.0.0/12**	**192.168.0.0./16**
<u>Loopback</u>	**127.0.0.0/8**		
<u>Link Local</u>	**169.254.0.0/16**		
<u>Test Net</u>	**192.0.2.0/24**		
<u>IANA Reserved</u>	**192.0.0.0/17**		
<u>IANA NS LAB</u>	**192.0.0.0/24**		

<u>Unallocated</u>

0.0.0.0/8	***1.0.0.0/8***	***2.0.0.0/8***	***5.0.0.0/8***
7.0.0.0/8		***23.0.0.0/8***	***27.0.0.0/8***
31.0.0.0/8	***36.0.0.0/8***	***37.0.0.0/8***	***39.0.0.0/8***
42.0.0.0/8	***77.0.0.0/8***	***78.0.0.0/8***	***79.0.0.0/8***
92.0.0.0/8	***93.0.0.0/8***	***94.0.0.0/8***	***95.0.0.0/8***
96.0.0.0/8	***97.0.0.0/8***	***98.0.0.0/8***	***99.0.0.0/8***
100.0.0.0/8	***101.0.0.0/8***	***102.0.0.0/8***	***103.0.0.0/8***
104.0.0.0/8	***105.0.0.0/8***	***106.0.0.0/8***	***107.0.0.0/8***
108.0.0.0/8	***109.0.0.0/8***	***110.0.0.0/8***	***111.0.0.0/8***
112.0.0.0/8	***113.0.0.0/8***	***114.0.0.0/8***	***115.0.0.0/8***
116.0.0.0/8	***117.0.0.0/8***	***118.0.0.0/8***	***119.0.0.0/8***
120.0.0.0/8	***121.0.0.0/8***	***122.0.0.0/8***	***123.0.0.0/8***
172.0.0.0/0	***173.0.0.0/8***	***174.0.0.0/8***	***175.0.0.0/8***
176.0.0.0/8	***177.0.0.0/8***	***178.0.0.0/8***	***179.0.0.0/8***
180.0.0.0/8	***181.0.0.0/8***	***182.0.0.0/8***	***183.0.0.0/8***
184.0.0.0/8	***185.0.0.0/8***	***186.0.0.0/8***	***187.0.0.0/8***
197.0.0.0/8	***223.0.0.0/8***		
<u>Class D multicast</u>	***<u>, Class E and</u>***	***<u>Broadcast</u>***	
224.0.0.0/8	***225.0.0.0/8***	***226.0.0.0/8***	***227.0.0.0/8***
229.0.0.0/8	***230.0.0.0/8***	***231.0.0.0/8***	***232.0.0.0/8***
233.0.0.0/8	***234.0.0.0/8***	***235.0.0.0/8***	***236.0.0.0/8***
239.0.0.0/8	***240.0.0.0/8***	***241.0.0.0/8***	***242.0.0.0/8***
243.0.0.0/8	***244.0.0.0/8***	***245.0.0.0/8***	***246.0.0.0/8***
247.0.0.0/8	***248.0.0.0/8***	***249.0.0.0/8***	***250.0.0.0/8***
251.0.0.0/8	***252.0.0.0/8***	***253.0.0.0/8***	***254.0.0.0/8***
255.0.0.0/8			

References	***RFC 3330***	***RFC 1918***	***RFC 1112***
	ARIN WhoIs		

APPENDIX D. LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ACK	Acknowledge Field Significant
ACL	Access Control List
AG	Approved Gateway
AH	Authentication Header
AIS	Automated Information System
ARP	Address Resolution Protocol
AS	Autonomous Systems
AS-NII	Assistant Secretary of Defense for Networks & Information Integration
ATC	Approval to Connect
ATM	Asynchronous Transfer Mode
ATO	Authority to Operate
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
BOOTP	Boot Protocol
CAP	Connection Approval Process
CCSD	Commercial Circuit System Designator
CDP	Cisco Discovery Protocol
CEF	Cisco Express Forwarding
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIP	Channel Interface Processor (Cisco product)
CJCSM	Chairman Joint Chiefs of Staff Manual
CLI	Command Line Interface
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
COOP	Continuity Of Operations
CS	Communication Server
CSU	Channel Service Unit
DAA	Designated Approving Authority
DDoS	Distributed Denial of Service
DECC	Defense Enterprise Computing Center
DECC-D	Defense Enterprise Computing Center-Detachment
DES	Digital Encryption Standard
3DES	Triple Digital Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DID	Defense-in-Depth
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DISN	Defense Information System Network

DITSCAP	DOD Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DNS	Domain Name Service
DOD	Department of Defense
DOD-CERT	Department of Defense-Computer Emergency Response Team
DoS	Denial of Service
DSU	Data Service Unit
DTP	Dynamic Trunking Protocol
EAL	Evaluated Assurance Level
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
EIA/TIA	Electronic Industry Association/Telecommunications Industry Association
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FA	Firewall Administrator
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FPC	Flexible PIC Concentrator
FTP	File Transfer Protocol
FSO	Field Security Office
FSO	Field Security Operations
GD	General Deployment
GIG	Global Information Grid
GNOSC	Global Network Operations and Security Center
GRE	Generic Routing Encapsulation
GSA	General Services Administration
HID	Host Intrusion Detection
HP	Hewlett Packard
HTTP	Hyper Text Transfer Protocol
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IANA	Internet Assigned Number Authority
IASE	Information Assurance Support Environment
IATC	Interim Approval to Connect
IATO	Interim Authority to Operate
IAVA	Information Assurance Vulnerability Alert
IAW	In Accordance With
ICMP	Internet Control Message Protocol
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System

IEEE	Institute for Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGRP	nterior Gateway Routing Protocol
IKE	Internet Key Exchange
INFOCON	Information Operations Condition
INFOSEC	Information Security
INFOWAR	Information Warfare
IOS	Internetworking Operating System
IP	Internet Protocol
IPSEC	IP Security
IS	Information System
ISC	Internet Software Consortium
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System to Intermediate System
ISL	Inter-Switch Link
ITSDN	Integrated Tactical Strategic Data Networking
JID	Joint Intrusion Detector
JIS	Joint Interoperability System
JTF	Joint Task Force
JTFCNO	Joint Task Force Computer Network Operations
KEA	Key Exchange Algorithm
LAN	Local Area Network
LEC	Local Carrier Exchange
L2F	Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
MD5	Message-Digest Five Algorithm
MIB	Management Information Base
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRU	Maximum Receive Unit
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NA	Network Administrator
NAS	Network Access Server
NAT	Network Address Translator
NIC	Network Information Center
NIC	Network Interface Card
NID	Network Intrusion Detector
NIPRNet	(unclassified but sensitive) Network Internet Protocol Routing Network
NIST	National Institute of Standards and Technology
NM	Network Management

NMS	Network Management System
NSA	National Security Agency
NSO	Network Security Officer
NTP	Network Time Protocol
OOB	out-of-band
OS	Operating System
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PAD	Packet Assembler Disassembler
PAP	Password Authentication
PagP	Port Aggregation Protocol
PDI	Potential Discrepancy Item
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
POC	Point-of-Contact
POP	Point-of-Presence
PPP	Point-to-Point Protocol
PPS	Ports Protocols and Services
PPTP	Point-to-Point-Tunneling Protocol
PSTN	Public Switched Telephone Network
RA	Registration Authority
RADIUS	Remote Authentication Dial-in User Service
RAS	Remote Access Server
RCP	Remote Copying
RFC	Request for Comments
RIP	Routing Information Protocol
RLOGIN	Remote Login
RNOSC	Regional Network Operations and Security Center (formerly ROSC)
RPC	Remote Procedure Call
RSH	Remote Command Execution
RST	Reset the Connection
SA	System Administrator
SCAO	SIPRNet Connection Approval Office
SCP	Secure Copy Protocol
SDID	Short Description Identifer
SHTTP	Secure Hyper Text Transfer Protocol
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLIP	Serial Line Interface Protocol
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture

SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Socket Layer
STIG	Security Technical Implementation Guide
STEP	Standardized Tactical Entry Point
STP	Spanning Tree Protocol
SRS	Software Requirement Specification
SWA	Secure Web Access
SYN	Synchronize Sequence Numbers
SYSLOG	System Log
TACACS	Terminal Access Controller Access System
TCP	Transmission Control Protocol
TDY	Temporary Duty
TFTP	Trivial File Transfer Protocol
TSL	Transport Layer Security
TTY	Terminal Type
TSIG	Transaction Signatures
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
URPF	Unicast Reverse Path Forwarding
USB	Universal Serial Bus
VCTS	Vulnerability Compliance Tracking System
VLAN	Virtual Local Area Network
VMPS	VLAN Management Policy Server
VMS	Vulnerability Management System
VQP	VMPS Query Protocol
VTP	VLAN Trunking Protocol
VTY	Virtual Teletype/Terminal
WAN	Wide Area Network
WESTHEM	Western Hemisphere
WWW	World Wide Web

This page is intentionally left blank.