



NETWORK INFRASTRUCTURE
SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 7, Release 1

25 October 2007

Developed by DISA for the DoD

UNCLASSIFIED

This page is intentionally blank.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Background.....	1
1.2 Authority.....	1
1.3 Scope	2
1.4 Writing Conventions	2
1.5 Vulnerability Severity Code Definitions	2
1.6 STIG Distribution.....	3
1.7 Document Revisions.....	3
2. ENCLAVE PERIMETER.....	5
2.1 Enclave Protection Mechanisms.....	5
2.2 Network Infrastructure Diagram	7
2.3 External Connections.....	8
2.4 Leased Lines.....	8
2.5 Approved Gateway / Internet Service Provider Connectivity	9
2.6 Backdoor Connections.....	11
2.7 Network Layer Addressing.....	12
2.8 IP Address Registration.....	13
2.9 IPv4 Address Privacy	14
2.10 IPv6 Addresses	14
2.10.1 IPv6 Address Privacy.....	15
2.11 Dynamic Host Configuration Protocol version 4	16
2.12 IPv6 Autoconfiguration	16
2.12.1 Stateful Autoconfiguration DHCPv6.....	16
2.12.2 Stateless Autoconfiguration	17
2.13 Physical Security	17
3. FIREWALLS.....	19
3.1 Firewall Technologies and Weaknesses.....	19
3.1.1 Packet Filters.....	19
3.1.2 Bastion Host.....	19
3.1.3 Stateful Inspection	20
3.1.4 Firewalls with Application Awareness	20
3.1.4.1 Deep Packet Inspection	20
3.1.4.2 Application-Proxy Gateway.....	20
3.1.4.3 Hybrid Firewall Technologies.....	21
3.1.5 Dedicated Proxy Servers.....	21
3.2 Layered Firewall Architecture.....	22
3.3 Content Filtering.....	25
3.4 Perimeter Protection	26
3.5 Configuration.....	26
4. ROUTERS.....	29
4.1 Route Table Integrity.....	29

4.1.1	OSPFv2, EIGRP, RIPv2, IS-IS.....	30
4.1.2	OSPFv3.....	30
4.1.3	Protecting Exterior Routing Protocol BGP.....	31
4.2	Key Management.....	32
4.3	Securing Router Planes.....	33
4.3.1	Operating System.....	33
4.3.2	Cisco Discovery Protocol.....	33
4.3.3	Trivial Services.....	34
4.3.4	Idle Timeout Connections.....	35
4.3.5	HTTP, DHCP and FTP Server.....	35
4.3.6	BSD Remote Services.....	35
4.3.7	Bootp Server.....	36
4.3.8	IP Source Routing.....	36
4.3.9	Proxy and Gratuitous ARPs.....	36
4.3.10	Directed Broadcasts.....	37
4.3.11	ICMP Exploits.....	37
4.3.12	Logging Integrity - NTP.....	38
4.3.13	Name Server.....	39
4.3.14	SNMP Service.....	39
4.3.15	Loopback Source Address.....	39
4.3.16	IPv6 Undetermined Transport.....	40
4.3.17	IPv6 Routing Header.....	41
4.4	Ports, Protocols, and Services.....	41
4.4.1	ICMPv4 Message Types.....	42
4.4.2	ICMPv6 Message Types.....	42
4.4.3	Traceroute.....	45
4.4.4	Distributed Denial of Service (DDoS) Attacks.....	45
4.5	IPv4 Address Filtering.....	46
4.6	IPv6 Address Filtering.....	47
4.6.1	Site Local Address.....	47
4.6.2	Loopback Address.....	48
4.6.3	Unspecified Address.....	48
4.6.4	Predefined Multicast Addresses.....	48
4.6.5	IPv4-compatible IPv6 addresses.....	49
4.6.6	IPv4-mapped IPv6 Addresses.....	49
4.6.7	Unique Local Addresses.....	50
4.7	Unicast Reverse-Path Forwarding.....	50
4.7.1	IPv6 Unicast Reverse-Path Forwarding.....	51
4.8	SYN Flood Attack – Protecting Servers or LANS.....	51
4.9	SYN Flood Attack –Protecting the Router.....	53
5.	DEVICE MANAGEMENT.....	55
5.1	Vulnerability & Asset Management.....	55
5.2	Out-of-band Management (OOB).....	55
5.2.1	Console Port Access.....	56
5.2.2	Terminal Server Implementation.....	56
5.2.3	Juniper Implementation.....	56

5.2.4	WAN Implementation.....	57
5.3	In-Band Management	58
5.3.1	Secure Shell Implementation	60
5.4	Simple Network Management Protocol (SNMP).....	61
5.4.1	The IP Management Model	61
5.4.2	Network Management Security Implications	61
5.4.3	Network Management Station	63
5.5	Logistics for Configuration Loading and Maintenance.....	64
5.6	Change Management and Configuration Management.....	66
6.	AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING.....	67
6.1	AAA Implementation	67
6.2	Administrator Accounts.....	68
6.3	Emergency Account	69
6.4	Two-factor Authentication	70
6.5	Auditing.....	70
6.5.1	Syslog Server	70
7.	PASSWORDS.....	75
7.1	Password Encryption	75
7.2	Juniper Diagnostic Port Protection.....	75
8.	NETWORK INTRUSION DETECTION.....	77
8.1	Local Area Network Intrusion Detection	77
8.2	External Intrusion Detection.....	78
9.	SWITCHES AND VLANS	81
9.1	Horizontal Wiring.....	81
9.2	Virtual Local Area Networks	81
9.3	Management VLAN and VLAN 1	82
9.4	VLAN Trunking.....	82
9.5	VLAN Access and Port Authentication	83
9.5.1	Port Security.....	84
9.5.1.1	Port Security using Sticky	84
9.5.2	Port Authentication with 802.1x.....	85
9.5.3	VLAN Management Policy Server (VMPS)	87
10.	VIRTUAL PRIVATE NETWORK.....	89
10.1	Virtual Private Networks (VPN)	89
10.2	Gateway-to-Gateway VPN.....	89
10.2.1	SIPRNet Gateway-to-Gateway Tunnels	91
10.3	Host-to-Gateway VPN.....	93
10.3.1	Layer 2 Tunneling Protocols.....	94
10.3.2	Transport Layer Tunnels.....	96
10.3.3	Contractor-to-Company Site VPN	97
10.4	Host-to-Host VPN	97
11.	IPV6 TRANSITION MECHANISMS	99

11.1	Dual Stack for IPv6 Transition.....	99
11.2	Split Domain Enterprise Architecture	101
11.3	IPv6 Encapsulation for IPv6 Transition	104
11.3.1	Enclave Perimeter employing VPN Tunnel in Non-Dual Stack Architecture	105
11.3.2	IPv6 Automatic Tunnels	107
11.3.2.1	Intra-Site Automatic Tunneling Protocol (ISATAP)	107
11.3.2.2	Tunnel Broker	108
11.3.2.3	6to4 Tunnels.....	109
11.3.2.4	Teredo.....	109
11.4	IPv6 Protocol Translation for IPv6 Transition.....	110
11.4.1	NAT-PT Architecture	111
APPENDIX A. RELATED PUBLICATIONS		113
APPENDIX B. FILE EXTENSIONS		119
APPENDIX C. BOGON LIST		121
APPENDIX D. LIST OF ACRONYMS.....		123
APPENDIX E. IPV6 ADDRESSES.....		129
APPENDIX F. VULNERABILITY UPDATES		131

LIST OF TABLES

Table 1-1. Vulnerability Severity Code Definitions	2
Table 2-1. Well-Known IPv6 Address.....	15
Table 4-1. ICMPv6 Message Types.....	44
Table 6-1. Authentication Parameters.....	68
Table 6-2. Logging.....	71

TABLE OF FIGURES

Figure 2-1. Enclave Network Architecture.....	6
Figure 2-2. Approved Gateway Architecture.....	10
Figure 2-3. DoD Backdoor Architecture	12
Figure 3-1. Firewall design with DMZ and Restricted Segments	23
Figure 4-1-A. Attacker Injecting False Route Advertisements	29
Figure 4-1-B. Signature Creation.....	30
Figure 4-2. DoD Enclave Authentication to Customer Edge (CE).....	32
Figure 5-1. Device Management.....	59
Figure 8-1. External IDS.....	79
Figure 11-1. Coexistence IPv4 and IPv6	99
Figure 11-2-A. Dual Stack Architecture and a Single CE Node	100
Figure 11-2-B. Dual Stack Architecture and Two CE Nodes.....	101
Figure 11-3. Split Domain Architecture	103
Figure 11-4. GRE Tunnel in Non-Dual Stack Architecture	105
Figure 11-5. VPN Tunnel in Non-Dual Stack Architecture	106
Figure 11-6. ISATAP Architecture.....	108
Figure 11-7. 6to4 Relay Architecture	109
Figure 11-8. NAT-PT Architecture.....	111

This page is intentionally blank.

SUMMARY OF CHANGES

GENERAL CHANGES:

The previous release was Version 6, Release 4, dated 16 December 2005.

This release concentrates on meeting the following objectives:

- 1) Integrate vulnerability discussion for Native IPv6 in the existing document where those vulnerabilities are defined in IPv4. Create IPv6 Transition section for vulnerabilities as they relate to technologies specific to the transition and the Dual Stack environment.
- 2) Establish enclave lines of defenses and boundaries including diagrams to assist the reader with DMZ designs, OOB remote management and Server placement.
- 3) Provide policy on tunneling C2 and non-C2 data.
- 4) Create a device management section with clearer policies.
- 5) Strengthen the firewall section and bring it current with NIAP medium protection profiles.
- 6) Remove redundancies from the router, switch, and firewall sections and reorganize the document.
- 7) Modified Appendix C. Due to the monthly IANA updates of the Bogon list the STIG Appendix provided false Bogon addresses leading to potential registered addresses being blocked.
- 8) Remote Access Server requirements can now be found in the Secure Remote Computing STIG.

HOW THIS STIG IS ORGANIZED AND CHANGED:

The following bullets describe detail changes that have occurred in each section of the Network STIG v7.0. Approximately 59 vulnerabilities were removed as a result of duplication found in the previous STIGs. Version 7 of the STIG had approximately 47 vulnerabilities modified to strengthen the description of the vulnerability. One hundred-thirty-three new vulnerabilities were created that focused in the weakest areas in previous STIGs. These areas were primarily the firewall and VPN section. Of the 133 new vulnerabilities, approximately 45 were in support of IPv6.

Section 1 Introduction

Minor modifications were added.

Section 2 Enclave

Much of Section 2 was rewritten, providing more detail.

A new diagram expands the scope of lines of defenses within the enclave. DMZ architecture is described with public services being segregated on separate segments from internal restricted LAN segments. All DMZ discussion in this STIG is considered enclave DMZ as defined in the PPS CAL boundary.

A diagram is added to support discussion of unapproved routing advertisements from Approved Gateways.

Defined Ports Protocols and Services and Joint Intrusion Detection Sensor requirements for Approved Gateways.

A diagram is added to describe and better define backdoor connections. Backdoor connections are different by STIG definition than ISP and Approved Gateways.

Concerns of privacy with IPv6 addressing are addressed in section 2.10.

Section 2.12 details DHCPv6 stateful and stateless autoconfiguration.

Section 3 Firewalls

The Firewall discussion is moved to Section 3 and rewritten to assist the users in understanding the types of firewalls available and identify their weaknesses. Centered much of the requirements based on NIAP guidelines for packet filter firewalls, application level firewalls and IPv6 firewalls. Many new vulnerability checks are added for alarms, etc.

The device management redundancy has been removed.

Section 4 Routers

Route Table Integrity Section 4.1 is rewritten and diagrams are added. OSPFv3 for IPv6 is added and BGP is segregated and expanded.

A new Key Management section 4.2 is added.

Many router-hardening practices were scattered over the previous STIG. This content is reorganized to have these grouped together in section 4.3.

IPv6 Router Header packet and Undetermined Transport Guidance is added to the section to harden the router.

ICMP filters and PPS discussions were in several areas of previous STIG. These are centrally located for improved structure. Guidance is added for IPv6 ICMPv6 filtering.

In section 4.5 IP Address filtering is consolidated. Adding new IPv6 route filters to the section to harden the threats from the IPv6 protocol.

The device management redundancy is removed.

Section 5 Device Management

A new Device Management section has been created and expanded in detail on out-of-band network management. Details include console access, juniper implementation, terminal server, remote Out of band and remote in-band management. Diagrams are provided to support discussion.

Section 6 Authentication

A new Authentication section has been created. Reused existing discussion and added some detail on two-factor authentication to help clear up confusions.

Section 7 Passwords

New section with existing discussion

Section 8 IDS

No changes

Section 9 Switches

The device management redundancy has been removed.

Added Sticky Port Security Guidance

Section 10 Tunneled Networks

Revised section and expands significantly on Gateway-to-Gateway tunnels and tunneling C2 and non-C2 traffic over the DISN core.

Section 11 IPv6 Transition Mechanisms

This new section details the transition mechanisms available during an IPv6 transition to Native IPv6. Native IPv6 is integrated throughout the STIG in the appropriate sections. This section briefly discusses the dual stack environment and leads into encapsulation where the focus becomes the tunnel end-points termination, visibility to sensors and filtering protocol 41. The section then begins to expand on tunnel types in subsections, manual and automated tunnels. The last topic in the transition section is a discussion of various translation mechanisms and their vulnerabilities.

This page is intentionally blank.

1. INTRODUCTION

1.1 Background

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 Implementation 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.

The Network Infrastructure STIG 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.

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.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The IAO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

The JTF-GNO has also established requirements (i.e., timelines), for training, verification, installation, and progress reporting. These guidelines can be found on their web site: <https://www.jtfgno.mil>. Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback to the JTF-GNO is encouraged. The JTF-GNO may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

1.3 Scope

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), Network Security Officers (NSO), and System Administrators (SAs) with configuring and maintaining security controls.

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**” indicates 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.

Each policy bullet includes the STIG Identifier (STIGID) in parentheses that precedes the policy text and references the corresponding vulnerability check in the SRR Checklist and Vulnerability Management System (VMS). An example of this will be as follows: "(*G111: CAT II*).” If the item presently does not have an STIGID, or the STIGID is being developed, it will contain a preliminary severity code and "N/A" (i.e., "[*N/A: CAT III*]"). Throughout the document accountability is directed to the IAO to “ensure” a task is carried out or monitored. These tasks may be carried out by the IAO or delegated to someone else as a responsibility or duty.

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. All reasonable attempts to meet this criterion will be made.

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 has a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.

Table 1-1. Vulnerability Severity Code Definitions

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 blank.

2. ENCLAVE PERIMETER

An enclave is a computing environment under the control of a single authority with personnel and physical security measures.

2.1 Enclave Protection Mechanisms

Controlling the flow of network traffic between networks employing differing security postures is required. By using Defense-in-Depth practices; firewalls, routers, Intrusion Detection System, Intrusion Prevention System (IDS/IPS), encryption technology and various other security devices and software combine to form layers of solutions within and among IT assets. 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. The enclave or system owner will identify security domain requirements in the Accreditation documentation (e.g. SSAA) System Security Authorization Agreement or the emerging DIACAP process. Procedures outlined in the *DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP)*, lay out the process for the enclave security architecture as they are applied to specific requirements. Each SSAA will include a description of the architectural implementation of the security requirements identified in this STIG. As the transition from DITSCAP to DoD Information Assurance Certification and Accreditation Process (DIACAP) nears completion, new DIACAP requirements will need to be met as replacement of the DITSCAP requirements. When the process is completed requirements will be found in new versions of the Network Checklist.

The FSO STIGs and the review process provide the specifications, standards, and inspections for each of the key enclave components.

The diagram below identifies architecture of many components that could make up an enclave. The minimum required components are briefly discussed here and depending of the deployment of components the security policy can change with additional requirements. The packet filtering router provides firewall features as the first line of defense securing at layer 3 of the Open Systems Interconnection (OSI) model. The downstream firewall provides stateful inspection and application levels of security. A Demilitarized Zone (DMZ) is defined and required by all medium robust DoD networks as documented in 8500.2. Sensors should be strategically placed to monitor traditional and wireless traffic. If the enclave has an Approved Gateway (AG) than an external IDS will be required. Additional components in the diagram may be required pending on the design of the enclave, review appropriate STIGs for details. It is not the intention of the diagram to define a standard architecture and DMZ solution.

Management of remote locations is necessary for many network operation centers within DoD. A private Wide Area Network (WAN) connection can be used with security measures in place such as an additional firewall to extend the out-of-band (OOB) network. This is one example of how this can be accomplished and is similar to some best practice blue prints. Further discussion and requirements are defined further in the STIG under their appropriate sections.

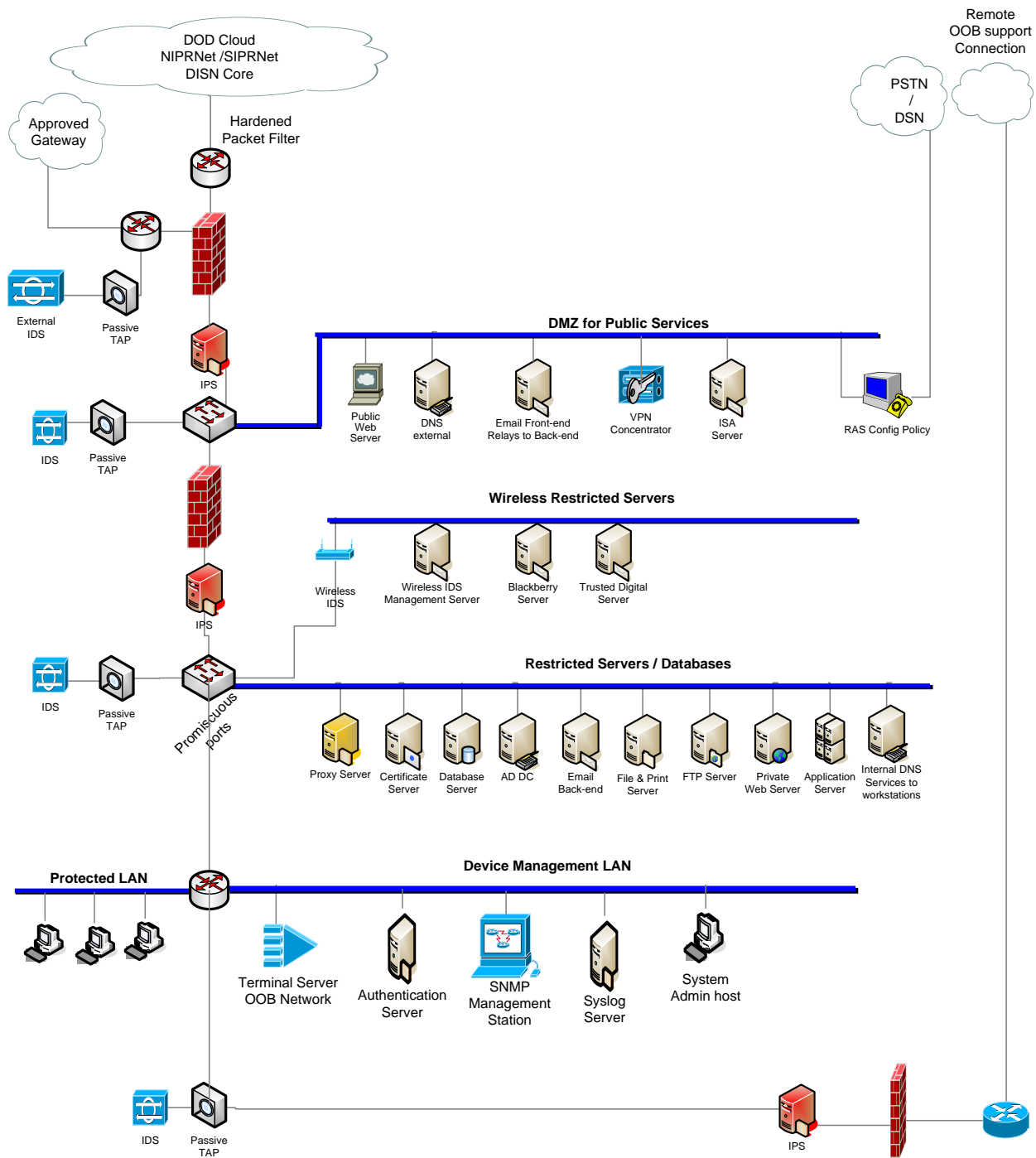


Figure 2-1. Enclave Network Architecture

The Diagram is not intended as a design guide or specific requirement for an enclave. Its purpose is to illustrate Network Perimeter Defense using hardened packet filter (perimeter router) and firewall positioning. The DMZ and restricted LANs are to help illustrate some best practices. Boundaries defined in the Ports, Protocols, and Services (PPS) Category Assignment List (CAL)

should be considered. Enclaves providing outside services will have external DMZ requirements defined in PPS CAL boundaries 9 and 10 and possibly 3 and 4.

This diagram is not intended to provide significant detail such as multiple firewalls and defense in depth practice that is usually found between the DMZ for Public Services and the Enclave DMZ. Network Test Access Ports (TAP) should be considered in network design where not defined. Taps can create a monitoring access port between any two network devices, including switches, routers, firewalls, and more. Taps can function as an access port for any monitoring device used to collect in-line data. Protocol analyzers, RMON probes, intrusion detection systems, and other management and security solutions are all commonly connected to the network via Taps.

Restricted LAN segments provide client services and backend servers such as internal DNS with split DNS architecture, backend mail servers, Active Directory Domain Controller (AD DC), file and print servers, FTP, private HTTP servers and various proxies. These services are generally found in protecting the enclave defined in PPS CAL boundary 11 and 12 and could be located in an Enclave DMZ.

The diagram also illustrates multiple restricted segments that are not security requirements but could be considered as design preferences or are hardware driven requirements. This diagram shows a Wireless IDS (WIDS) and a wireless LAN segment separated from the traditional internal DMZ servers.

This diagram does not indicate IDS requirements that may be identified in other OS STIGs such as Host- Based IDS (HIDS). Refer to the appropriate STIGs for particular IDS requirements for each server identified. More IDS requirements may be required than identified in this diagram.

PPS Boundary Descriptions mentioned:

- PPS Boundary 3 - External to DoD DMZ
- PPS Boundary 4 - DoD DMZ to External
- PPS Boundary 9 - DoD Network to Enclave DMZ
- PPS Boundary 10 - Enclave DMZ to DoD Network
- PPS Boundary 11 - Enclave DMZ to Enclave
- PPS Boundary 12 - Enclave to Enclave DMZ

2.2 Network Infrastructure Diagram

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 (e.g., 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.*

2.3 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 such as the Defense Information System Network (DISN), 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 unacceptable risk to the network. Every site must have a security policy to address filtering of the traffic to and from those connections. This documentation along with diagrams of the network topology is required to be submitted to the Connection Approval Process (CAP) for approval to connect to the Systems/Network Approval Process for NIPRNet or SIPRNet. Depending on the command, service, or activity, additional approvals may be required.

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

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

2.4 Leased Lines

DoD leased lines carry an aggregate of sensitive and non-sensitive data; therefore unauthorized access must be restricted. Leased and dedicated circuits from local exchange carrier (LEC), channel service units (CSU), data service units (DSU) and demarcation points (DEMARC) will

reside in a secured area as defined in the Traditional Security STIG. These devices should be secured at a minimum in a controlled access room or a locked closet.

- *(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.*

2.5 Approved Gateway / Internet Service Provider Connectivity

An AG is any external connection from a DoD NIPRNet enclave to an Internet Service Provider (ISP), or network owned by a contractor, or non-DoD federal agency that has been approved.

NIPRNet enclave connections to contractor or non-DoD federal agency networks must be approved by the Office of the Secretary Defense (OSD).

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.

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

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. Regardless of protocol used, no protocol will redistribute routes into the AG, no neighbors will be defined as peer routers from an AS belonging to any AG. The only method to be used to reach the AG will be through a static route. Unsolicited traffic that may inadvertently attempt to enter the NIPRNet by traversing the enclave's premise router can be avoided by not redistributing NIPRNet routes into the AG.

All AG connections will have an external IDS installed and implemented in front of the premise or border router and must be monitored by the certified Computer Network Defense Service Provider (CNDSP).

The enclave perimeter requirement for filtering will include Joint Task Force Global Network Operations (JTF-GNO) and Ports, Protocols and Services (PPS) Category Assignment List

(CAL) filtering rules. Monitoring traffic will be enforced for any traffic from the AG. All traffic entering the enclave from the AG must enter through the firewall and be monitored by internal IDS. All traffic leaving the enclave, regardless of the destination--AG or NIPRNet addresses, will be filtered by the premise router's egress filter to verify that the source IP address belongs to the enclave. PPS CAL: <http://iase.disa.mil/ports/index.html>

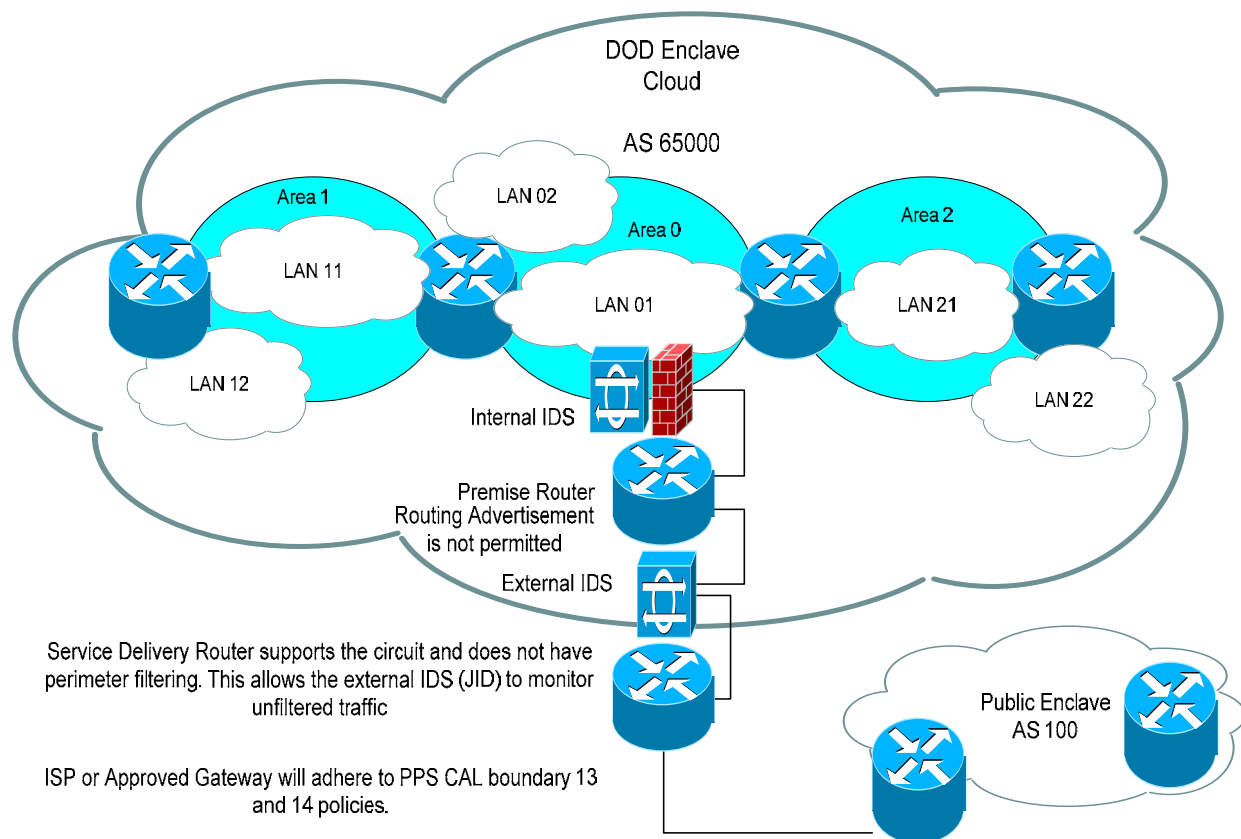


Figure 2-2. Approved Gateway Architecture

- (NET0160: CAT I) The IAM will ensure 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. A static route is the only acceptable route to an AG.

- *(NET0166: CAT III) The IAO/NSO will ensure the AG network service provider IP addresses are not redistributed into or advertised to the NIPRNet or any router belonging to any other Autonomous System (AS) i.e. to another AG device in another AS.*
- *(NET0167: CAT II) The IAO/NSO will ensure the route to the AG network adheres to the PPS CAL boundary 13 and 14 policies and is in compliance with all perimeter filtering defined in the perimeter and router sections of the Network STIG.*
- *(NET0168: CAT II) If the site has a non-DoD external connection (AG), the IAO/NSO will ensure that the external NIDS is located between the site's AG (Service Delivery Router) and the premise router.*

2.6 Backdoor Connections

The term “backdoor connection” is used to refer to a connection between two customer sites (DoD Enclaves) that do not traverse the provider’s network, in this case, the Defense Information System Network (DISN). Routes over this connection are called “backdoor routes”. Without taking the proper safeguard steps, this connection could impose security risks to either site. For example, as a result of connection availability or routing protocol administrative distances (i.e., the backdoor route is more favorable), it is possible that traffic destined for other networks from site B’s network and vice versa could pass through Site A’s premise router. It is also possible that traffic from Site B’s network could be destined for Site A’s network. In either case, the premise router external interface providing the backdoor connection must have the same ingress filtering applied as an external interface providing a connection to the NIPRNet, SIPRNet, or ISP.

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.

- *(NET0170: CAT II) The IAO/NSO will ensure no backdoor connections exist between the site's secured private network and the NIPRNet, SIPRNet, or other external DoD networks unless approved by the DAA and the SCAO.*

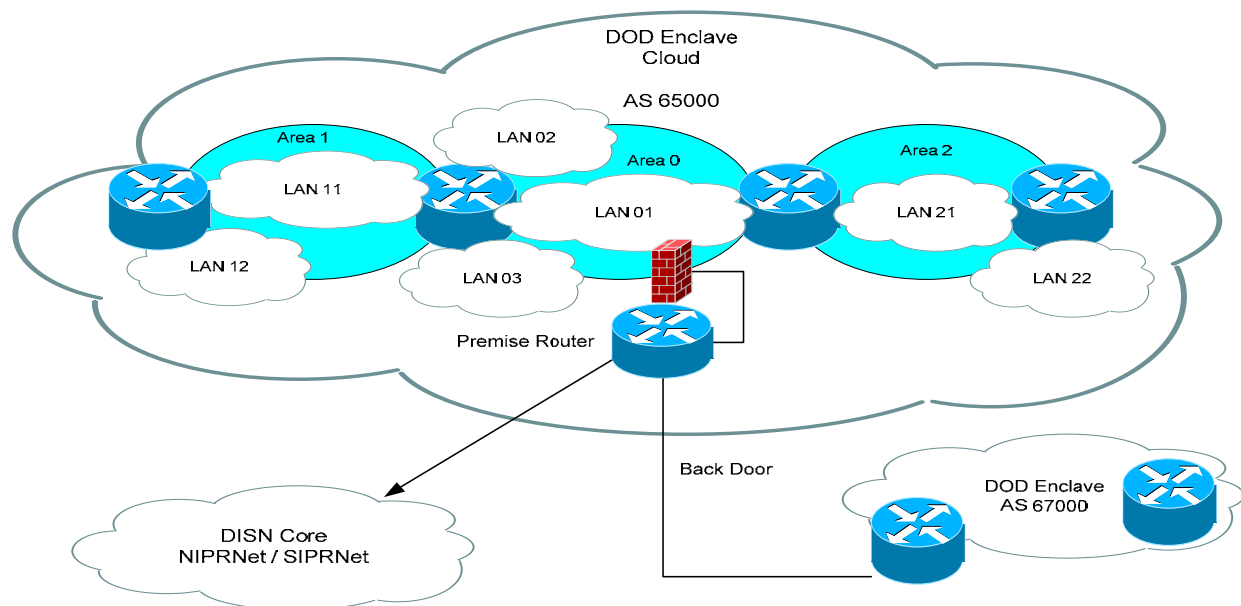


Figure 2-3. DoD Backdoor Architecture

2.7 Network Layer Addressing

The method by which Cooperating Enclaves exchange IPv6 traffic must be approved in accordance with the DISN connection approval process to ensure compliance with IA policies. Multiple certification and accreditation authorities may be involved in Milestone Objective (MO2) established by DoD IPv6 Transition Office (DITO). MO2 permits applications to test IPv6 specific end-to-end capabilities and routing schema efficiencies. Limiting operation to within DoD, and only at approved locations, reduces risk to IA and operational impacts on existing IPv4 networks. The following Enclave network system security components will require examination and modification for MO2:

- Network Protection: Intrusion Detection System (IDS) scanners, configuration and network management, auditing and logging
- Perimeter Security: firewalls and web proxies
- Host Security: host IDS and host filters
- Data Protection: Virtual Private Network (VPN) and Internet Protocol Security (IPsec) components
- Transport: edge routers and switches
- Configuration: Domain Name Service (DNS), NAT, Access Control List (ACL), Ports, Protocols, and Services (PPS)
- Infrastructure and Services: Dynamic Host Configuration Protocol (DHCP), DNS, network IDS, Network Time Protocol (NTP)

The following existing network system security components will NOT require examination and modification for MO2:

- Assurance Devices: HAIPE, encryptors
- Transport: core routers and switches

MO2 will employ a phased approach based on six (6) architectures, discussed in IPv6 Transition Mechanisms section.

To ensure a successful migration to IPv6, there will be a transitional period when IPv4 and IPv6 are used simultaneously to ensure network connectivity. This version of the Network Infrastructure STIG details vulnerability and mitigation for IPv4 and IPv6 during the DoD transition to IPv6.

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

2.8 IP Address Registration

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

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

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

Using RFC1918 addresses and NAT on the SIPRNet is prohibited, and if implemented requires DSAWG approval.

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

2.9 IPv4 Address Privacy

Using the private addressing scheme in accordance with RFC 1918 will require an organization to use Network Address Translation (NAT) for global access. NAT works well with the implementation of RFC 1918 addressing scheme, it also has the privacy benefit of hiding real internal addresses.

- *(NET0190: CAT III) The IAO/NSO will ensure IPv4 real addresses within the enclave are not revealed outside the enclave by implementing NAT on the firewall or the premise 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.

2.10 IPv6 Addresses

An IPv6 address contains 128 bits consisting of two 64 bit parts. The left most 64 bits contains the network part (prefix) and the right most 64 bits contain the host part (interface identifier). The network part is commonly called the prefix and the host part is identified as the interface identifier. The structure of the IPv6 address space is defined in RFC 3513.

Network Prefix		Interface Identifier	
0	63	64	128

IPv6 addresses are represented in eight hex groups of 4 hex decimals each, separated by colons. Each group contains sixteen binary bits. Below is an example of an IPv6 address in hexadecimal format. The four leftmost groups contain the network prefix and the remaining four rightmost groups of hex digits contain the interface identifier.

2001:0db8:0000:0000:0000:0000:0000:0001

The previous IPv6 address has a run of zeros and can be written as described below.

2001:db8:0:0:0:0:0:1

The IPv6 address has a run of zeros and also can be represented as described below. In IPv6 leading zeros can be omitted and a run of zeros can be replaced with a double colon.

2001:db8::0001

The text representation of IPv6 address prefixes is similar to the way IPv4 addresses prefixes are written in Classless Interdomain Routing (CIDR) notation. An IPv6 address prefix is represented by the notation: ipv6-address / prefix-length. Prefix notation is used to designate how many bits are used for the network part. A /48 is a common network allocation for a large network. The left most 48 bits would identify the network prefix. The remaining would be used for the hosts.

Examples:

2001:0db8:0000::/48 or

2001:db8::/48

Appendix E contains a dated IANA IPv6 address allocation for a quick reference. For current IPv6 allocations visit the IANA web site identified in the Appendix E. Listed in the following table are some common IPv6 addresses and some address that have specific security guidance found in this STIG.

Address Assignment	Address Prefix
Unspecified	::/128
Loopback [RFC 2460]	::1/128
IPv4-compatible IPv6 address [Deprecated by RFC 4291]	::/96
IPv4-mapped IPv6 address	::ffff/96
Unicast Global Address [RFC 3513]	2000::/3
Initial Global IPv6 Internet address space [RFC 3056]	2001::/16
6bone testing (retired, do not use) [RFC 2471]	3ffe::/16
Unique Local Unicast Address (ULA) [RFC 4193]	fc00::/7
Link Local Address [RFC 3513]	fe80::/10
Site Local Address [RFC 3879]	fec0::/10
Multicast Address [RFC 3513]	ff00::/8

Table 2-1. Well-Known IPv6 Address

2.10.1 IPv6 Address Privacy

The DoD Network Information Center (NIC) will assign blocks of IPv6 network addressees, to local administrators. The IPv6 address, as currently defined, consists of 64 bits of network number and 64 bits of host number. The large address space of IPv6 makes scanning impractical, but attackers can guess important router addresses by assuming that the obvious addresses would be chosen. Avoid assigning easily guessed addresses such as 2001:db8::1, ::2, ::10, ::20, ::30, and etc., for network device interfaces. It is recommended that you devise a scheme for assigning hard to guess addresses for the enclave network devices. Those concerned with privacy issues should note that 64 bits makes a large enough field to maintain excellent privacy for the enclave.

IETF's IPNG working group has recommended that the address block given to a single edge network, which may be recursively, subnetted be a 48-bit prefix. This gives each such network 2^{16} (65,536) subnet numbers to use in routing. A /48 prefix under the 001 Global Unicast Address prefix contains 45 variable bits. That is, the number of available prefixes is 2 to the power 45 or about 35 trillion (35,184,372,088,832).

- *(NET0196: CAT III) The IA0/NSO will ensure a devised hard to guess IPv6 scheme is implemented throughout the infrastructure.*

2.11 Dynamic Host Configuration Protocol version 4

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 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 any DHCP server used within SIPRNet infrastructure is configured with a lease duration time of 30 days or more.*

2.12 IPv6 Autoconfiguration

IPv6 offers two mechanisms for a client to receive an IPv6 address. RFC 3315 documents the standards for DHCPv6 stateful autoconfiguration and RFC 2462 documents the standards for stateless autoconfiguration.

2.12.1 Stateful Autoconfiguration DHCPv6

Currently, many vendors are not prepared for DHCPv6 stateful autoconfiguration, thus there are very few implementations of it. DHCPv6 is a completely separate protocol than DHCPv4. Unlike IPv4 DHCPDISCOVER use of the unspecified address 0.0.0.0 with a broadcast address, these messages are sent with a FF02::1:2 (well-known DHCPv6 all-DHCPv6-Relays-and-Servers) via IPv6 support of link-local autoconfiguration. There is also DHCPv6-Prefix Delegation that allows nodes to request not just an address, but also the entire prefix. DHCPv6-PD is primarily used by routers. Stateful autoconfiguration offers the best auditing capabilities due to the logs being centralized at the DHCP server and will become the preferred implementation.

2.12.2 Stateless Autoconfiguration

Stateless autoconfiguration requires no manual configuration of hosts and minimum configuration, if any, of routers to advertise the routing prefix. The stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers. Routers advertise prefixes that identify the subnet associated with a link, while hosts generate an interface identifier that uniquely identifies an interface on a subnet combining the two forms an address. In the absence of routers, a host can only generate link-local addresses. However, link-local addresses are sufficient for allowing communication among nodes attached to the same link.

One of the design goals of stateless autoconfiguration was giving system administrators the ability to specify whether stateless autoconfiguration, stateful autoconfiguration, or both should be used. Router Advertisements include flags specifying which mechanisms a host should use.

The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages.

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

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

- *(NET0201: CAT II) The IAQ/NSO will ensure all external interfaces on Premise, AG, and Backdoor have router advertisements suppressed.*

2.13 Physical Security

A secure communications environment is necessary to protect the enclave from physical threats. Cabinets, closets, and rooms need to meet the traditional security guidance.

- *(NET0210: CAT II) The IAQ/NSO will ensure all network devices (i.e., IDS, routers, RAS, NAS, firewalls, etc.) are located in a secure room with limited access.*

This page is intentionally blank.

3. FIREWALLS

3.1 Firewall Technologies and Weaknesses

The industry has engineered many firewall platforms over the course of the Internet creation and expansion as an attempt to provide customers with tools to protect their intranet. The sections in 3.1 identify and help the reader understand the weaknesses in many solutions available in today's market. The following firewall discussion ultimately defines the firewall requirements for DoD enclaves, where many are derived by National Information Assurance Partnership (NIAP) medium robustness standards.

3.1.1 Packet Filters

A packet filter firewall is a routing device that provides access control for system addresses and communication sessions via a rule-set. The packet filter operates at layer 3 and filters on source and destination addresses, and communication session parameters such as source and destination ports. 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 are allowed through the firewall will be configured IAW DoD Instruction 8551.1. 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. Packet filtering alone does not achieve the enclave robust protection requirements due to its limitations in examining upper-layer data and limitations in providing detailed log data. Packet filtering firewalls allow a direct connection to be made between the two endpoints. Although this type of packet screening is configured to allow or deny traffic between two networks, the client/server model is never broken. Packet filtering firewalls are an all-or-nothing approach. If ports are open, they are open to all traffic passing through that port, which in effect leaves a security hole in your network. There are three common exploits to which packet filtering firewalls are susceptible. These are IP spoofing, buffer overruns, and ICMP tunneling. *IP spoofing* is sending your data and faking a source address that the firewall will trust. *Buffer overruns* typically occur when data sizes inside a buffer exceed what was allotted. *ICMP tunneling* allows a hacker to insert data into a legitimate ICMP packet.

3.1.2 Bastion Host

The firewall can be configured as a "Bastion Host", that is, a host that is minimally configured (containing only necessary software/services) and carefully managed to be as secure as possible. This architecture is sometimes referred to as a Screened Host. The Screened Host is typically located on the trusted network, protected from the untrusted network by a packet filtering router. All traffic coming in through the packet filtering router is directed to the screened host. Outbound traffic may or may not be directed to the screened host. This type of firewall is most often software based and runs on a general-purpose computer that is running a secure version of

the operating system. Security is usually implemented at the application level. The most common threat to the Bastion Host is to the operating system that is not hardened.

3.1.3 Stateful Inspection

Stateful Inspection firewalls incorporate added awareness to firewalls at layer 4 and accommodate features in the TCP/IP protocol suite.

When a TCP connection is established a source port and a destination port pair become part of the session allowing the source system to receive information from the destination system. The client source port should be some port number greater than 1023 and less than 16384. Stateful Inspection firewalls solve the vulnerability of permitting all the high numbered ports by creating a state table containing the outbound TCP connections and their associated high numbered port. The directory known as the state table is then used to validate inbound traffic. Entries are created only for those TCP connections or UDP streams that satisfy a defined security policy. Stateful Inspection examines only the headers of data packets, which contain information such as the sender's and receivers' addresses and the type of protocol and data contained in the packet payload. As a result, Stateful Inspection technology cannot tell the difference between valid and harmful data. Like packet filtering, stateful packet inspection does not break the client/server model and therefore allows a direct connection to be made between the two endpoints.

3.1.4 Firewalls with Application Awareness

Recent advances in network infrastructure engineering and information security have resulted in a blurring of the lines that differentiates the various firewall platforms. Deep Packet Inspection (DPI), Application-Proxy Gateway and Hybrid firewall technology are all catchy terms used in the information technology industry for firewall technology that uses stateful inspection, proxies, and with some IDS signatures and application protocol anomaly detection rules.

3.1.4.1 Deep Packet Inspection

Firewalls using deep packet inspection also operate at layer 4 of the OSI model with added enhancements to Stateful Inspection technology.

Attacks can traverse a traditional stateful firewall even if the firewall is deployed and working as it should be. By adding application-oriented checking logic into processing modules, essentially merging IDS signatures into the firewall traffic-processing engines of products the firewall industry increased the depth of protection against worms, trojans, email viruses, and exploits against software vulnerabilities. Deep Packet Inspection uses an Attack Object Database to store protocol anomalies and attack patterns (sometimes referred to as signatures), grouping them by protocol and security level (severity). Packet processing is typically described as performing application level checks as well as stateful inspection. The primary limitation of the technology is that it generally cannot detect threats that require many packets to transmit across the Internet.

3.1.4.2 Application-Proxy Gateway

Application-Proxy Gateway firewalls are advanced firewalls that combine lower layer access control with upper layer (Layer 7 Application Layer) functionality.

In an application-proxy gateway, two TCP connections are established: one between the packet source and the firewall, another between the firewall and the packet destination. Application proxies intercept arriving packets on behalf of the destination, examine application payload, and then relay permitted packets to the destination. The technology of application-proxy gateway does not require network layer routes between the firewall interfaces. The firewall software performs the routing; meaning packets that traverse the firewall must do so under software control. Proxy implementations can offer very granular application-level control such as blocking file transfers involving filenames ending in .exe. Advantages also include capabilities to enforce user authentication, hardware or software token authentication, source address authentication, and biometric authentication. Due to full packet awareness application-proxy gateways can degrade high-bandwidth or real-time solutions. These gateways also tend to be limited for new applications and protocols and can become capable of tunneling the new applications in a vendor generic proxy agent. These generic proxy-agents tend to negate many strengths of the application-proxy gateway.

3.1.4.3 Hybrid Firewall Technologies

To provide the best of both worlds, many firewalls are actually hybrids that combine stateful inspection and application proxy methods. Many Application-Proxy Gateway firewall vendors have implemented basic packet filter functionality in order to provide better support for UDP (User Datagram) based applications. Likewise, many packet filter or Stateful Inspection packet filter firewall vendors have implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewall vendors implement application proxies to provide improved network traffic logging and user authentication in their firewalls.

3.1.5 Dedicated Proxy Servers

Dedicated proxy servers differ from application-proxy gateway firewalls in that they retain proxy control of traffic but they do not contain firewall capability. They are typically deployed behind traditional firewall platforms for this reason. In typical use, a main firewall might accept inbound traffic; determine which application is being targeted, and then hand off the traffic to the appropriate proxy server, (e.g., an email proxy server). The proxy server typically would perform filtering or logging operations on the traffic and then forward it to internal systems. A proxy server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery. An example of this would be an HTTP proxy deployed behind the firewall; users would need to connect to this proxy en route to connecting to external web servers. Typically, dedicated proxy servers are used to decrease the work load on the firewall and to perform more specialized filtering and logging that otherwise might be difficult to perform on the firewall itself.

As with application-proxy gateway firewalls, dedicated proxies allow an organization to enforce user authentication requirements as well as other filtering and logging on any traffic that traverses the proxy server. The implications are that an organization can restrict outbound traffic to certain locations or could examine all outbound email for viruses or restrict internal users from writing to the organizations web server. Security experts have stated that most security problems occur from within an organization; proxy servers can assist in foiling internally based attacks or

malicious behavior. At the same time, filtering outbound traffic will place a heavier load on the firewall. Dedicated proxy servers are useful for web and email content scanning, including the following:

- Java applet or application filtering (signed versus unsigned or universal)
- ActiveX® control filtering (signed versus unsigned or universal)
- JavaScript filtering
- Blocking specific Multipurpose Internet Multimedia Extensions (MIME) types for example, .application/msword for Microsoft® Word documents (see Appendix B File Extensions for suggestions for specific types)
- Virus scanning and removal
- Macro virus scanning, filtering, and removal
- Application-specific commands, for example, blocking the HTTP .delete command
- User- specific controls, including blocking certain content types for certain users

3.2 Layered Firewall Architecture

A packet filtering firewall such as a customer premise edge router must be implemented to filter traffic from external networks such as the NIPRNet, SIPRNet and Internet. This premise router is the first line of defense in a defense-in-depth firewall solution. The premise router can block certain attacks, filter PPS CAL red ports and protocols prior to filtering operations at higher layers of the OSI stack by other firewall technologies.

Following DoD Instruction 8500.2, a DMZ is required for confidentiality levels of High and Medium identified as classified and sensitive domain respectively. A DMZ is created between two policy-enforcing components such as two or more firewall components existing in an environment or off a third firewall interface. Hubs should never be used in a DMZ environment because they allow any device connected to them to see all the network traffic destined and originating from any other device connected to the same hub.

Network switches are components that can be found in a DMZ environment to provide connectivity points making up a defense-in-depth architecture. Unlike hubs, systems that connect to a switch cannot eavesdrop on each other when switches are in use. Switches are useful for implementing DMZ environments.

A firewall can be placed at several locations to provide protection from attacks. Each implementation will differ depending on several 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 (LAN to LAN). When the main firewall is located behind the premise router the DMZ is created. There are many variations in firewall designs and figure 3-2 is not a recommendation, but a reference to the discussion in this guide.

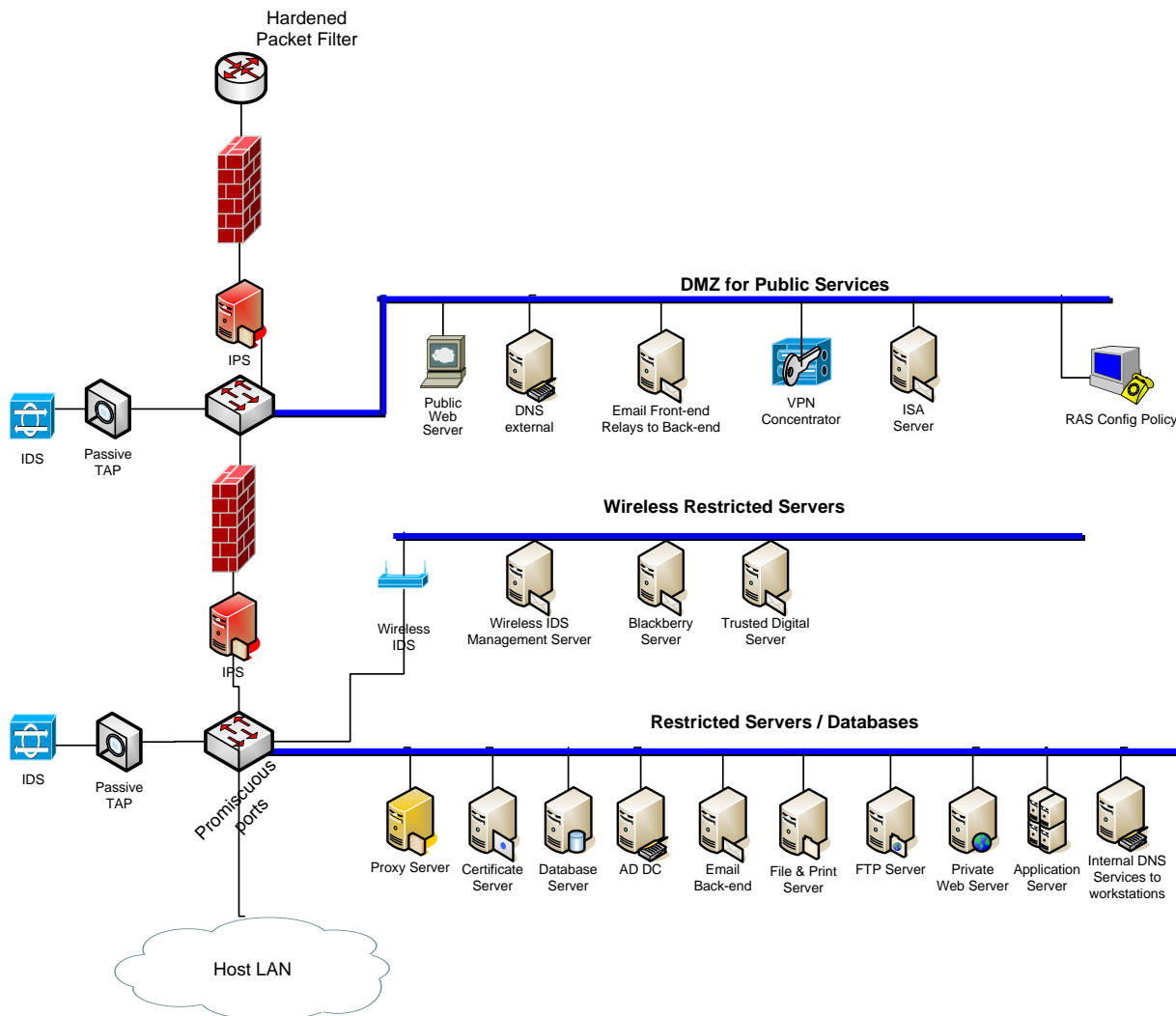


Figure 3-1. Firewall design with DMZ and Restricted Segments

- (NET0345: CAT II) The IAIO will ensure only firewalls that have obtained the DoD Application-Level for Medium Robustness Environments Protection Profile (PP) are placed in the network infrastructure meeting a Common Criteria PP of EAL 4 or greater.
- (NET0346: CAT II) The IAIO/NSO will ensure a DMZ Architecture is implemented, providing boundary protection for classified and sensitive architectures that interconnect enclaves.
- (NET0347: CAT III) The IAIO will ensure the Accreditation documentation (e.g., SSAA) is updated to reflect the installation or modification of the site's firewall.
- (NET0348: CAT II) The IAIO will ensure publicly accessible servers (i.e., web servers) are placed in an enclave DMZ.

- *(NET0351: CAT II) The IAO/NSO will ensure, when protecting the boundaries of a network, the firewall is placed between the private network and the premise router.*

Many vendors are providing integrated router, firewall, IPS and IDS solutions to reduce operation costs, space, and power requirements in the remote and small site locations. An integrated solution implemented within DoD should not waive from defense in depth practices. Router and firewall integration approved by NIAP is an acceptable solution however; Design Engineers should consider the number of concurrent sessions and application services the firewall will inspect to ensure degradation is avoided.

The current trend in firewall development is the incorporation of advanced security features. Most midrange enterprise firewall manufacturers are rolling in features such as IPS, anti-spam, and anti-virus. Therefore, it *may* become increasingly more difficult to find a firewall that only performs "traditional" firewall functions. As such, guidance for the usage/deployment of integrated security solutions will be provided. These solutions have leveraged processors and memory. Once this technology is compromised, all security layers of defense are subject to DOS in a single attack. The possibility of all of the segments in an integrated security solution losing functionality (which would result in the loss of external network availability) during an attack of one of the security features does indeed exist. This is especially the case in situations where similar code may exist on certain parts of the packet processing functions. Thus, even if different components are running on separate hardware, have separate CPUs, and separate memory, any similar code that may exist on certain parts of the packet processing functions could open the device up for attacks that could span multiple components of the integrated security solution.

It is important to note that even though the hardware modules are separated, they can be configured to run inline and running inline defeats the purpose of having separate hardware. The IPS can run in either promiscuous mode or inline mode. In inline mode, the IPS interfaces are associated with the ingress and egress interfaces of the firewall. If the IPS is under attack and crashed, no traffic will flow to the egress interface of the firewall. However, if running in promiscuous mode and the IPS module is attacked, the firewall will still function properly, as the IPS only receives a copy of the traffic, not wedge itself in between the firewalls egress and ingress interfaces. The drawback in the scenario is that the firewall is not able to stop the first packet in an attack. Some attacks are only one packet. As such, it may be possible to send one attack that could crash the integrated security solution. The probability of this or any other DoS condition occurring depends on the product itself (e.g., how well it performs its functions and its underlying code) and how it is deployed in the network. Integrated solutions within DoD require the firewall and the IDS solution to be on separate devices.

- *(NET0355: CAT II) The IAO/NSO will ensure, when protecting the boundaries of a network, the firewall and IDS/IPS are separate components.*

3.3 Content Filtering

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

- A firewall with application awareness (Deep Packet Inspection, Application-Proxy Gateway, Hybrid) at the perimeter to protect the whole Enclave, having application-proxy functionality, IDS signatures and application protocol anomaly detection rules.
- A non application-level firewall at the perimeter (e.g., packet-filter, stateful inspection) with an application-proxy gateway having IDS signatures and application protocol anomaly detection rules.

Due to technological advances there are devices such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or Stateful Inspection firewall, in collaboration with application level proxy devices to service all connections identified in the PPS CAL boundaries 8, 12, 13, and 16 is an acceptable alternative. Creating a filter to allow a port or service through the firewall without a proxy, creates a direct connection between the host in the private network and a host on the outside; thereby, bypassing additional security measures that could be provided by a proxy server. This places internal hosts at greater risk of exploitation and could make the entire network vulnerable to an attack. A solution with a proxy server can accept outbound traffic directly from internal systems, break the connection and filter or log the traffic, prior to passing it to the firewall for outbound delivery.

- *(NET0365: CAT I) The IAO will ensure the enclave is protected by providing a firewall that provides full packet awareness as provided by application-level gateways, hybrid firewalls or a non application-level firewall solution using an application-proxy gateway.*
- *(NET0366: CAT II) The IAO will ensure proxies are implemented between the enclave and external network boundaries defined in the PPS CAL for listed examples in the following boundaries:*

<i>Boundary 8</i>	<i>Outbound from Enclave to DoD Network</i>
<i>Boundary 12</i>	<i>Outbound from Enclave to Enclave DMZ</i>
<i>Boundary 13</i>	<i>Outbound from Enclave to External</i>
<i>Boundary 16</i>	<i>Outbound from Enclave to Enclave</i>

Examples:

- *Simple Mail Transfer Protocol (SMTP)*
- *HyperText Transfer Protocol (HTTP) See Note below*
- *File Transfer Protocol (FTP)*
- *Secure Shell (SSH)*

NOTE: Not required for Web Services. This is Client only, in an outbound direction.

NOTE: The PPS CAL can be located at the IASE website <http://iase.disa.mil/index2.html> by clicking the link to Ports Protocols and Services.

3.4 Perimeter Protection

There are a number of firewall solutions available to secure the enclave environment. To obtain the minimum requirements to secure the enclave, a defense-in-depth practice is required.

If the perimeter is in a Deny-by-Default posture, and what is allowed through the perimeter filtering is IAW DoD Instruction 8551.1 then the PPS would be covered under the Deny-by-Default rule, if permit rules are created for each approved port and protocol or all red ports were explicitly blocked. The permit rule with the port or protocol definition is required to prevent red PPS ports from traversing trusted subnets, otherwise a trusted subnet could use untrusted or red ports identified by the PPS, thus negating the blocking of ports identified in the PPS CAL.

Allowing only approved IP addresses through the perimeter router will control access to required ports and services. The perimeter will be protected IAW the guidance defined in Appendix C.

- *(NET0368: CAT II) The IAM will ensure that the firewall policy is in accordance with DoD Instruction 8551.1 and Appendix C.*

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

- *(NET0369: CAT I) The IAO will ensure the Enclave perimeter is protected via deny by default policy implemented at the perimeter router or at the firewall. This does not negate the firewall requirement.*

3.5 Configuration

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.

- *(NET0375: CAT II) The IAO/NSO will ensure the firewall is configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.*

The firewall must protect the private network from external attacks. The firewall will be maintained with the current supported version of the software and the Operating System (OS) will have 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. The firewall itself must be resistant to penetration to assist in preventing hackers from breaking through the firewall and accessing the entire network. Firewalls running on a standard OS must be stripped-down and hardened. Unnecessary executables, compilers, and other dangerous files must be removed and unnecessary services turned off. These functions are likely to be running using default configurations, which are usually much less secure. Disabling unused protocols ensures that attacks on the firewall utilizing protocol encapsulation techniques will not be effective.

- *(NET0377: CAT II) The FA will ensure the firewall does not utilize any services or capabilities other than firewall software (e.g., DNS servers, e-mail client servers, ftp servers,*

web servers, etc.), and if these services are part of the standard firewall suite, they will be either uninstalled or disabled.

- *(NET0378: CAT II) The FA will use a supported version of the firewall software with all security-related patches applied.*
- *(NET0379: CAT II) The FA will ensure if the firewall product operates on an OS platform, the host must be STIG compliant prior to the installation of the firewall product.*
- *(NET0380: CAT II) The IAO will ensure the firewall rejects requests for access or services where the source address received by the firewall specifies a loopback address.*
- *(NET0381: CAT II) The IAO will ensure the firewall rejects SMTP traffic that contains source routing symbols (e.g., in the mailer RCPT commands).*

If an IAVM is issued against the OS any time after the firewall installation and implementation, the FA must contact the firewall vendor 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.

- *(NET0384: CAT III) The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.*

By configuring the firewall to provide a message to the local console regardless of whether an administrator is logged in by sending alerts due to modification or exceeding capacity of audit logs ensures administrative staff is aware of critical alerts. The message should be displayed at the remote console if an administrator is already logged in, or when an administrator logs in. This requirement specifies that the message be sent to the first established session for each of the defined roles to ensure someone in the administrator staff is aware of the alert as soon as possible.

- *(NET0386: CAT III) The firewall will immediately alert the administrators by displaying a message at the local console, the remote administrative console, generate an audible alarm, and page or send an electronic message if the audit trail exceeds 75 % percentage or more of storage capacity.*
- *(NET0388: CAT III) The FA will have a procedure in place to dump logs when they reach 75% capacity to a syslog server.*

The firewall shall immediately display an alarm message, identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) that generated the alarm. The firewall provides a message to the local console regardless of whether an administrator is logged in or not. The message is displayed at the remote console if an administrator is already logged in, or when an administrator logs in if the alarm message has not been acknowledged. The audit records contents associated with the alarm may or may not be

part of the message displayed; however the relevant audit information must be available to administrators.

- *(NET0390: CAT II) The IAO/NSO will ensure the firewall is configured to alert the administrator of a potential attack or system failure.*
- *(NET0391: CAT II) The IAO/NSO will ensure the firewall provides critical alert message levels 0, 1, and 2 to the local console regardless of whether an administrator is logged in.*
- *(NET0392: CAT II) The IAO/NSO will ensure the message is displayed at the remote console if an administrator is already logged in, or when an administrator logs in if the alarm message has not been acknowledged.*

The firewall will display the alarm message identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) until it has been acknowledged. An audible alarm will sound until acknowledged by an administrator. The requirements are necessary to ensure an administrator will be aware of the alarm. The intent is to ensure that if an administrator is logged in and not physically at the console or remote workstation the message will remain displayed until they have acknowledged it. The message will not be scrolled off the screen due to other activities taking place (e.g., the Audit Administrator is running an audit report).

- *(NET0395: CAT III) The IAO/NSO will ensure the alarm message identifying the potential security violation makes accessible the audit record contents associated with the auditable event(s) until it has been acknowledged.*
- *(NET0396: CAT III) The IAO/NSO will ensure an audible alarm sounds until acknowledged by an administrator.*

Acknowledging the message and audible alarm could be a single event, or different events. In addition, assurance is required that each administrator that received the alarm message also receives the acknowledgement message, which includes some form of reference to the alarm message, who acknowledged the message and when. The firewall shall display an acknowledgement message identifying a reference to the potential security violation, a notice that it has been acknowledged, the time of the acknowledgement, and the user identifier that acknowledged the alarm at the local console and remote administrator sessions that received the alarm.

- *(NET0398: CAT III) The IAO/NSO will ensure an acknowledgement message identifying a reference to the potential security violation is logged and it contains a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm, at the local console, and remote administrator sessions that received the alarm.*

4. ROUTERS

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.

The following diagram describes an attack when traffic is misdirected to a Black Hole that can be avoided when authentication is implemented properly.

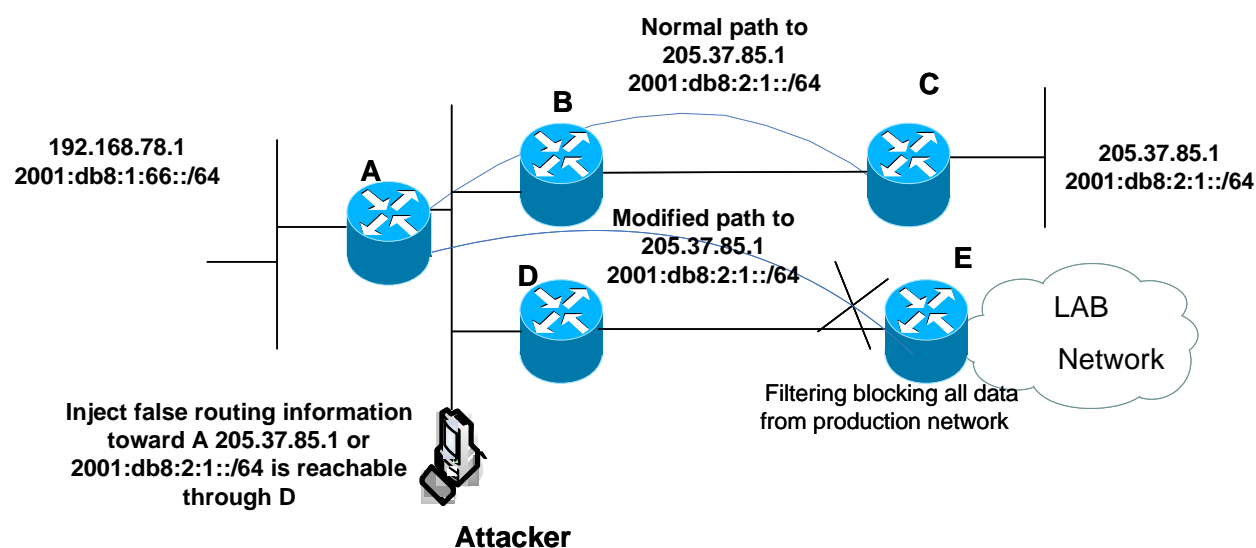


Figure 4-1-A. Attacker Injecting False Route Advertisements

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 or when there is only one path to the NIPRnet / SIPRNet. When routing protocols 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 and security measures are in place to ensure that a router receives routing information only from a trusted source.

The best way to protect routing information is to authenticate routing protocol packets using Message Digest Algorithm 5 (MD5) or IP Security (IPSec) signatures. A cryptographic signature combines three things:

1. The encryption Algorithm

2. The key used in the encryption algorithm, which is a secret shared by the routers authenticating their packets
3. Contents of the packet

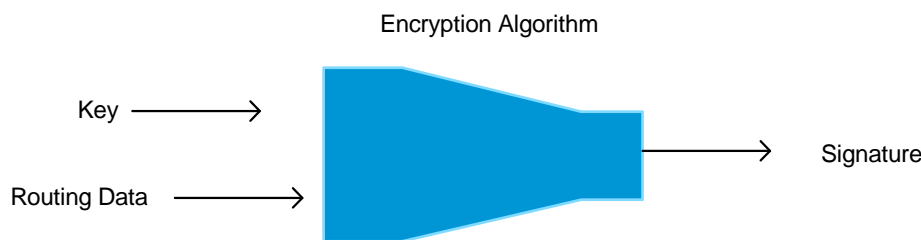


Figure 4-1-B. Signature Creation

All of the routing protocols support MD5 authentication except RIP Version 1 and Interior Gateway Routing Protocol (IGRP). 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 confidential by using controlled methods for exchanging the keys as well as changing the keys on a regular basis.

4.1.1 OSPFv2, EIGRP, RIPv2, IS-IS

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.

- *(NET0400: CAT II) The router administrator will ensure neighbor authentication with IPsec or MD5 Signatures are implemented for interior routing protocols with all peer routers within the same or between Autonomous Systems (AS).*

The MD5 Signature is an effective security mechanism, but requires manual configuration and key management. See Key Management section below for additional requirements.

4.1.2 OSPFv3

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

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

The authentication fields found in OSPFv2 are not present in OSPFv3 for IPv6 thus no longer making MD5 an authentication option. OSPFv3 relies on the IP Authentication Header and the IP Encapsulating Security Payload to ensure integrity, authentication, and confidentiality of routing exchanges. IPv6 AH in transport mode will provide authentication to OSPFv3 protocol packets as well as selected portions of IPv6 header.

IPSec can be configured for OSPFv3 on an interface or on an OSPF area. IPSec has two operations: authentication and encryption. With routing protocols the concern is with routing integrity that is protected by the authentication option, and not the information in the routing protocol packet that the encryption option protects. Therefore the parameter null indicating no encryption is an acceptable implementation for OSPF authentication.

- *(NET0402: CAT II) The IAO/NSO will ensure neighbor authentication with IPSec AH is implemented between OSPFv3 peer routers within the same or between AS.*

4.1.3 Protecting Exterior Routing Protocol BGP

Border Gateway Protocol (BGP) with multi-protocol extensions was released with version 4 of BGP. Unlike OSPF ships-in-the-night, the protocol exchanges information on IPv4 and IPv6 routes concurrently. Two mechanisms available to protect the integrity of BGP peers are TCP MD5 Signature and IPSec.

MD5 Signature, defined in RFC 2385, uses a cryptographic checksum (one-way hash) between peers to ensure the integrity of the contents of the route update. This feature must be configured with the same password on both BGP peers; otherwise, the BGP session will not be established. In addition, each external BGP (eBGP) router must use unique keys for each eBGP peering neighbor. The MD5 Signature is an effective security mechanism, but requires manual configuration and key management. Reference the Key Management section below for additional requirements.

You can apply IPSec to BGP traffic. IPSec is a protocol suite used for protecting IP traffic at the packet level. IPSec is based on Security Associations (SAs). An SA is a simple connection that provides security services to the packets carried by the SA. After configuring the security association, you can apply the SA to BGP peers.

MD5 Signature is most common in current BGP implementations, and sets up a secure signature for the TCP packets based on a cryptographic protection. Regardless of the IGRP (OSPFv2, OSPFv3, IS-IS, EIGRP) the peers require authentication.

The Exterior Gateway Protocol connected link to the SIPRNet or NIPRNet Hub will also be authenticated. The diagram below describes an OSPF enclave with a directly connected link to a hub router.

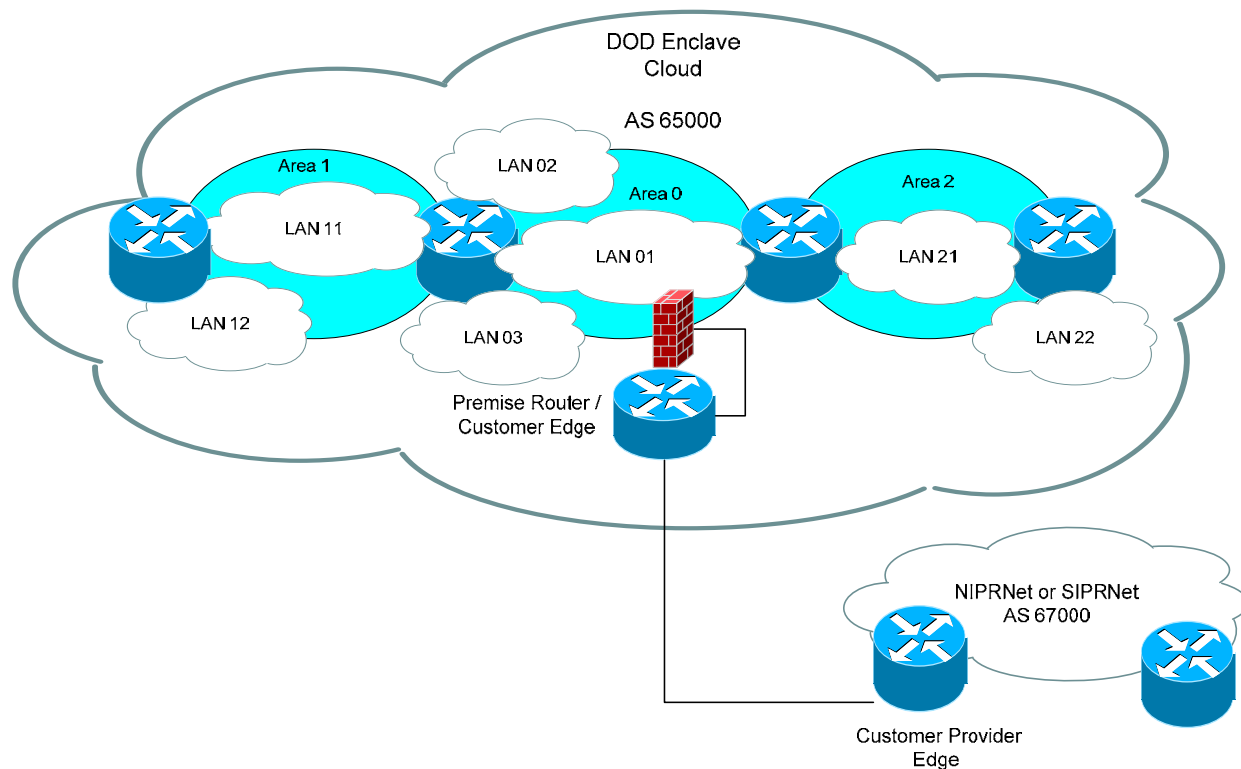


Figure 4-2. DoD Enclave Authentication to Customer Edge (CE)

- (NET0408: CAT II) The router administrator will ensure neighbor authentication with IPsec AH or MD5 signatures are implemented for all BGP 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 trusted Autonomous Systems.
- (NET0412: CAT II) If multiple eBGP peers are defined in the network, the IAO will ensure all eBGP neighbor authentications are configured with unique passwords when TCP MD5 Signature option is implemented.

4.2 Key Management

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

- *(NET0420: CAT II) The IAO/NSO will ensure a key management policy has been implemented to include key generation, distribution, storage, usage, lifetime duration, and destruction of all keys used for encryption.*
- *(NET0422: CAT II) The IAO/NSO will ensure a rotating key does not have a duration exceeding 180 days.*

Only EIGRP and 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.

- *(NET0425: CAT I) The IAO/NSO will ensure the lifetime of 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.*

4.3 Securing Router Planes

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 unused 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.

4.3.1 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.*

4.3.2 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.*

4.3.3 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 DoS 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 routers they are turned off by default.

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

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 to 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.

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.

- *(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 unless approved by the DAA.*
- *(NET0726: CAT III) The router administrator will ensure identification support is disabled.*
- *(NET0730: CAT III) The router administrator will ensure Finger is disabled.*

4.3.4 Idle Timeout Connections

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 keep-alive messages, letting it detect and drop broken Telnet connections.

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

4.3.5 HTTP, DHCP and FTP Server

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

By sending a large packet to the DHCP port, it is possible to freeze the router's processing engine or certain crafted DHCP packets may be undeliverable, but will remain in the queue instead of being dropped. If a number of packets are sent that equal the size of the input queue, no more traffic will be accepted on that interface. On a blocked Ethernet interface, Address Resolution Protocol (ARP) can time out and no inbound or outbound traffic can be processed, including both IP and non-IP traffic such as IPX. The device must be rebooted to clear the input queue on the interface, and will not reload without user intervention. The attack may be repeated on all interfaces, causing the router to be remotely inaccessible, excluding the console port where DHCP packets are not processed by default and which can be used for out-of-band management and configured for remote access. DHCP service is enabled by default. A router should never be configured to function as an FTP server or DHCP server. Enabling these additional services on any router simply increases the risk for compromise.

- *(NET0728: CAT III) The router administrator will ensure DHCP Services are disabled on premise routers.*
- *(NET0740: CAT II) The router administrator will ensure HTTP servers are disabled.*
- *(NET0742: CAT II) The router administrator will ensure FTP server is disabled.*

4.3.6 BSD Remote Services

Berkeley Software Distribution (BSD) "r" commands allow users to execute commands on remote systems using a variety of protocols. The BSD "r" commands (e.g., rsh, rlogin, rcp, rdump, rrestore, and rdist) are designed to provide convenient remote access without passwords to services such as remote command execution (rsh), remote login (rlogin), and remote file copy (rcp and rdist). The difficulty with these commands is that they use address-based authentication. An attacker who convinces a server that he is coming from a "trusted" machine

can essentially get complete and unrestricted access to a system. The attacker can convince the server by impersonating a trusted machine and using IP address, by confusing DNS so that DNS thinks that the attacker's IP address maps to a trusted machine's name and using its IP address or by a number of other methods.

- *(NET0744: CAT II) The router administrator will ensure all BSD r-command servers are disabled.*

4.3.7 Bootp Server

Bootp is a UDP based protocol 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). It is a security risk to allow a router to automatically obtain and load its configuration file from the network. 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.*

4.3.8 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.*

4.3.9 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. Disable Proxy ARP on all router interfaces that do not require it.

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.*

4.3.10 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 Internet Control Message Protocol (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.

The default behavior changed to directed broadcast being dropped (disable) in releases 12.0 and higher.

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

4.3.11 ICMP Exploits

The 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, Redirects, and Mask Reply.

An ICMP redirect message instructs an end node to use a specific router in 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 never send a redirect, and redirect will not traverse more than one network hop. However, an attacker may violate these rules; some attacks are based on this. This will prevent 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. This 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.*
- *(NET0802: CAT II) The router administrator will ensure ICMPv6 unreachable notifications and mask redirects are disabled on all external interfaces of the premise router.*

4.3.12 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, 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 to update or to affect its time settings. NTP peers can provide time synchronization to each other.

Timing source should be derived from a stable and acceptable source commonly referred to as a Primary Reference Source (PRS). The PRS should be a Stratum 1 clock system whether locally installed or derived from an available network source such as the approved NTP timeservers provided by the U.S. Naval Observatory. Specifically, NIPRNet and SIPRNet accessible NTP servers are identified at <http://tycho.usno.navy.mil/ntp.html>.

Alternatively, a PRS source can be a clock system employing direct control from Coordinated Universal Time (UTC) frequency and time services, such as Global Positioning System (GPS) navigational systems. The GPS System may be used to provide high accuracy, low cost timing of Stratum 1 quality.

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.

Since NTP is used to ensure accurate log file timestamp information, NTP could pose a security risk if a malicious user were able to falsify NTP information. Implementing MD5 authentication

between NTP peers can mitigate this risk. When MD5 authentication is enforced, there is a greater level of assurance that NTP updates are from a trusted source.

- *(NET0810: CAT III) The IAO/NSO will ensure the enclave has two Network Time Protocol (NTP) servers defined to synchronize time.*
- *(NET0811: CAT II) The IAO/NSO will ensure the premise router is acting as an NTP server for only internal clients.*
- *(NET0812: CAT III) The IAO/NSO will ensure all internal routers are configured to use the premise router to synchronize time in an external trusted NTP implementation.*
- *(NET0813: CAT II) When the NTP source originates from an internal clock, the router administrator will ensure all routers use MD5 to authenticate the time source.*

4.3.13 Name Server

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 attacker's host, rather than the intended target.

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

4.3.14 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.*

4.3.15 Loopback Source Address

Using a loopback address as the source address offers a multitude of uses for security, access, management, and scalability of the router. It is easier to construct appropriate ingress filters for

router management plane traffic destined to the network management subnet since the source addresses will be from the range used for loopback interfaces instead of a larger range of addresses used for physical interfaces. Log information recorded by authentication and syslog servers will record the router's loopback address instead of the numerous physical interface addresses. Messages sent to the following management servers should also use the loopback address as the source address: TACACS+, RADIUS, Syslog, NTP, SNMP, NetFlow Collector, TFTP, and core dumps to FTP servers.

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

- *(NET0897: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating TACACS+ or RADIUS traffic.*
- *(NET0898: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating syslog traffic.*
- *(NET0899: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating NTP traffic.*
- *(NET0900: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating SNMP traffic.*
- *(NET0901: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating NetFlow traffic.*
- *(NET0902: CAT III) The router administrator will ensure the router's loopback address is used as the source address when originating TFTP or FTP traffic.*
- *(NET0903: CAT III) The router administrator will ensure the router's loopback address is used as the source address for BGP peering sessions.*

4.3.16 IPv6 Undetermined Transport

One of the fragmentation weaknesses known in IPv6 is the undetermined transport packet. This is a packet that contains an undetermined protocol due to fragmentation. Depending on the length of the IPv6 extension header chain, the initial fragment may not contain the layer four port information of the packet. Undetermined transport headers can be blocked by using the keyword undetermined-trans on the deny statement. Packets with unknown payload or protocol will be dropped at the perimeter.

- *(NET00906: CAT II) The router administrator will ensure the undetermined transport packet is blocked at the perimeter in an IPv6 enclave.*

4.3.17 IPv6 Routing Header

The Routing header is used by an IPv6 source to specify a list of intermediate nodes that a packet has to traverse on the path to its destination. If the packet cannot take the path, it is returned to the source node in an ICMPv6 unreachable error message. This header supports a function very similar to the IPv4 packet Loose Source Routing. Use of the routing extension header has few legitimate uses other than as implemented by Mobile IPv6. The Routing header is identified by a Next Header value of 43 and should be filtered by type using an ACL similar to: deny ipv6 any routing-type 0 log.

The routing header can be used maliciously to send a packet through a path where less robust security is in place, than through the presumably preferred path by routing protocols.

- *(NET0907: CAT II) The router administrator will ensure the routing header extension is blocked; type 0 is rejected in an IPv6 enclave.*

4.4 Ports, Protocols, and Services

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 guidelines described in this STIG.

As of this writing PPS 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 Ports: 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 SA will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in Appendix C and DoD Instruction 8551.1 for all ports and protocols required for operational commitments.*

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

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

4.4.1 ICMPv4 Message Types

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.

- *(NET0911: CAT II) The System Administrator can permit inbound ICMP messages Echo Reply (type 0), ICMP Destination Unreachable - fragmentation needed (type 3 - code 4), Source Quench (type 4), Time Exceeded (type 11), and Parameter Problem (type 12). All other inbound ICMP messages are prohibited. The following exception: All ICMP messages must be denied from external AG addresses.*

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.

- *(NET0912: CAT II) The System Administrator can permit outbound ICMP messages Source Quench (type 4), Echo Request (type 8), and Time Exceeded (type 11). All other outbound ICMP messages are prohibited. The following exception: All ICMP messages must be denied to external AG addresses.*

4.4.2 ICMPv6 Message Types

IPv6 uses the Internet Control Message Protocol (ICMP) as defined for IPv4 RFC-792, with a number of changes. The resulting protocol is called ICMPv6 and is document in RFC 44443. In addition, ICMPv6 has new message types that can be found in other RFC documents such as RFC 2461, Neighbor Discovery (ND) for IPv6.

ICMPv6 messages are grouped into two classes: error messages and informational messages. Error messages are identified as such by a zero in the high-order bit of their message Type field

values. Thus, error messages have message types from 0 to 127; informational messages have message types from 128 to 255.

The following table initially provided by NSA and modified by FSO with additional guidance gives a brief description of ICMPv6 and provides guidance that should be used for IPv6 ICMPv6 message filters. At the time of this writing the PPS CAL had not reviewed ICMPv6. Future consideration of ICMPv6 should be made when the PPS completes ICMPv6 vulnerability assessment.

ICMPv6 Message Type	AllowIn	AllowOut	Remarks
Destination unreachable (1)	C	N	This message type is very useful for probing and network mapping; Conditional , allow only to trusted partners.
Packet-too-big (2)	Y	Y	Allow this, it is necessary for PMTUD.
Time exceeded (3)	Y	N	While this message is necessary, in theory, for correct operation of IPv6, in practice it only facilitates probing.
Parameter problem (4)	Y	N	May not wish to allow this message type out of the network, it can be used for probing.
Echo request (128)	N	Y	Allow echo requests outbound if you want to allow internal hosts to ping external hosts. Consider allowing echo requests to the router.
Echo reply (129)	Y	N	Prohibit echo reply outbound.
MLD (130-132)	N	C	Conditional , These messages are necessary within your network, but not on external router-to-router links. If the external network segment does not support hosts, then block MLD report messages (type 131) inbound.
RD (133-134)	N	Y	If the external network segment does not support hosts, then block these messages inbound.
ND (135-136)	Y	Y	Allow, Necessary for correct operation.
Redirect (137)	N	N	Redirect messages provide a significant security risk and administrators should not accept these messages on external interfaces.
Router Renumbering (138)	N	N	Router Renumbering messages should not be forwarded across site boundaries.
Node info query (139)	N	Y	Though this message is not commonly supported, block it at your network border.
Node info response (140)	Y	N	Though few hosts will send this message, do not allow it to exit your network.
Experimental allocations (100, 101, 200, 201)	N	N	Drop experimental ICMP messages.

ICMPv6 Message Type	AllowIn	AllowOut	Remarks
Messages using the extension type numbers (127, 255)	N	N	Drop until such time as ICMPv6 needs to use such extensions. Reserved for expansion of ICMPv6 informational messages.
Informational messages (154-199) and (202-254)	N	N	Drop, not explicitly assigned by IANA.
Inverse Neighbor Discovery Solicitation (141)	N	N	In most cases during normal operation these messages will have link local destination addresses.
Listener Report v2 (143)			Must have link-local source address.
Home Agent Address Discovery Request (144)	N	N	Drop these messages, unless the firewall is providing approved mobile services.
Home Agent Address Discovery Reply (Type 145)	N	N	Drop these messages, unless the firewall is providing approved mobile services.
Mobile Prefix Solicitation (146)	N	N	Drop these messages, unless the firewall is providing approved mobile services.
Mobile Prefix Advertisement (147)	N	N	Drop these messages, unless the firewall is providing approved mobile services.
Certificate Path Solicitation and Advertisement (148 and 149)	N	N	Sent from nodes to routers on the same local link to obtain a certificate path which will allow the node to authenticate the router's claim to provide routing services for certain prefixes. If a link connected to a firewall/router is using SEND, the firewall must be able to exchange these messages with nodes on the link that will use its routing services. Must be received with hop limit = 255
Seamoby Experimental (150)	N	N	Experimental use in two protocols
Multicast Router Advertisement (151)	N	N	Drop these messages unless multicast is required. Must have link-local source address and hop limit = 1
Multicast Router Solicitation (152)	N	N	Drop these messages unless multicast is required. Must have link-local source address and hop limit = 1
Multicast Router Termination (153)	N	N	Drop these messages unless multicast is required. Must have link-local source address and hop limit = 1

Table 4-1. ICMPv6 Message Types

- *(NET0915: CAT II) The system administrator can permit inbound ICMPv6 messages Packet-too-big (type 2), Time Exceeded (type 3), Parameter Problem (type 4), Echo Reply (type 129), Network Discovery (type 135-136), Router, Node Response (type 140). Remaining ICMPv6 messages must be blocked inbound.*

NOTE: Exceptions to the permit: Destination Unreachable (1) must be denied from external AG addresses, otherwise permitted.

- *(NET0916: CAT II) The system administrator can permit outbound ICMPv6 messages Packet-too-big (type 2), Echo Request (type 128), MLD (130-132), Network Discovery (type 135-136), Router Discovery (type 133-134), Node Info Query (type 139).*

4.4.3 Traceroute

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.

- *(NET0918: CAT III) The router administrator will block all inbound traceroutes to prevent network discovery by unauthorized users.*

4.4.4 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.

If the router is in a Deny-by-Default posture and what is allowed through the router filtering is IAW DoD Instruction 8551.1 and if the permit rule is explicitly defined with explicit ports and protocols allowed, then the enclave is protected. Many of these ports are blocked at the DoD Internet Access Point.

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 system

```
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
```

4.5 IPv4 Address Filtering

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

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

Inbound access lists can be used to prevent some types of IP address spoofing, whereas outbound access lists alone will not provide sufficient security. Sites will implement router ingress and egress filtering based on a policy meeting security requirements documented in this STIG and DoD Instruction 8551.1.

- *(NET0920: CAT II) The router administrator will bind the ingress ACL filtering packets entering the network to the external interface on an inbound direction.*
- *(NET0921: CAT II) The router administrator will bind the egress ACL filtering packets leaving the network to the internal interface on an inbound direction.*
- *(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.*
- *(NET0923: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets with a local host loop back address (127.0.0.0/8).*
- *(NET0924: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets with a link-local IP address range (169.254.0.0/16).*

In addition to the private IP addresses mentioned, all sites need to be aware that IANA has also reserved blocks of IP addresses listed at the IANA website, and the appropriate ACLs need to be applied to filter this traffic. BOGON or Martian addresses are unassigned or reserved by 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 <http://www.iana.org>. The appropriate ACLs need to be applied to filter this traffic.

- *(NET0926: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets having a source field from BOGON, Martian IP addresses.*
- *(NET0927: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets having a source field from RFC1918 IP addresses.*
- *(NET0928: CAT III) The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.*

4.6 IPv6 Address Filtering

4.6.1 Site Local Address

As currently defined, site local addresses are ambiguous and can be present in multiple sites. The address itself does not contain any indication of the site to which it belongs. The use of site-local addresses has the potential to adversely affect network security through leaks, ambiguity and potential misrouting, as documented in section 2 of RFC3879.

RFC3879 formally deprecates the IPv6 site-local unicast prefix defined in RFC3513, i.e., 1111111011 binary or FEC0::/10.

- (NET0941: CAT II) The IAO/NSO will ensure IPv6 Site Local Unicast addresses are not defined in the enclave, (FEC0::/10).
- (NET0942: CAT I) The IAO/NSO will ensure IPv6 Site Local Unicast addresses are blocked on the ingress and egress filters, (FEC0::/10).

4.6.2 Loopback Address

The unicast address 0:0:0:0:0:0:1, also defined ::1/128 is called the loopback address. A node could use it to send an IPv6 packet to itself. It should never be assigned to any physical interface. It is treated as having link-local scope, and may be thought of as the link-local unicast address of a virtual interface to an imaginary link that goes nowhere.

The loopback address must not be used as the source address in IPv6 packets that are sent outside of a single node. An IPv6 packet with a destination address of loopback must never be sent outside of a single node and must never be forwarded by an IPv6 router. A packet received on an interface with destination address of loopback must be dropped.

- (NET0943: CAT I) The router administrator will restrict the premise router from accepting any inbound IP packets with a local host loop back address, (0:0:0:0:0:0:1 or ::1/128).

4.6.3 Unspecified Address

The address 0:0:0:0:0:0:0, also defined ::/128 is called the unspecified address. It must never be assigned to any node. It indicates the absence of an address. One example of its use is in the Source Address field of any IPv6 packets sent by an initializing host before it has learned its own address.

The unspecified address must not be used as the destination address of IPv6 packets or in IPv6 Routing Headers. A router must never forward an IPv6 packet with a source address of unspecified.

- (NET0944: CAT I) The router administrator will restrict the premise router from accepting any IP packets from the unspecified address, (0:0:0:0:0:0:0 or ::/128).

4.6.4 Predefined Multicast Addresses

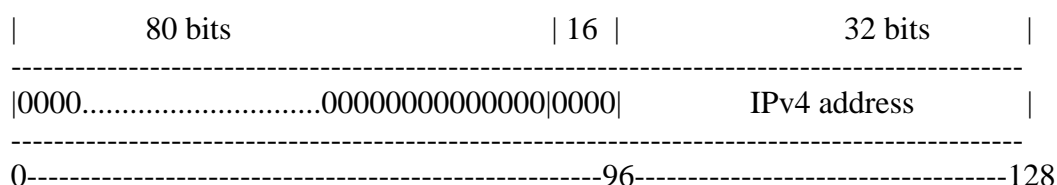
The following well-known multicast addresses are predefined and shall never be assigned to any multicast group.

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

- (NET0945: CAT II) The IAO/NSO will ensure IPv6 well-known Multicast addresses are blocked on the ingress and egress filters, (FF00::/16).

4.6.5 IPv4-compatible IPv6 addresses

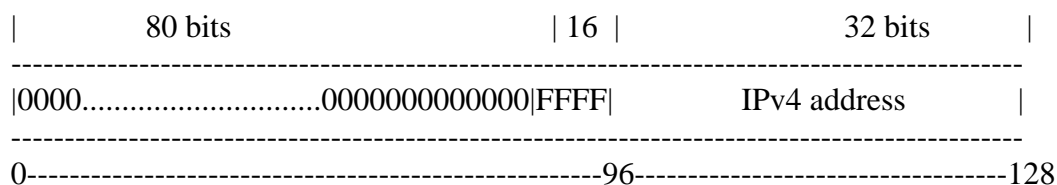
The IPv6 transition mechanisms include a technique for hosts and routers to dynamically tunnel IPv6 packets over IPv4 routing infrastructure. IPv6 nodes that use this technique are assigned special IPv6 unicast addresses that carry a global IPv4 address in the low-order 32 bits. IPv4-compatible IPv6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



- (NET0946: CAT II) The IAO/NSO will ensure IPv6 addresses with embedded IPv4-compatible IPv6 addresses are blocked on the ingress and egress filters, (0::/96).

4.6.6 IPv4-mapped IPv6 Addresses

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



- (NET0947: CAT II) The IAO/NSO will ensure IPv6 addresses with embedded IPv4-mapped IPv6 addresses are blocked on the ingress and egress filters, (0::FFFF/96).

4.6.7 Unique Local Addresses

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

- *(NET0948: CAT II) The IAO/NSO will ensure IPv6 Unique Local Unicast Addresses are blocked on the ingress and egress filter, (FC00::7).*

4.7 Unicast Reverse-Path Forwarding

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. In a CISCO environment, enabling CEF is required to utilize the Unicast RPF feature.

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, i.e., such as a SYN flood attack. 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 forward. If the router is process switching or even fast switching (cache), the router could easily become overwhelmed. Consequently, routers configured for CEF have a greater probability of avoiding a potential DoS during SYN floods directed at a customer network than routers using traditional switching.

Juniper's Flexible PIC Concentrator (FPC) 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 are not configurable.

- *(NET0949: CAT II) The router administrator will enable CEF to improve router stability during a SYN flood attack to the network.*

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

Global command	ip cef
Interface command	ip verify unicast source reachable-via rx 102

OR in Juniper: Apply rpf-check fail-filter

- (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 Strick mode.

In CISCO, by default failed packets are dropped when unicast reverse-path is enabled on the interface. If an access is applied, then the failed packets are tested against the filter, and dropped or forwarded as specified by the access rule. In Juniper as well as CISCO, the permit statements must qualify the source address with the internal network address range.

4.7.1 IPv6 Unicast Reverse-Path Forwarding

The unicast reverse-path forwarding protection is implemented very similar as in IPv4 environments. To protect the router from address spoofing attacks in an IPv6 environment the following commands should be implemented:

Global command **ipv6 cef**
Interface command **ipv6 verify unicast source reachable-via rx outbound-from-enclave**

OR in Juniper: Apply rpf-check fail-filter

- (NET0953: CAT II) The router administrator will enable CEF to improve router stability during a SYN flood attack in an IPv6 enclave.

As discussed previously, CEF does not apply to Juniper environments.

- (NET0954: 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 Strict mode in an IPv6 enclave.

4.8 SYN Flood Attack – Protecting Servers or LANS

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. By default, the software still manages a connection for 24 hours after no activity.

To optimize router resources, it is recommended to reduce the watch timeout to 10 seconds. It is also recommended to change the connection timeout to 60 seconds. Use the following CISCO commands:

```
ip tcp intercept watch-timeout 10
ip tcp intercept connection-timeout 60
```

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 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 protected. 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).

```
filter ingress-filter {
  policer tcp-syn-control {
    if-exceeding {
      bandwidth-limit 5000k;
      burst-size-limit 150k;
    }
    then discard;
  }
}
```

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

4.9 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 syn wait-time` command that should be set to 10 seconds or less. If the router does not peer with any BGP speakers across WAN links, this value could be set to an even more aggressive interval. The implementation for CISCO follows:

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

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 DoS on the Routing Engine. Rate limiting TCP SYN packets with JUNOS can be performed using either of the following two techniques:

- Specify the number of allowable connection attempts per minute for each service (i.e., ssh, telnet, ftp) enabled on the router.
- Create a firewall filter protecting the routing engine that rate limits TCP SYN traffic based on its bandwidth utilization and the maximum burst size.

Juniper's Flexible PIC Concentrator (FPC) 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 are not configurable.

- *(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.*

This page is intentionally blank.

5. DEVICE MANAGEMENT

All network components within the enclave and described in the Network STIG will follow the device management policies defined. The most common methods of taking advantage of firewall, router, switch and IDS systems are using the resources for remote management that are available. Securing these access points and controlling access via filters, encryption, authentication and disabling interfaces that are not required are best practices that need to be followed.

5.1 Vulnerability & Asset Management

The Vulnerability Management System (VMS) was developed to interface with the DoD Enterprise tools to assist all DoD CC/S/As in the identification of security vulnerabilities and track the issues through the lifecycle of the vulnerabilities existence. To ensure both the emerging and known vulnerabilities are addressed on a system, the VMS tracks the potential existence of all vulnerabilities based on the posture of an asset. All vulnerabilities are tracked through their lifecycle.

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

Running the most current, approved version of software or firmware on each network component will help maintain a stable base of security fixes as well as security enhancements. Network components that are not running the latest tested and approved versions of software are vulnerable to the network attacks. Furthermore, if the component is no longer supported by the vendor, patches or new firmware will not be made available to address weaknesses exposing new vulnerabilities, nor will IAVM notices be made available that provide announcements of these new vulnerabilities along with measures to mitigate their associated risks.

- *(NET1621: CAT II) The IAO will properly register all network components in VMS.*

5.2 Out-of-band Management (OOB)

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 and devices should have a direct local connection to the OOB network.

The biggest advantage to implementation of an OOB network is providing support and maintenance to the network that has become degraded or compromised. During an outage or degradation period the inband management link may not be available. The consequences of loss of availability of a MAC I system is unacceptable and could include the immediate and sustained

loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures. Maintenance support for key IT assets must be available to respond 24 X 7 immediately upon failure.

- *(NET1622: CAT II) The IAO/NSO will ensure an OOB management network is in place for MAC I systems or 24x7 personnel have immediate console access (direct connection method) for communication device management.*

5.2.1 Console Port Access

The console port is mainly used for local system access using a console terminal and is considered a form of OOB management. 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.

The use of this form of OOB management can have limitations to hardening of the network pending the implementation. The use of local user identification and passwords use CISCO's Type 7 defined encryption algorithm, which is regarded as weak in the commercial security community. The implementation of local user accounts does not satisfy two-factor authentication requirements.

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. Reference the AAA Implementation section for additional details.

5.2.2 Terminal Server Implementation

A terminal or communication server commonly provides out-of-band access for multiple devices. A terminal server is a router with multiple, low speed, asynchronous ports that provide connection to console ports on routers or switches. The terminal server allows you to use a single point to access the console ports of many devices. Access lists will be configured to allow access only to the terminal server from certain IP addresses. Accessing the console ports on other routers from the terminal server is performed by reverse telnet. Reverse Telnet allows you to establish a telnet connection out of the same device you telnet from, but on a different interface. The terminal server should not reside on the production LAN segment.

In order to control and authorize access, an authentication server that provides extended user authentication and authority levels will be implemented. See AAA Implementation section for additional details.

5.2.3 Juniper Implementation

The JUNOS software automatically creates the routing platform's management Ethernet interface, FXPO, which is an out-of-band management interface for connecting to the M-series and T-series router. On the J-series routing platform, the JUNOS software automatically creates the routing platform's management Ethernet interface, FE-0/0/0. To use the management port on front of the router you must configure its logical interface, with a valid IP address. By default,

the routing platform's management Ethernet interface uses its MAC address that is burned into the Ethernet card.

5.2.4 WAN Implementation

Extending the management network to leverage support personnel and resources is a design used by many network operation centers. When this design is implemented consideration of traffic volume from the management nodes should be considered. Throughput requirements in the management network are high; consider the use of a dedicated firewall. This design never traverses the production network.

Other design options can be implemented if the enclave is not weakened at the premise edge and the data is encrypted end-to-end. This would entail the tunnel being terminated at the edge, and technology such as SSH and TLS 3.1 being used on the local enclave. Use of this design should be carefully analyzed due to volume of management traffic and potential vulnerability to the production network if not carefully planned. The IAO/NSO will approve in writing, the use for each specified purpose.

- *(NET1623: CAT I) The IAO/NSO will ensure all OOB management connections to the device require passwords.*
- *(NET1624: CAT II) The system administrator will ensure the console port is configured to time out after 10 minutes or less of inactivity.*

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

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

- *(NET1628: CAT II) The IAO/NSO will ensure modems are not connected to the console port.*
- *(NET1629: CAT III) The system administrator will ensure the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.*

5.3 In-Band Management

In-band management administration with telnet is vulnerable because anyone with a network sniffer and access to the right LAN segment can acquire the router account and password information. 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 will only occur when the application itself would not function out of band or if the device being managed did not physically have enough interfaces to support the normal management connection. The IAO/NSO will approve in writing, the use for the specific purpose.

When in-band management of a device is required, identify what management protocols the device supports and limit the traffic to these protocols by filters. 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. Devices with IP Security (IPSec) should be managed by simply creating a tunnel from the management network to the device. This setup allows many insecure management protocols to flow over a single encrypted tunnel. When IPSec is not possible because it is not supported on a device, other less-secure alternatives must be chosen. For configuration of the device, SSH or Secure Sockets Layer (SSL) will be used instead of Telnet to encrypt any configuration modifications made to a device.

Management subnets will operate under an address space that is completely separate from the rest of the production network. This is an effective way to mitigate the effects of a single compromised host. Setting a small filtering router or firewall between the management stations and the rest of the network can improve overall security.

Any in-band management or WAN access will occur through a NAT process on the router that translates the non-routable management IP addresses to pre-specified production IP ranges. If remote access is used to connect to a network component for administrative access, the most stringent security controls will be implemented. Reference the WAN section for additional details. The management module provides configuration management for nearly all devices in the network through the use of two primary technologies: Routers acting as terminal servers and a dedicated management network segment. The routers provide a reverse-telnet function to the console ports on the Cisco devices throughout the enclave. Reference the Terminal Server section and the Management Module diagram for additional information. More extensive management features (software changes, content updates, log and alarm aggregation, and SNMP management) are provided through the dedicated management network segment.

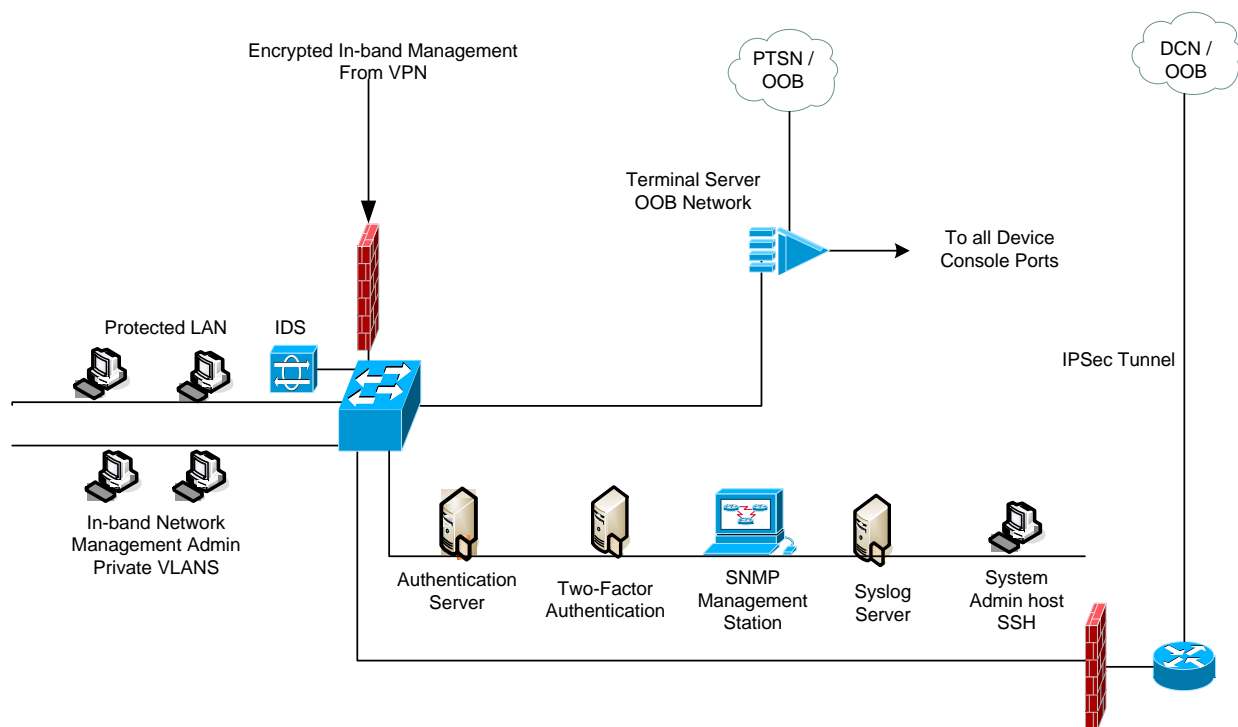


Figure 5-1. Device Management

The management network describes several variations of network management. The Data Communications Network (DCN) is an OOB Network used for Remote Device Management that can be architected for a Operations Center managing a remote site. The diagram also describes a second design for OOB networks, terminating a circuit to a terminal server. The terminal server extends the OOB to each console interface.

The diagram also describes an in-band management using VPN for Remote Management. Once the VPN is terminated at the firewall management traffic runs in the clear. Another weakness in this and all In-band management designs is when the production network is down or not routing as designed the management network is down or degraded at the same level, thus unmanageable.

- *(NET1635: 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.*
- *(NET1636: CAT I) The IAO/NSO will ensure all in-band management connections to the device require passwords.*
- *(NET1637: CAT II) The system administrator will ensure the device only allows in-band management sessions from authorized IP addresses from the internal network.*

- *(NET1638: CAT II) The system administrator will ensure in-band management access to the device is secured using an encryption such as AES, 3DES, SSH, or SSL.*
- *(NET1639: CAT II) The system administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.*
- *(NET1640: CAT III) The system administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*

5.3.1 Secure Shell Implementation

A secure shell (SSH) implementation is required in an In-band management network design to encrypt and authenticate the remote login session. Use of telnet in clear text is prohibited. SSH runs on top of a reliable transport layer and provides strong authentication and encryption capabilities. Currently, the only reliable transport that is defined for SSH is TCP. SSH provides a means to securely access and securely execute commands on another computer over a network. The Secure Copy Protocol (SCP) feature that is provided with SSH also allows for the secure transfer of files.

SSH Version 1 is a protocol that has never been defined in a standard. To prevent the management session from falling back to the undefined protocol (Version 1), you must use the “ip ssh version” command and specify Version 2.

To prevent non-SSH telnets the command “transport input ssh” must be coded on the vty interface. Secure Shell version 2 is a more secure version and its use is required. This version was made available in IOS release 12.2(25) and is available in the required version 12.3. Version 12.3 also supports IPv6, which is discussed in the appropriate section.

SSH retries default to 3 and should not be coded to extend the default. The timeout value defaults to 120 seconds and should be changed to 60 seconds. These settings apply to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.

There are several encryption options using SSH version 2. Select an approved FIPS 140-2 encryption algorithm in your implementation of In-band management.

- *(NET1645: CAT II) The system administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.*
- *(NET1646: CAT II) The system administrator will ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.*
- *(NET1647: CAT II) The system administrator will ensure SSH version 2 is implemented.*

5.4 Simple Network Management Protocol (SNMP)

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.

5.4.1 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.

5.4.2 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, SNMP version 2 and above uses Symmetric Privacy Protocol, this 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, 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 ACLs 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 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 and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category II.

- *(NET1665: CAT I) The IAO/NSO will ensure all SNMP community strings are changed from the default values.*
- *(NET1666: CAT II) The IAO/NSO will ensure all SNMP community strings and usernames are protected via technology that secures using an 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 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 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 are illegally modified, deleted, or added.*
- *Operational Violation: Indicates that a desired object or service can not be used.*
- *Physical Violation: Indicates that a physical part of the network (such as a cable) is damaged or modified without authorization.*
- *Security Mechanism Violation: Indicates that the network's security system is compromised or breached.*
- *Time Domain Violation: Indicates that an event is happening outside its allowed or typical time slot.*
- *(NET1720: CAT III) The IAO/NSO will ensure 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 is 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.*

5.4.3 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 the management workstation is located in a secure environment.*
- *(NET1740: CAT II) The IAO/NSO will ensure 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 all in-band sessions to the NMS is secured using an 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.*

SNMP should be treated with the utmost care because the underlying protocol has its own set of security vulnerabilities. If required, consider providing read-only access to devices via SNMP and treat the SNMP community string with the same care you might treat a root password on a critical UNIX host. Know that by introducing SNMP into your production network you are introducing a potential vulnerability into your environment.

SNMP management has its own set of security needs. Keeping SNMP traffic on the management segment allows it to traverse an isolated segment when pulling management information from devices. With SAFE, SNMP management pulls information only from devices rather than allowing it to push changes. To ensure this, each device is only configured with a “read-only” string.

SNMP "read-write" may be configured when using an OOB network but be aware of the increased security risk due to a clear text string allowing modification of device configurations.

5.5 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:

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

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 III) 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 administrator uses the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).*
- *(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.*

5.6 Change Management and Configuration Management

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

- *(NET1110: CAT II) The IAQ/NSO will ensure all changes and updates are documented in a manner suitable for review and audit.*
- *(NET1111: CAT II) The IAQ/NSO will ensure request forms are used to aid in recording the audit trail.*
- *(NET1113: CAT II) The IAQ/NSO will ensure current paper or electronic copies of configurations are maintained in a secure location.*
- *(NET1114: CAT II) The IAQ/NSO will ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.*

6. AUTHENTICATION, AUTHORIZATION, AND ACCOUNTING

6.1 AAA Implementation

Authentication, authorization, and accounting (AAA) network security services provide the primary framework through which an access control is set up on your network device. The network device uses information retrieved from the user's profile, which is located either in the local user database or on the security server.

Authentication is the way a user is identified prior to being allowed access to the network and network services. Authorization provides authorization for each service per-user account list and profile. Accounting provides the method for collecting and sending security server information used for auditing, and reporting, such as user identities, start and stop times, executed commands, number of packets, and number of bytes.

AAA network security services are made available to the device if the command *aaa new model* is defined. If AAA is not enabled then the authentication requirement is not being implemented, as a result of the default being disabled. Restricting access to network devices 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.

The AAA authentication login statement identifies the method list name and the method used to authenticate. A named list of authentication methods must be defined and applied to each interfaces using the authentication method. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list. The method argument refers to the actual method the authentication algorithm tries. The arguments are identified in the following table. The use of the 'none' keyword turns authentication off and essentially allows any user to authenticate. A configuration using the 'group radius' keyword implements group accounts. The implementation of security protocols Kerberos, Radius, Tacacs+ and group-name are implementations of an authentication server meeting the requirements. The local username database is not an implementation of an authentication server meeting the requirements defined in this guide and users should be aware that defining passwords in the local database can be easily cracked due to the type 7 level of encryption.

Keyword	Description
enable	Uses the enable password for authentication.
line	Uses the line password for authentication.
none	Uses no authentication.
group radius	Uses the list of all RADIUS hosts for authentication. Note: The RADIUS method does not work on a per-username basis.
group tacacs+	Uses the list of all TACACS+ hosts for authentication.
group group-name	Uses a subset of RADIUS or TACACS+ servers for authentication as defined by the aaa group server radius or aaa group server tacacs+ command.

Table 6-1. Authentication Parameters

- (NET0430: CAT II) The IAO/NSO will ensure an authentication server is used to gain administrative access to all network devices.
- (NET0431: CAT III) The IAO/NSO will ensure all AAA authentication services are configured to use two-factor authentication during normal operation.
- (NET0432: CAT III) The IAO/NSO will ensure the device is configured to use AAA tiered authorization groups for management authentication.
- (NET0433: CAT II) The IAO/NSO will ensure an authentication method list is applied to all interfaces via an explicit definition or by use of default key word.
- (NET0434: CAT II) The IAO/NSO will ensure the AAA authentication method implements user authentication.

6.2 Administrator Accounts

Individual user accounts with passwords must be set up and maintained in accordance with the guidance contained in DoDI 8500.2 IAIA-1 and IAIA-2. Sharing group accounts on any router is strictly prohibited. If these group accounts are not changed when someone leaves the group, that person could possibly gain control of the router. Furthermore, group accounts do not allow for proper auditing of who is accessing or changing the network.

Network disruptions or outages could be caused by mistakes made by inexperienced administrators. By not restricting router administrators to their proper privilege levels, access to restricted functions may be granted before they are trained or experienced enough to make configuration changes. Allowing unnecessary or unauthorized accounts to exist are at risk to be utilized by unauthorized users who could then gain full control of the router.

Many attacks against network components are launched from within the network by unsatisfied or disgruntled employees. It is imperative that all router passwords are encrypted so they cannot be viewed when the router configuration is displayed on the console or copied to a viewable document. All passwords must be encrypted when the router configuration is displayed.

- IOS

IOS requires an enable password to grant the administrator the ability to enter configuration mode. When the configuration is displayed, the enable password is shown in clear text. The enable secret password is MD5 encrypted and must be configured in lieu of the enable password.

- JUNOS

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.

- *(NET0460: CAT I) The IAO/NSO will ensure each user accessing the device locally have their own account with username and password.*
- *(NET0465: CAT II) The IAO/NSO will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.*
- *(NET0470: CAT II) The IAO/NSO will immediately have accounts removed from the authentication server or device, which are no longer required.*

6.3 Emergency Account

Only one user account will be configured locally on a router to be used solely for the purpose of accessing the router in the event that the AAA server, SecurID, or alternate token logon services are not available. The local account will default to the lowest authorization level when authenticated and should be restricted to only the enable command.

- *(NET0440: CAT II) The IAO/NSO will ensure only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).*
- *(NET0441: CAT I) The IAO/NSO will ensure the emergency account defaults to the lowest authorization level and the password is in a locked safe.*

When an authentication server is implemented the administrator will ensure a banner is implemented indicating unauthorized access is prohibited. This can be accomplished by using the AAA authentication banner statement. The implementation of a banner must also be defined locally in the network device configuration if local database is implemented.

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

6.4 Two-factor Authentication

Two-factor authentication is a security process that confirms user identities using two distinctive factors (i.e., 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.

- *(NET0445: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure device management is restricted by two-factor authentication (e.g., Secure ID, DoD PKI, or alternate token logon).*

6.5 Auditing

6.5.1 Syslog Server

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

real time to identify suspicious behavior or be archived for review at a later time for research and analysis.

A malicious user or intruder could attempt to cover his tracks by polluting the syslog data or even force the server to crash. Disabling the syslog server would eliminate visibility of the network infrastructure that security analysts depend on. The first line of defense is to ensure that the syslog server will only accept syslog packets from known managed devices and administrative access from trusted management workstations.

Because syslog messages are sent from managed devices to the syslog server in clear text an attacker on the network can easily sniff the messages. Furthermore, the syslog protocol uses UDP; thereby, making it relatively easy to spoof a managed device. Placing the syslog server on a separate subnet such as the management network isolated from general access and transient traffic will assist in reducing these risks. A host intrusion detection system (HIDS) should also be implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.

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. 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 6-2. Logging

- *(NET1020: CAT III) The IAO/NSO will ensure all attempts to any port, protocol, or service that is denied is logged.*
- *(NET1021: CAT III) The IAO/NSO will configure all devices to log severity levels 0 through 7 and send log data to a syslog server.*

- *(NET1022: CAT III) The IAO will ensure the syslog server is only connected to the management network.*
- *(NET1023: CAT II) The IAO will ensure the syslog servers are configured IAW the appropriate OS STIG.*
- *(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 7.*
- *(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).*
- *(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.*
- *(NET1281: CAT III) The IAO will ensure an HIDS is implemented on the syslog server to provide access control for the syslog data as well as provide the necessary protection against unauthorized user and service access.*
- *(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 audit log data is backed up weekly.*
- *(NET1287: CAT II) The IAO/NSO will ensure audit logs are protected from deletion.*
- *(NET1288: CAT III) The IAO/NSO will ensure the audit trail events are stamped with accurate date and time.*
- *(NET1289: CAT III) The IAO/NSO will ensure the audit trail events include source IP, destination IP, protocol used and action taken.*
- *(NET1300: CAT III) The IAO/NSO will ensure administrator logons, changes to the administrator group, and account lockouts are logged.*

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

- *(NET1299: CATIII) The IAO will ensure the firewall provides the ability to perform searches and sorting of audit data, based on user identity, source identity, destination identity, and provides ranges of one or more of the following: dates, times, user identities, service identifiers, or transport layer protocol, rule identity, and network interfaces.*

This page is intentionally blank.

7. PASSWORDS

7.1 Password Encryption

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 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 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.

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.

- *(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.*
- *(NET0590: CAT III) The router administrator will ensure the CISCO 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).*

7.2 Juniper Diagnostic Port Protection

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.

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

8. NETWORK INTRUSION DETECTION

8.1 Local Area Network Intrusion Detection

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 in promiscuous mode with all connections (e.g., LAN and WAN) being monitored.*
- *(NET1331: CAT II) The IAO will ensure only NIAP approved IDS components are placed in the network infrastructure meeting a Common Criteria PP of EAL 2 or greater.*
- *(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 authorized reviewers of Network IDS data are identified in writing by the site's IAM.*
- *(NET1344: CAT II) The IAO/NSO will ensure 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.*
- *(NET1351: 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.

8.2 External Intrusion Detection

An external NIDS must be installed and implemented in front of the premise or border router connecting to an AG or a link connecting directly to the NIPRNet / SIPRNet node router and must be monitored by the certified CNDSP. Placing the external NIDS on the exterior—that is, between the premise router and the service delivery router will enable the CNDSP to detect attempted attacks that may otherwise be blocked by the premise router or firewall. Reference the diagram in the AG section for AG connectivity.

Placing the external NIDS on the exterior between the premise router and the NIPRNet / SIPRNet customer edge (CE) 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

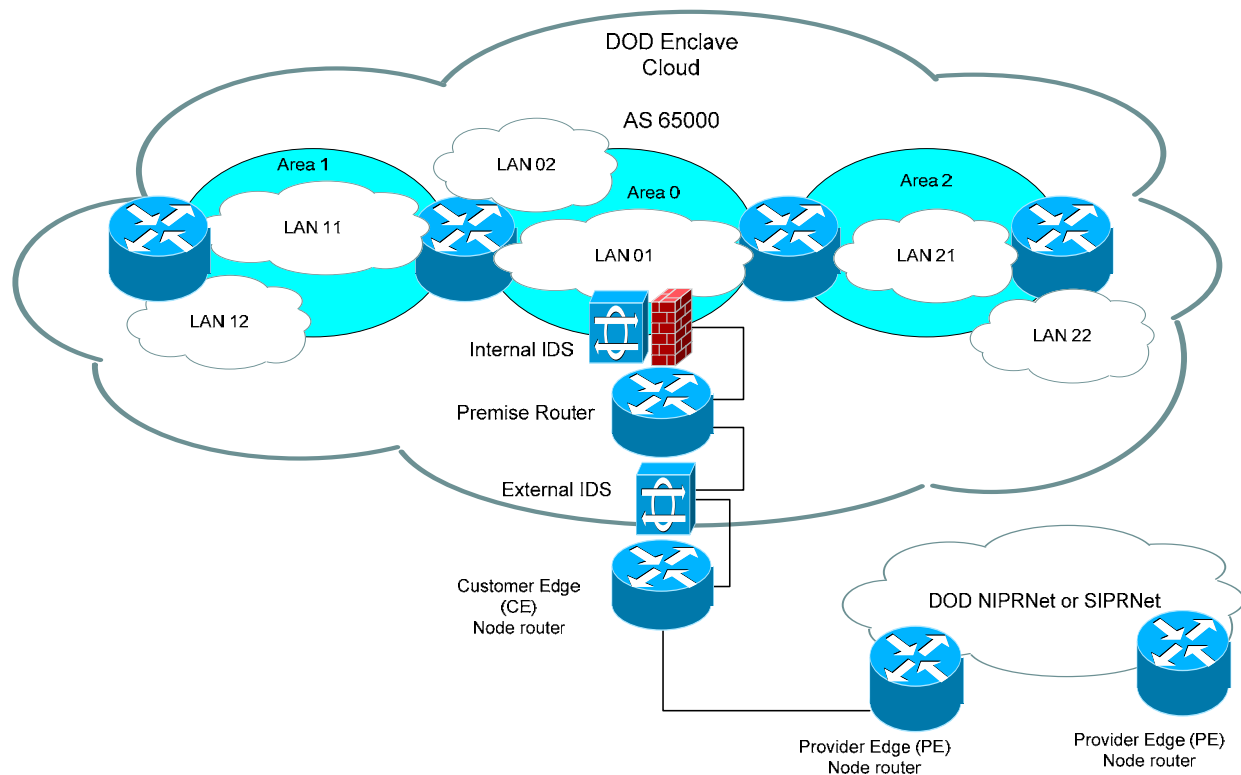


Figure 8-1. External IDS

- (NET1325: CAT II) If a NID is required by the CNDSP, the IAO/NSO will ensure 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 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. Reference the AG section for additional information.

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

This page is intentionally blank.

9. SWITCHES AND VLANS

9.1 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 all switches and associated cross-connect hardware are kept in a secured IDF or an enclosed cabinet that is kept locked.*

9.2 Virtual Local Area Networks

Virtual Local Area Network (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, and enabling networks to scale at ease.

9.3 Management VLAN and VLAN 1

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 IAQ/NSO will ensure VLAN1 is not used for in-band management traffic. The IAQ/NSO will assign a dedicated management VLAN to keep management traffic separate from user data and control plane traffic.*
- *(NET1411: CAT III) The IAQ/NSO will ensure the management VLAN is not configured on any trunk or access port that does not require it.*
- *(NET1412: CAT II) The IAQ/NSO will ensure VLAN1 is not used for user VLANs.*
- *(NET1413: CAT III) The IAQ/NSO will ensure VLAN1 is pruned from all trunk and access ports that do not require it.*

9.4 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.*

9.5 VLAN Access and 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:

- Port security
- Port authentication with 802.1X
- VLAN Management Policy Server (VMPS)

Additional requirements are necessary when implementing port security on the SIPRNet. If the implementation of securing the port is accomplished by traditional port security via MAC address without use of authentication, a data communications enclosure such as a Hoffman box will be required at the wall jack.

- *(NET1421: CAT II) The IAO/NSO will ensure Port Security implementation without authentication on the SIPRNet will have additional physical controls using a box to enclose the communication port.*
- *(NET1435: CAT II) 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.*

9.5.1 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 is implemented, the MAC addresses are statically configured on all access ports.*

9.5.1.1 Port Security using Sticky

Sticky addresses are learned like dynamic secure MAC addresses, but persist through switch reboots and link flaps like static secure MAC addresses. You might want to use this type if a

large number of fixed MAC addresses exist and you do not want to configure MAC addresses manually.

The sticky secure MAC addresses do not automatically become part of the configuration file, which is the startup configuration used each time the switch restarts. If the site implements a Sticky Port Security policy the running and startup configurations will be identical.

- *(NET1432: CAT II) The IAO/NSO will ensure if Sticky Port Security is implemented, the running and startup configuration files are identical.*

The port activation process will require a security policy where the switch port does not get enabled unless there is a connection approval for the device.

- *(NET1433: CAT II) The IAO/NSO will ensure if Sticky Port Security is implemented a security policy is in place where the switch port is not enabled unless there is a connection approval process.*

9.5.2 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 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: CAT II) 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.*

9.5.3 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 acts as VMPS clients. The VMPS server opens a UDP socket to communicate and listen to client requests using VMPS Query Protocol (VQP). When the VMPS server receives a valid request from a client, it searches its database for a MAC address-to-VLAN mapping. If the assigned VLAN is restricted to a group of ports, VMPS verifies the requesting port against this group. If the VLAN is allowed on the port, the VLAN name is returned to the client. If the VLAN is not allowed on the port, the host receives an "access denied" response when VMPS is not configured in secure mode or the port is shut down if in secure mode.

VQP is 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.

- *(NET1440: CAT II) The IAO/NSO will ensure VMPS is not being used to provide port authentication or dynamic VLAN assignment.*

This page is intentionally blank.

10. VIRTUAL PRIVATE NETWORK

10.1 Virtual Private Networks (VPN)

Traditional router-based networks connected customer sites through routers via dedicated point-to-point links. A VPN is a virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. VPN technologies have been designed to run on most of the OSI model's layers to leverage existing infrastructure to reduce costs. Because a VPN can be used over existing networks, it can facilitate the secure transfer of sensitive data across public networks. There are a number of technologies available, but VPNs can be categorized in two basic types, remote access or site-to-site.

There are three primary models for VPN architecture discussed in this procedure guide. NIST Special publication 800-77 Guide to IPSec VPNs provides an excellent description of the three architectures.

- **Gateway-to-gateway.** It connects two networks by deploying a gateway to each network and establishing a VPN connection between the two gateways. The VPN protects communications only between the two gateways.
- **Host-to-gateway.** It connects hosts on various networks with hosts on the organization's network by deploying a gateway to the organization's network and permitting external hosts to establish individual VPN connections to that gateway. The VPN protects communications only between the hosts and the gateway.
- **Host-to-host.** It connects hosts to a single target host by deploying VPN software to each host and configuring the target host to receive VPN connections from the other hosts. This is the only VPN model that provides protection for data throughout its transit, however has drawbacks that could impact the enclave.

10.2 Gateway-to-Gateway VPN

Tunneling is the encapsulation of the protocol at the same or higher layer of the OSI model. Layer 3 tunnels provide IP-based virtual connections. Two well-known network layer 3 VPN implementations over IP backbones involving tunneling technologies are Generic Routing Encapsulation (GRE) and IPSec. GRE supports multiple routed protocols, but does not secure the data; this alone may not be suitable in some DoD implementations. IPSec provides network layer authentication and optional encryption to make data transfer secure.

A Gateway-to-Gateway VPN, also known as Site-to-Site can be used to connect a DoD site location to a DoD site location. Encrypting network traffic is intended to prevent anyone other than those authorized from reading the data thus providing confidentiality controls. A VPN connection adds a level of data integrity protection beyond that offered by TCP, by ensuring that data diversion or man in the middle attack will not take place.

To understand the requirement using GRE tunnels an understanding of IPsec operation is necessary. During the IPsec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow. Some transform sets are set up to use both AH and ESP so that the benefits of both services can be realized. If a transform set specifies both AH and ESP then two pairs of uni-directional security associations will be set up because you cannot implement both AH and ESP on one security association. This is important when you are using certain IP protocols such as OSPF which uses a different IP protocol number (i.e., 89), the two protocols cannot therefore exist side by side, this is why IPsec cannot support broadcast and multicast traffic directly, routing protocols rely on broadcasts. By combining GRE tunnels with IPsec encryption, you can use IP routing protocols (OSPF, BGP, and EIGRP) to update the routing tables on both ends of the encrypted tunnel. GRE tunnels do support transporting IP multicast and broadcast packets to the other end of the GRE tunnel. The GRE tunnel packet is an IP unicast packet, so the GRE packet can be encrypted using IPsec. GRE does the tunneling work and IPsec does the encryption part of supporting the VPN network.

An IPsec VPN is a private secure distributed network that is *transported* or *tunneled* across a public and/or private network. IPsec provides two main facilities for creating VPN connections: an authentication-only function referred to as an AH and a combined authentication/encryption function called ESP which can operate either in transport mode or tunnel mode.

AH provides integrity protection for packet headers and data, as well as user authentication. Because authentication was added to ESP in the second version of IPsec, AH has become less significant and not supported with many IPsec software products.

Using IPsec ESP in transport mode, the data is encrypted but the header is left unchanged. A risk exists because the IPsec header sits within the original IP header. This allows an attacker to make intelligent guesses as to where servers are on a network (busiest IP addresses) and begin to build a picture of the network. Using IPsec in tunnel mode encrypts both the header and the payload. This type of SA is more secure because a new IP header unrelated to the hosts using the tunnel is created around the IPsec datagram. The original IP header is included within the encrypted IPsec datagram and so the originating device's addresses are hidden. Using the tunnel mode hackers can only determine the start and end point of the tunnel.

- *(NET1800: CAT II) The IAO/NSO will ensure VPNs are established as tunnel type VPNs.*

The placement of the VPN at the local network entry point (i.e., the firewall or Premise Router) 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, TLS) 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.

- *(NET1802: CAT II) The IAO/NSO will ensure gateway-to-gateway VPNs are terminated outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).*

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 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.*

10.2.1 SIPRNet Gateway-to-Gateway Tunnels

GRE tunnels found on a premise or edge SIPRNet router that have an endpoint within the Releasable (REL) IP address space must be documented in the SSAA. If a REL LAN environment is present the IAM will ensure REL LAN reviews are performed annually.

- *(NET1815: CAT II) The IAM will ensure REL LAN environments are documented in the Accreditation documentation (e.g. SSAA).*
- *(NET1816: CAT II) The IAM will ensure annual reviews are performed on REL LAN environments.*

Networks that provide encrypting tunnels are viable solutions for classified information (e.g., Secret, Top Secret); however they do not address availability or reliability. The SIPRNet provides an infrastructure designed to address security aspects for handling classified data and robustness associated with command and control (C2) traffic. The SIPRNet should be the network of choice for C2 traffic. If tunneling of classified information across an unclassified IP infrastructure is deemed necessary, then SIPRNet Connection Approval Process is in place to achieve connectivity. Exceptions can be sought due to mission requirements. The Joint Staff (JS) has established the conditions of “operationally urgent” to be:

- Joint Staff validated mission
- US forces engaged
- Loss of life potential
- Speed of mission is of paramount importance

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

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

the site must comply with the GIG Waiver Policy, reference DoDD 8100.1, Global Information Grid (GIG) Overarching Policy, September 19, 2002.

- *(NET1822: CAT II) Tunneling of non-C2 must be accepted by the Classified Data Service Manager (DISA/GS21) via request expressing the requirement with supporting rationale and must be IAW CJCSI 6211.02B, DISN policy.*
- *(NET1823: CAT II) If the non-C2 solution will be in place for more than 365 days, then the SIPRNet must be used or the IAO be in receipt of GIG Waiver Policy, DoDD 8100.1 .*
- *(NET1824: CAT I) If non-C2 traffic is being tunneled on a commercial ISP it must be approved by the OSD GIG Waiver Panel and the IAO be in receipt of GIG Waiver Policy, DoDD 8100.1 .*

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

- *(NET1826: CAT I) Leasing of point-to-point circuits that extend classified backside connectivity to any non-DoD, foreign or contractor facility is prohibited unless the termination is government operated in the contractor or foreign government facility.*

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

- *(NET1827: CAT II) The IAO/NSO will have all C2 and non-C2 exceptions of SIPRNet use documented in the enclave’s accreditation package and an Interim Authority to Connect/Authority to Connect (IATC/ATC) amending the connection approval received, prior to implementation.*

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

- *(NET1829: CAT II) If the non-DISN C2 solution proposed by the DISN Service Manager is accepted, Type 1 cryptography is employed for data protection.*

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

- *(NET1830: CAT II) The IAM will ensure the controls over the type of data to be moved are described in classification guidance, Executive Orders, or other issuances pertaining to controls over categories of information.*

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

- *(NET1832: CAT II) The IAM will ensure the tunnel demarcation is located in facilities authorized to process classified US government information, classified at the Secret Level (for SIPRNet).*

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

- *(NET1833: CAT I) If C2 traffic is being tunneled on the NIPRNet, the IAM has a plan of action and milestones detailing the effort to move the traffic to the SIPRNet.*

10.3 Host-to-Gateway VPN

In the host-to-gateway architecture the external host system handles the encryption and decryption activity on the host itself, while the connected network provides VPN encryption and decryption at the boundary. The security implication in this case is that only one of the two participating networks has the ability to inspect and filter the traffic content unencrypted using the security services at the boundary. The remote host computer is connected to an external network, which the enclave network does not trust. That remote physical network could be a personal home network connected to a commercial ISP, it could be a wireless hot spot provided for public use, or it could be a guest connection network provided in a hotel room. The traveling user who needs recurring connection to the supporting organizational network via VPN, may connect from a wide range of such external networks.

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

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

network, since it can enforce all security policies on the VPN-connected computer. The operational drawback of using tunnel-all mode is that the individual computer no longer has access to local network services on the physical network where it resides. This means the computer cannot use local networked printers, or connect to local servers that are not accessible to the outside world (typically the internet). The solution to this local service access problem would be to use the split-tunnel configuration.

Changing to the split-tunnel mode in order to reach local network printers or other services eases operational aspects, but complicates the security status. In split-tunnel mode, the VPN software only encrypts and routes to the remote gateway traffic addressed to the remote network served by that gateway. All other IP traffic is left unencrypted and handled by the normal local physical network routing steps. This has the effect of making the host computer a simultaneous node on two networks, and thus a bridge connecting them. If the two networks have different security policies, or if the remote network simply has no basis in policy or agreement to trust the security state of the network to which the host is physically connected, this bridging effect breaches the security boundary of the remote, protected network. If the client host were compromised, a remote attacker could connect to the host secretly and use its IPSec tunnel to gain unauthorized access to the organization's network.

- *(NET1834: CAT II) The IAO/NSO will ensure Remote Access VPN gateways terminate on or outside of the firewall.*
- *(NET1835: CAT II) The IAO/NSO will ensure remote access via VPN technology uses tunnel-all mode. Split-tunneling entering or leaving the enclave boundary is prohibited.*

By virtue of tunneling, users are in essence creating their own private virtual enclaves. Any problems encountered by the users would require extraordinary efforts to resolve and are typically caused by internal user mis-configuration. This requires network transport level personnel to troubleshoot, but they cannot gain access to the interior of the VPN.

- *(NET1836: CAT III) The IAO/NSO will ensure remote access via VPN technology complies with solutions in JTF-GNO Technical Bulletin 05-015 version 2, Virtual Private Networks (VPN) Implementation Best Practices, dated 19OCT2005.*

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. If a host-to-host VPN is required, it will be established between trusted known hosts with a host IDS implementation.

- *(NET1820: CAT II) The IAM will require the customer to provide a Host Based IDS capability for any gateway-to-host VPN established that bypasses the site's current IDS capability.*

10.3.1 Layer 2 Tunneling Protocols

Service providers implemented a layer 2 tunnel technology to make the service providers transparent in dialup solutions by encapsulating or tunneling PPP frames over IP. With this

implementation the customer was responsible for establishing layer 3 connectivity above PPP. Layer 2 tunnels carry point-to-point data link connections between end points of the VPN. Data Link or layer 2 tunnels provide a viable option for protecting networks running non-IP protocols such as IPX, and NetBEUI.

There are three well-known PPP forwarding implementations, identified below.

- Layer 2 Forwarding Protocol (L2F Protocol)
- Layer 2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)

A remote client uses the Internet and NIPRNet as the backbone for VPN connectivity to a DoD local area 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 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. Vulnerabilities of PPTP identified and publicly released in 1998 by Bruce Schneier and Mudge included serious flaws in the following areas:

- Password hashing -- weak algorithms allow eavesdroppers to learn the user's password
- Challenge/Reply Authentication Protocol -- a design flaw allows an attacker to masquerade as the server
- Encryption -- implementation mistakes allow encrypted data to be recovered
- Encryption key -- common passwords yield breakable keys, even for 128-bit encryption
- Control channel -- unauthenticated messages let attackers crash PPTP servers

Version 2 of PPTP corrected many of these vulnerabilities however password guessing is easily obtainable via use of publicly available hacker tools.

Layer 2 Forwarding protocol was developed by CISCO Systems. In a L2F implementation, users establish unprotected connections from their computers to the ISP. L2F is not client-based, users' systems do not need L2F client software or configuration. However, this also means that communications between the users' systems and the ISP are completely unprotected. L2F can use authentication protocols such as RADIUS and TACACS+, however L2F does not support encryption. Because L2F can provide only limited protection for portions of communications that involve a participating ISP it should not be used in DoD networks.

L2TP does not use GRE protocols, but uses its own protocol, which runs over UDP port 1701. Based on Microsoft's PPTP and Cisco's Layer 2 Forwarding Protocol (L2F), a L2TP VPN implementation model has a similar feature to GRE. It encapsulates the payload, but 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).

- *(NET1837: CAT II) The IAO/NSO will ensure 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 an encryption such as AES, 3DES, SSH, or SSL.*

10.3.2 Transport Layer Tunnels

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

- SSL
- TLS / SSL 3.1
- SSL Proxy Servers

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

- *(NET1838: CAT II) The IAO/NSO will ensure remote access VPNs using SSL protocol use the approved FIPS TLS protocol, also known as SSL 3.1.*

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

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

- *(NET1839: CAT II) The IAO/NSO will ensure their remote access solution verifies user identity and restricts access to authorized users.*

10.3.3 Contractor-to-Company Site VPN

This connection is established as an exclusive connection between the VPN client and the VPN network device; all other connectivity is blocked after establishment of the VPN session, so there is no chance of IP packets being forwarded between the contractor company and the DoD network. 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 in addition to guidance located in Host-to-Gateway VPN section.

- *(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.*
- *(NET1844: 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.*
- *(NET1845: CAT III) The remote user will ensure all communication to and from the site network employs security using an encryption such as AES, 3DES, SSH, or SSL.*

10.4 Host-to-Host VPN

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

- *(NET1850: CAT II) The IAO/NSO will ensure host-to-host VPNs do not bypass the enclave perimeter protections.*

This page is intentionally blank.

11. IPV6 TRANSITION MECHANISMS

Environments running IPv4 have various transition mechanisms available to transition the current IPv4 environment to a routed IPv6 network. There are three transition mechanisms available that will provide varying strategies. These transition mechanisms are Dual Stack, Encapsulation and Translation.

11.1 Dual Stack for IPv6 Transition

Dual-Stack is an environment running IPv4 and IPv6 and provides complete support for both protocols. Native IPv6 is the DoD goal: however, dual-stack is the best interim step in achieving this goal. Of the three strategies provided by the IETF, dual-stack is easier to secure and should be the preference over other strategies. In an environment carrying IPv4 and IPv6 the enclave is faced with risks from both protocols. Management, Control and Data plane threats for IPv6 are integrated into this STIG under existing IPv4 discussion under separate IPv6 headings. Refer to these when securing the dual-stack environment.

Dual-stack provides flexibility for both protocols to coexist. When the dual-stack environment is established routers and hosts support the IPv4 32 bit addressing and the IPv6 128 bit addressing. The protocols run transparent to the applications as “ships in the night”. Host will be able to detect the protocol the frame is carrying by the frame protocol ID.

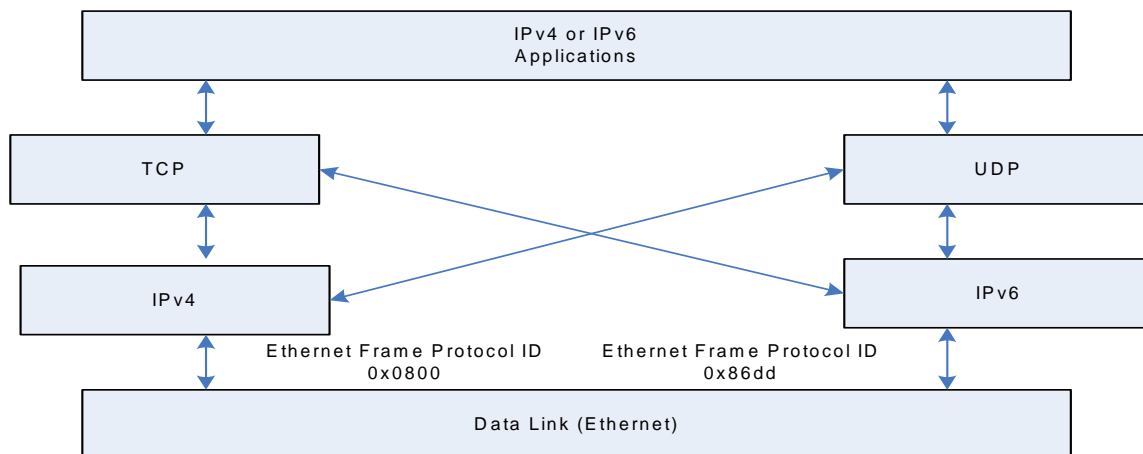


Figure 11-1. Coexistence IPv4 and IPv6

In a dual-stack environment protocol and address assignment is achieved in one of two implementations of DHCPv6. Stateless DHCP and Stateful DHCP are discussed in detail in the IPv6 Autoconfiguration section of this document.

In a dual-stack environment the protocol address selection can be administrator set by a manual LMHOST lookup or by DNS forced. The DNS resolution of name to address is discussed in the

DNS STIG, and additional vulnerability and mitigation for DNS in an IPv6 environment can also be found in the DNS STIG.

The DoD IPv6 Transition Office (DITO) Milestone Objective 2 (M02) introduced the Dual Stack as an approved architecture. The major objective for the MO2 time period beginning September 30, 2006 is to prevent any IPv6 traffic from leaking into non-participating domains or core networks. This version of the Network STIG will provide security guidance for MO2 to meet these requirements. As time progresses towards milestone objective 3 some protection mechanisms become obsolete, and the STIG will provide end-of-life requirements where applicable.

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

In a dual stack environment the enclave perimeter devices will not support IPv6 in IPv4 GRE or VPN tunnels between enclave internal devices. This means that nesting IPv6 in IPv4 in IPsec or IPv6 in IPv4 in GRE tunnel is not permitted.

The System Administrators shall implement a mirrored security policy for the enclave that matches the IPv6 security policy to the IPv4 security policy.

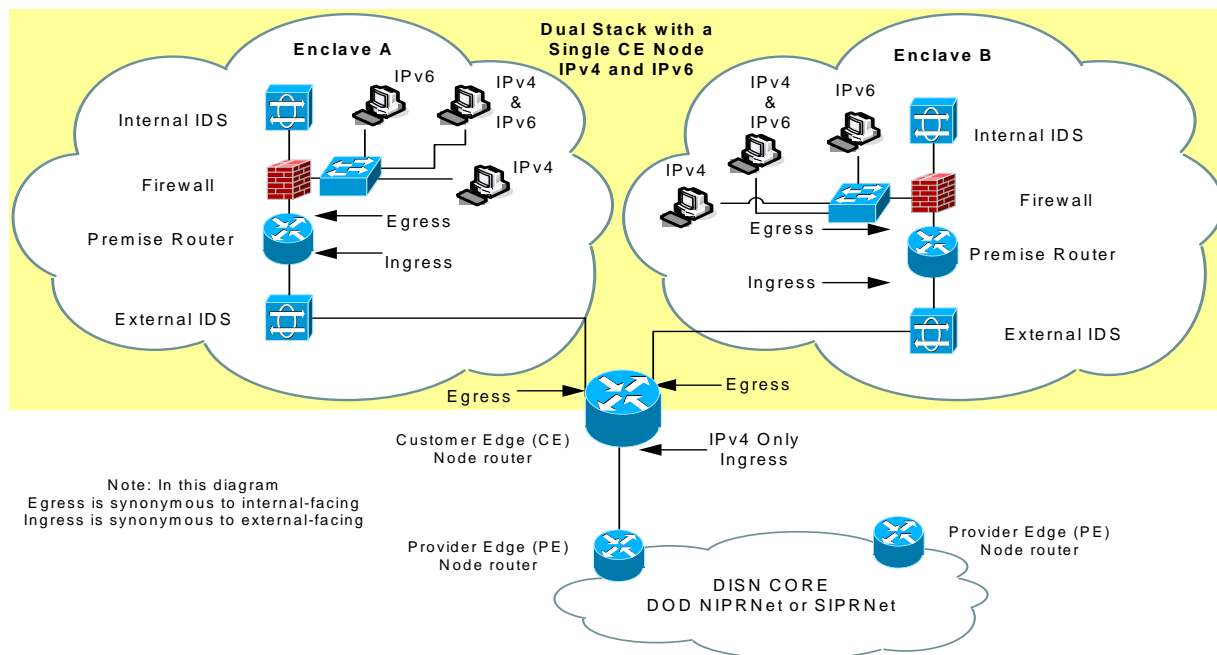


Figure 11-2-A. Dual Stack Architecture and a Single CE Node

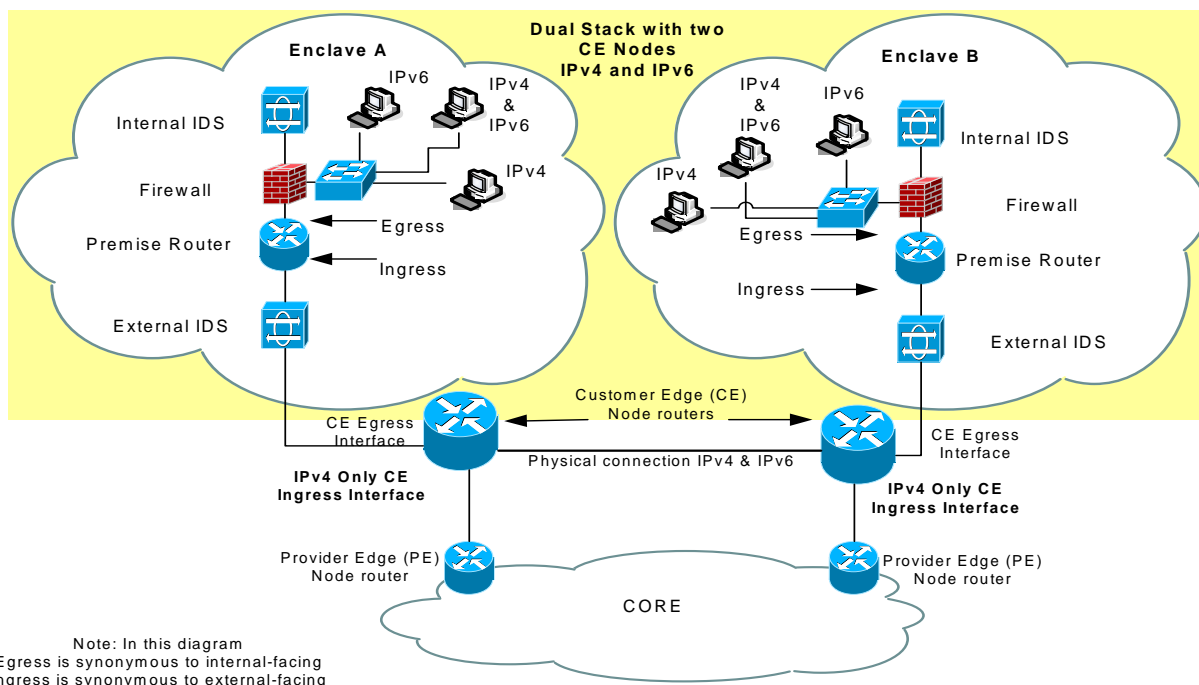


Figure 11-2-B. Dual Stack Architecture and Two CE Nodes

- (NET1900: CAT II) The IAO/NSO will ensure the customer edge interface facing the core's provider edge does not allow native IPv6 traffic during MO2.
- (NET1901: CAT II) The IAO/NSO will ensure the customer edge interface facing the core's provider edge does not allow native IPv6 network layer reachability information (NLRI) during MO2.
- (NET1905: CAT II) The IAO/NSO will ensure in a dual stack environment the enclave perimeter devices does not support IPv6 in IPv4 GRE or VPN tunnels between enclave internal devices.
- (NET1908: CAT I) The IAO/NSO will ensure in a dual stack environment the enclave IPv6 security policy mirrors the IPv4 security policy.

11.2 Split Domain Enterprise Architecture

RFC 4554 describes the use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, described as Split Domain Enterprise Architecture in this document. The architecture utilizes VLANs that can be readily used to deploy IPv6 networking in an enterprise, which focuses on the scenario of early deployment prior to availability of IPv6-capable switch-router equipment. In this method, IPv6 may be routed in parallel with the existing IPv4 in the enterprise and delivered at Layer 2 via VLAN technology. The IPv6 connectivity to the enterprise may or may not enter the site via the same physical link.

Sites migrating to dual-stack networking will either upgrade existing switch-router equipment to support IPv6 or procure new equipment that supports IPv6. If a site already has production routers deployed that support IPv6, the procedures described in this section are not required. In the interim, however, a method is required for early IPv6 adopters that enable IPv6 to be deployed in a structured, managed way to some or all of an enterprise network that currently lacks IPv6 support in its core infrastructure.

Many IPv4 enterprise networks are utilizing VLAN technology. Where a site does not have IPv6-capable Layer 2/3 switch-router equipment, but VLANs are supported, a simple yet effective method exists to gradually introduce IPv6 to some or all of that site's network in advance of the site's core infrastructure having dual-stack capability.

This architecture can be accomplished by deploying a parallel IPv6 routing infrastructure (which is likely to be a different platform to the site's main infrastructure equipment, i.e., one that supports IPv6 where the existing equipment does not), and then using VLAN technology to "overlay" IPv6 links onto existing IPv4 links.

In the Split Domain Enterprise diagram two IPv6 capable routers have been implemented and are running Dual Stack. Additionally an IPv6 enabled firewall and IDS have been added to the enterprise. In this example the enterprise has not been completely upgraded to IPv6 capable products. The legacy architecture remains in place running IPv4, connected to an internal dual stack router. VLAN trunks identified in the color red support an overlay configuration without requiring immediate router upgrades. This approach relies on VLAN tagging to enable Layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payload to one or more IPv6 capable routers. By upgrading one router to support IPv6, the switch ports to which its interfaces are connected can be configured as the IPv6 VLAN. Other IPv6 or dual-stacked devices could then be configured as members of the VLAN, and multiple VLANs could be configured likewise.

The implementation of this architecture requires the following guidelines be implemented. Referencing the Split Domain diagram, interfaces I1.A and P1.B will not receive any IPv4 traffic by not enabling IPv4 on I1.B. The SA will configure the architecture so that interfaces I1.D and P1.C will not receive any IPv6 traffic by not enabling IPv6 on I1.C. To prevent IPv4 frames from leaking onto the trunk supporting IPv6, the IPv4 VLANs will be pruned from the IPv6 trunk. To prevent IPv6 frames from leaking onto the trunk supporting IPv4, the IPv6 VLANs will be pruned from the IPv4 trunk. In the Split Domain architecture there must not be any IPv4 in IPv6 tunnel traffic between interfaces I1.A and P1.B, and interfaces I1.D and P1.C. The enterprise will not have any other IPv6 Transition Mechanisms implemented in the enclave when supporting Split Domain architecture.

- *(NET1910: CAT II) The IAO/NSO will ensure trunks supporting IPv6 vlans are pruned and do not leak IPv4 broadcast in Split Domain Architecture.*
- *(NET1911: CAT II) The IAO/NSO will ensure trunks supporting IPv4 vlans are pruned and do not leak IPv6 broadcast in Split Domain Architecture.*

- (NET1914: CAT II) The IAO/NSO will ensure interfaces on the Dual Stack device connecting to the IPv4 trunk do not have IPv6 enabled in Split Domain Architecture.
- (NET1915: CAT II) The IAO/NSO will ensure interfaces on the Dual Stack device connecting to the IPv6 trunk do not have IPv4 enabled in Split Domain Architecture.
- (NET1918: CAT II) The IAO/NSO will ensure interfaces supporting IPv6 in Split Domain Architecture do not have any IPv4 in IPv6 tunnel traffic between the interfaces.
- (NET1919: CAT II) The IAO/NSO will ensure interfaces supporting IPv4 in Split Domain Architecture do not have any IPv4 in IPv6 tunnel traffic between the interfaces.
- (NET1920: CAT II) The IAO/NSO will ensure the enclave boundary does not have any other IPv6 Transition Mechanisms implemented when supporting Split Domain.

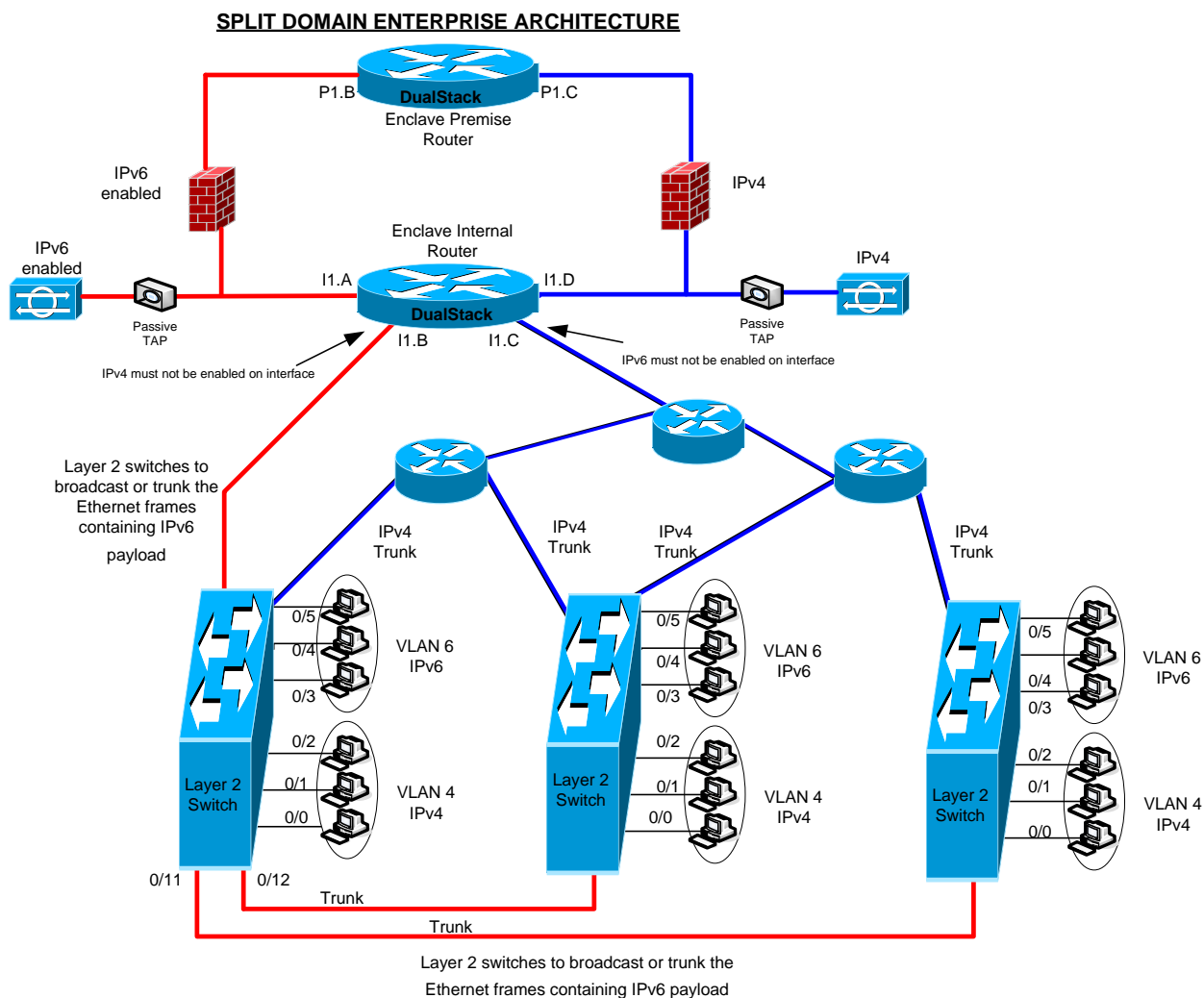


Figure 11-3. Split Domain Architecture

11.3 IPv6 Encapsulation for IPv6 Transition

Encapsulating data, also known as tunneling, will be used as an IPv6 transition mechanism when a backbone does not support IPv6 or when the network service provided to the premise router, also known as the CE, does not support IPv6. There are a number of IPv6 tunneling techniques that are provided by the IETF during the IPv6 transition. The tunnels supporting IPv6 transition fall into one of two categories, manually configured or automatic. When connecting IPv6 islands with tunnels, manual tunnels are preferred due to being more secure as a result of control and tunnel set-up. There are a number of automatic tunnels and each will be discussed in following sections. Many of the mitigations associated with manual or automatic tunnels are similar and will be described in this section as they apply to all IPv6 tunnel mechanisms. Vulnerabilities and mitigations associated with specific tunnel mechanisms will be described in their appropriate sections.

The encapsulating end-point of the tunnel will provide an IPv4 header to the packet and the tunnel encapsulation will also add an additional header for the encapsulating technology such as GRE or VPN. The encapsulating node also has to determine when to fragment and when to report an ICMPv6 "packet too big" error back to the source. In IPv6, the payload length field is 16 bits, limiting the IPv6 packet to 65,535 bytes. The encapsulating node must not treat the tunnel as an interface with a MTU of 64 kilobytes, but instead use a static MTU or optional dynamic MTU determination based on the IPv4 path MTU to the tunnel endpoint. Tunnel fragmentation can degrade performance of the end node and possibly lead to DOS.

Regardless of the tunnel type, the tunnel needs to terminate at an IPv4 interface of the perimeter router. The diagrams for the perimeter implementation indicate the tunnel endpoint will terminate at the ingress interface of the perimeter router.

It is also important to note that much of the discussion in this STIG concerning tunneling is in support of encapsulating IPv6 packets in IPv4 traffic and using the IPv4 network as a link-layer mechanism. As the DISN backbone transitions to IPv6 the encapsulation may become reversed, by connecting IPv4 islands over an IPv6 backbone. The discussion to support encapsulating IPv4 packets in IPv6 traffic will be documented in future releases.

The IPv6 IA tunneling guidance documented in the MO2 dated January 2006 establishes several approved tunneling designs. Two are discussed below:

- Enclave Perimeter Device GRE Tunnel
- Enclave Perimeter Device VPN Tunnel
- Enclave Perimeter employing GRE Tunnel in Non-Dual Stack Architecture.

IPv6 traffic can be carried over IPv4 GRE tunnels using the standard GRE tunneling technique that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme. The tunnels are not tied to a specific passenger or transport protocol, but in this case carry IPv6 as the passenger protocol with the GRE as the carrier protocol and IPv4 as the transport protocol. Enclaves connected via a GRE tunnel between their respective Enclave Perimeter devices should receive DAA approval prior to deploying this design due to the GRE protocol being identified as red by the PPS CAL, as of this writing. Because native IPv6 is not

permitted in the Intra-Enclave Security Zone in this architecture, it must be encapsulated inside of IPv4. The IPv6 in IPv4 tunnel is established between Enclave Interior devices.

The architecture in the following diagram prevents native IPv6 from reaching the perimeter router and the DISN core. Tunneler IPv6 traffic exiting the GRE end-point is routed to the enclave's internal device's IPv4 only interface, internal router ingress interface. The enclave perimeter device is not allowed to exchange exterior routes with internal devices.

The enclave perimeter devices will not support IPv6 in IPv4 IPsec tunnels and will not support other tunnel types between enclave internal devices. This means that nesting IPv6 in IPv4 in IPsec in GRE tunnel is not permitted in this scenario.

IPv6 in IPv4 tunnels use protocol 41 and filters will be established to except protocol 41 traffic using only trusted IPv4 source addresses that are explicitly configured. At the tunnel decapsulator end-point, all tunneled IPv6 traffic will be inspected prior to entering the enclave.

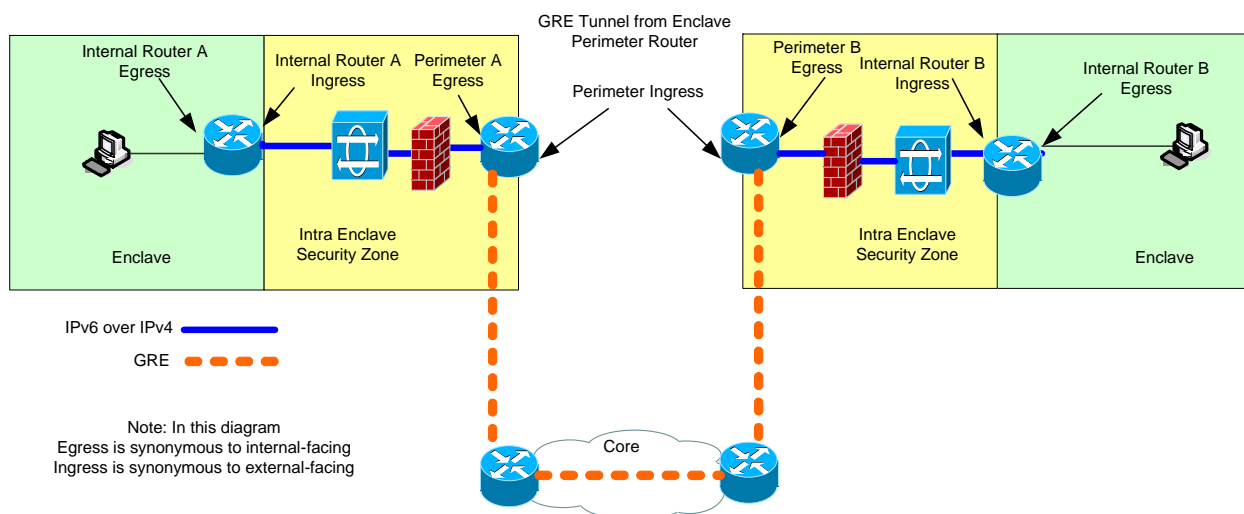


Figure 11-4. GRE Tunnel in Non-Dual Stack Architecture

11.3.1 Enclave Perimeter employing VPN Tunnel in Non-Dual Stack Architecture

Enclaves can be connected via a VPN tunnel between their respective Enclave Perimeter devices. Because native IPv6 is not permitted in the Intra-Enclave Security Zone, it must be encapsulated inside of IPv4. The IPv6 in IPv4 tunnel is established between Enclave Interior devices. The architecture in the following diagram prevents native IPv6 from reaching the perimeter router and the DISN core. Tunneler IPv6 traffic exiting the VPN end-point is routed to the enclave's internal device's IPv4 only interface. The enclave perimeter device is not allowed to exchange exterior routes with internal devices.

The enclave perimeter device ensures that only IPv4 datagrams are transferred between the internal network and the core network and that IPv6 and IPv4 datagrams may be transferred between the closed domains. IPv6 over IPv4 tunnels use protocol 41 and filters will be established to accept protocol 41 traffic using only trusted IPv4 source addresses that are explicitly configured. At the tunnel decapsulator end-point, all tunneled IPv6 traffic will be inspected prior to entering the enclave.

The enclave perimeter devices will not support IPv6 in IPv4 GRE tunnels and will not support other tunnel types between enclave internal devices. This means that nesting IPv6 in IPv4 in IPsec in GRE tunnel is not permitted in this scenario.

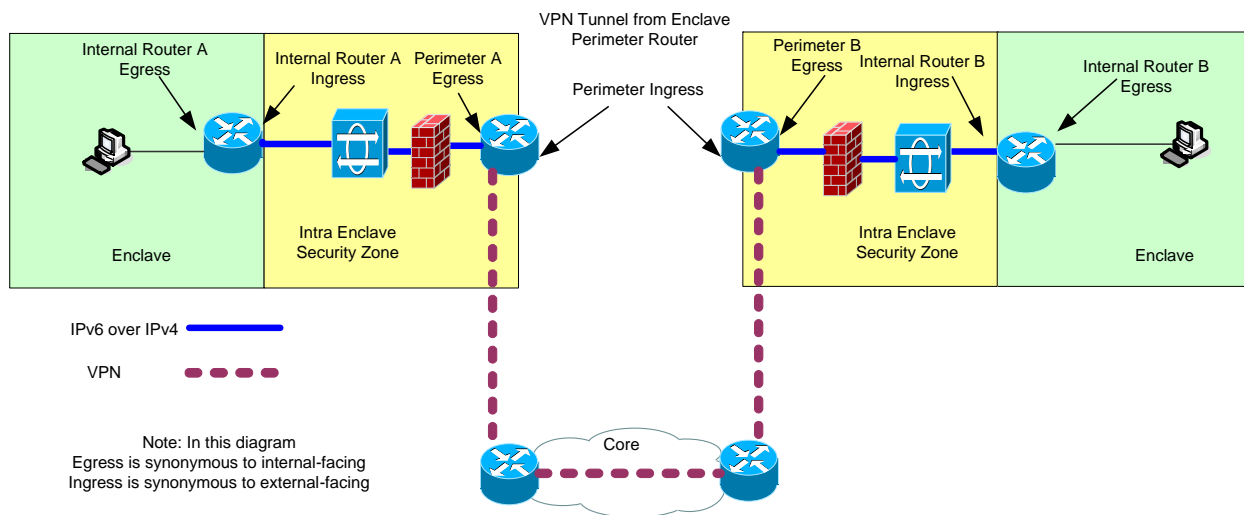


Figure 11-5. VPN Tunnel in Non-Dual Stack Architecture

- (NET1930: CAT II) The IAO/NSO will ensure the internal router's egress interface is the only interface accepting native IPv6 traffic.
- (NET1931: CAT II) The IAO/NSO will ensure the internal router's ingress interfaces does not allow native IPv6 traffic.
- (NET1934: CAT II) The IAO/NSO will ensure the internal router's ingress interfaces do not allow native IPv6 NLRI exchanges.
- (NET1935: CAT II) The IAO/NSO will ensure there is only one IPv6 to IPv4 tunnel between the interfaces of the internal router's ingress interface and the perimeter router's egress interface.

- *(NET1937: CAT II) The IAO/NSO will ensure the tunnel between the internal router's ingress interface and the perimeter router's egress interface is accessible to an IDS device capable of analyzing IPv6 in IPv4 traffic.*
- *(NET1938: CAT I) The IAO/NSO will ensure the tunnel between the internal router's ingress interface and the perimeter router's egress interface is accessible to a firewall device capable of inspecting and filtering IPv6 in IPv4 traffic.*
- *(NET1940: CAT II) The IAO/NSO will ensure the perimeter router does not route native IPv6 traffic during MO2.*
- *(NET1942: CAT II) The IAO/NSO will ensure an access list is applied on all interfaces not supporting IPv6 that blocks native IPv6 traffic when IPv6 is used in an enclave environment.*
- *(NET1944: CAT II) The IAO/NSO will ensure perimeter devices do not run routing protocols capable of advertising IPv6 NLRI during MO2.*
- *(NET1945: CAT II) The IAO/NSO will ensure tunnels used for IPv6 transition are filtered by protocol 41 and the endpoints are explicitly defined on the permit filter.*

11.3.2 IPv6 Automatic Tunnels

DoD locations that have a large number of tunnels may choose an automatic tunnel mechanism over manually configured tunnels. Automatic tunneling will scale much better than manual tunnels in an enterprise environment. The IETF has made available a number of automated tunnel mechanisms and each are briefly covered in this section. Most of the automated tunneling mechanisms will share the same mitigations with exception to Teredo, discussed later.

Automatic tunnels are required to discard unexpected protocol 41 packets and inspect IPv6 traffic at the decapsulator end-point as mentioned above in IPv6 Encapsulation for IPv6 Transition section.

It is also strongly recommended that prior to implementing any automated tunneling mechanism, a thorough evaluation of the vendor product is performed due to the demand on process switching resources tunneling has on the devices. Some devices will recommend manual tunnels only.

11.3.2.1 Intra-Site Automatic Tunneling Protocol (ISATAP)

ISATAP is an automatic tunnel mechanism that does not provide authentication such as IPSec. As a result of this limitation ISATAP is thought of as a tool that is used inside the enclave among trusted hosts, which would limit it to internal attacks. ISATAP is a service versus a product and is readily available to most users. If a user knows the ISATAP router IP address they can essentially get onto the IPv6 intranet. To control the vulnerability of this tunnel mechanism it is

critical to control the use of protocol 41 and use IPv4 filters to control what IPv4 nodes can send protocol 41 packets to an ISATAP router interface. Although the ISATAP tunneling mechanism is similar to other automatic tunneling mechanisms, such as IPv6 6to4 tunneling, ISATAP is designed for transporting IPv6 packets within a site, not between sites.

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

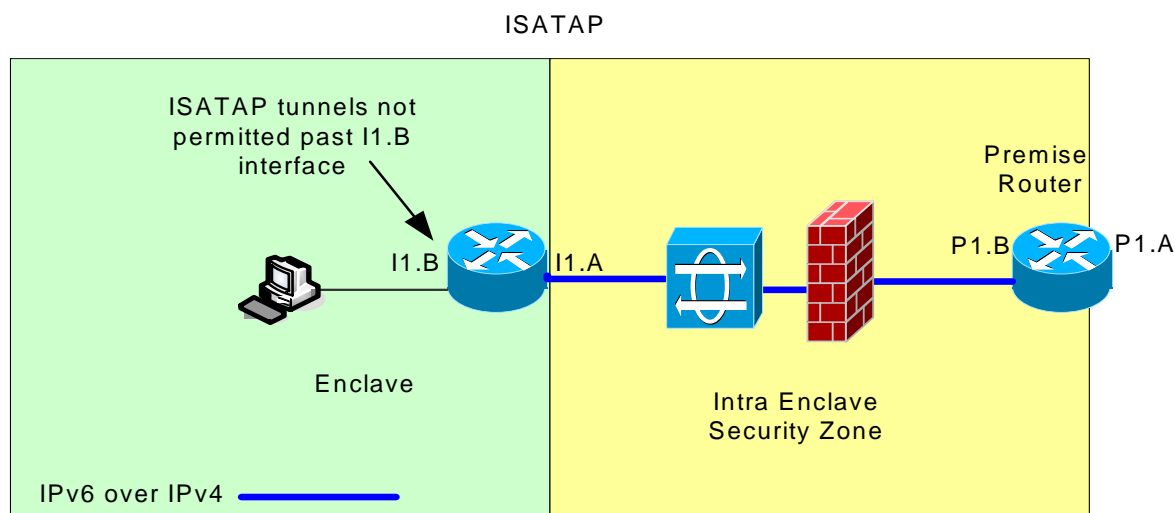


Figure 11-6. ISATAP Architecture

- (NET1950: CAT I) The IAO/NSO will ensure ISATAP tunnels do not breach the perimeter boundary.
- (NET1951: CAT II) The IAO/NSO will ensure ISATAP tunnels terminate at an interior router.
- (NET1954: CAT II) The IAO/NSO will ensure in ISATAP architectures, the enclave boundary does not have any other IPv6 Transition Mechanisms implemented.

11.3.2.2 Tunnel Broker

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

- (NET1960: CAT I) The IAO/NSO will ensure AG does not have Tunnel Broker solutions implemented for IPv6 transition.

11.3.2.3 6to4 Tunnels

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

6to4 tunnels are required to discard unexpected protocol 41 packets and inspect IPv6 traffic at the decapsulator end-point as mentioned above in IPv6 Encapsulation for IPv6 Transition section. The vulnerabilities defined in the IPv6 Encapsulation for IPv6 transition apply to automatic 6to4 tunnels also.

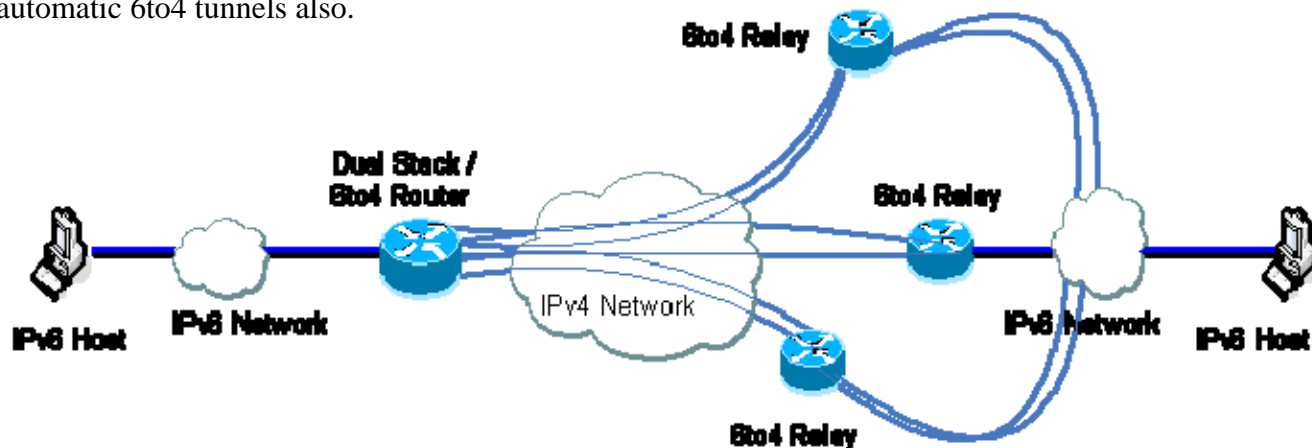


Figure 11-7. 6to4 Relay Architecture

- (NET1965: CAT II) The IAO/NSO will ensure the ingress filter drops unexpected protocol 41 packets at the 6to4 site router before sensor inspection.

11.3.2.4 Teredo

Teredo is a tunneling mechanism that allows nodes located behind NAT devices to obtain global IPv6 connectivity. In a Teredo implementation the IPv6 packet is encapsulated in IPv4 UDP.

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

- *(NET1970: CAT I) The IAO/NSO will ensure Teredo is blocked by filtering UDP protocol 17 port 3544 in the enclave environment.*

11.4 IPv6 Protocol Translation for IPv6 Transition

There is a variety of translation mechanisms available or being considered by the IETF for the IPv6 transition. Some of these transition mechanisms are:

- Network Address Translation-Protocol Translation (NAT-PT)
- TCP-UDP Relay
- Bump-in-the-Stack (BIS)
- Dual Stack Transition Mechanism (DSTM)
- SOCKS-Based Gateway

These protocol translation mechanisms become more relevant as IPv6 becomes more prevalent, and even as IPv6 becomes the protocol of choice to allow legacy IPv4 systems to be part of the overall IPv6 network. The translation mechanisms that will be discussed in this release are DSTM and NAT-PT.

DSTM will provide a late-stage mechanism for dual-stack nodes in an IPv6-only network environment. DSTM is in early stages in IETF draft and could see significant changes prior to standardization, but merits mentioning as a promising tool in the future.

At the time of this writing many of the listed translation mechanisms identified in this section do not meet the needs of the Department of Defense IPv6 Transition Office (DITO) Information Assurance Guidance for M02 and Milestone Objective 3 (M03) and are not approved.

- *(NET1975: CAT I) The IAO/NSO will ensure TCP-UDP Relay is not implemented in the enclave.*
- *(NET1976: CAT I) The IAO/NSO will ensure Bump-in-the-Stack (BIS) is not implemented in the enclave.*
- *(NET1977: CAT II) The IAO/NSO will ensure Dual Stack Transition Mechanism (DSTM) is not implemented in the enclave.*

- (NET1979: CAT I) The IAO/NSO will ensure SOCKS-Based Gateway is not implemented in the enclave.

11.4.1 NAT-PT Architecture

The NAT-PT translation mechanism translates at the network layer between IPv4 and IPv6. It will be primarily used where new hosts run only native IPv6 or the network has not implemented the dual-stack approach of IPv6. NAT-PT does not support IPv6 extension headers or IPv4 options and is incompatible with IPsec. NAT-PT is also known to have performance issues, and very vulnerable to DoS attacks.

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

The implementation of this architecture requires the following guidelines be implemented. Referencing the NAT-PT diagram, interface I1.B will not receive any IPv6 traffic. In the NAT-PT architecture there must not be any IPv4 in IPv6 tunnel traffic between interfaces I1.A and P1.B. The enterprise will not have any other IPv6 Transition Mechanisms implemented in the enclave when supporting NAT-PT architecture.

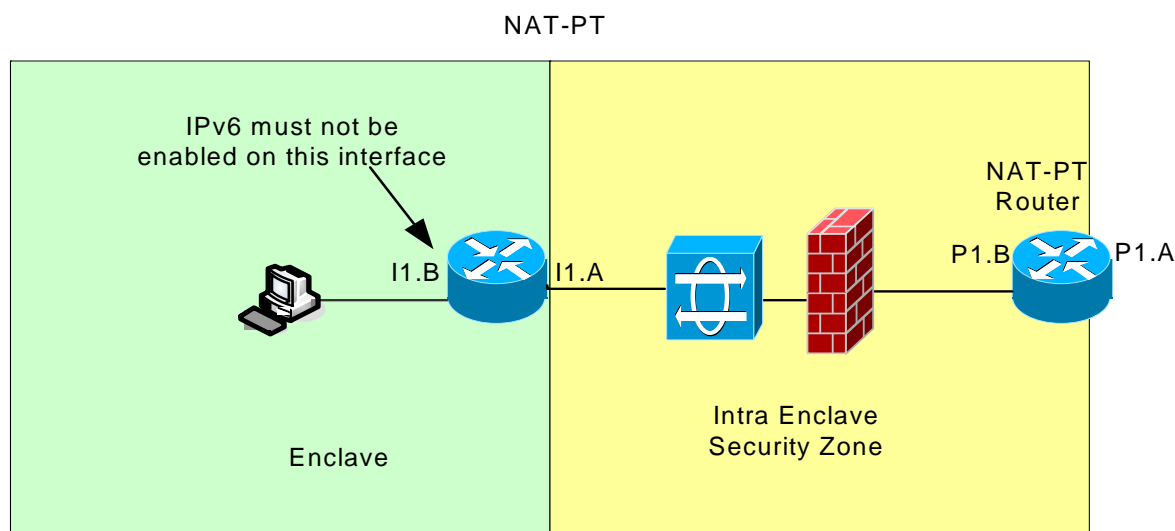


Figure 11-8. NAT-PT Architecture

- (NET1990: CAT II) The IAO/NSO will ensure interfaces supporting IPv4 in NAT-PT Architecture do not receive IPv6 traffic.
- (NET1992: CAT II) The IAO/NSO will ensure in NAT-PT architecture there is no tunneled IPv4 in IPv6 traffic.

- *(NET1993: CAT II) The IAO/NSO will ensure the enclave boundary does not have any other IPv6 Transition Mechanisms implemented when supporting NAT-PT.*

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

ASD (NII) Memo, "Internet Protocol Version 6" (IPv6), June 9, 2003

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://www.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>

CISCO, SAFE Blueprint, Best Practices for Securing Routing Protocols

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

DoD-CERT Home Page – <http://www.cert.mil>

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>

Firewall References

Guidelines on Firewalls and Firewall Policies, NIST Special Publication 800-41, January 2002

U.S. Government Firewall Protection Profile for Medium Robustness Environments, NIAP, July 2002

Firewall Evolution, Deep Packet Inspection, Ido Dubrawsky, July 2003

The Perils of Deep Packet Inspection, Dr. Thomas Porter, January 2005

Stateful Inspection Technology, Checkpoint, August 2005

Addressing the Limitations of Deep Packet Inspection with Complete Content Protection, FORTINET Whitepaper, 2004

An Introduction to Network Firewalls and the Firewall Selection Process, March 25, 2003 Whitepaper

VPN References

NIST Special publication 800-77 (draft), Guide to IPsec VPNs

Virtual Private Networks (VPNs) and Encrypted Connections, Information Assurance Policy & Management Considerations February, 2006, MITRE

FINAL DSAWG Position Paper v5A 3/10/06. Tunneling Classified Information over other than SIPRNet

<http://ipsec.cybersabotage.com/ipsec.htm> Rhys Haden 1998-2002

Communication News March 2005 Issue: SSL VPN vs IPsec VPN

Face Off: IPsec vs SSL VPNs Whitepaper

IPv6 References

Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objectives 2 (MO2), January 2006

[RFC1981] J. McCann, S. Deering, and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996

[RFC2401] E. Nordmark & R. Gilligan, "Basic IPv6 Transition Mechanisms", October 2005

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998

[RFC2460] S. Deering. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998

[RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998

[RFC2470] R. Coltun, D. Ferguson and J. Moy, "OSPF for IPv6", RFC 2470, December 1999

[RFC3053] A. Durand, P. Fasano, I. Guardini, D. Lento, " IPv6 Tunnel Broker", RFC 3513, January 2001

[RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001

[RFC3177] Internet Architecture Board and Internet Engineering Steering Group, " IAB/IESG Recommendations on IPv6 Address Allocations to Sites ", RFC 3177, September 2001

[RFC3484] Draves, R. "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003

[RFC3513] Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003

IPv6 for Security Professionals v5.5.0, Command Information, 2006

[V6SEC] Savola, P., "IPv6 Transition/Co-existence Security Considerations", Work in Progress, October 2004

[V64IPSEC] Graveman, R., et al., "Using IPsec to Secure IPv6-over-IPv4 Tunnels", Work in Progress, December 2004

North American IPv6 Task Force (NAv6TF) Technology Report, M. Kaeo, D. Green, J. Bound, and Y. Pouffary, "IPv6 Security Technology Paper" v1.0, July 22, 2006

CISCO, C. Popoviciu, E. Levy-Abegnoli, P. Grossetete, "Deploying IPv6 Networks", February 2006

CISCO, CISCO IOS IPv6 Configuration Guide, Release 12.4, Implementing Tunneling for IPv6

CISCO, IPv6 Deployment Strategies, December 23, 2002

NSA, N. Ziring, "Router Security Configuration Guide Supplement – Security for IPv6 Routers", v0.6, March 7, 2006

Recommendations for Filtering ICMPv6 Messages in Firewalls draft-ietf-v6ops-icmpv6-filtering-recs-03.txt, Davies & Mohacsi, February 13, 2007

Use of VLAN for IPv4 - IPv6 Coexistence in Enterprise Networks, Tim Chown, University of Southampton Southampton, Hampshire SO17 1BJ United Kingdom

Device Management

CISCO – Configuring a Terminal /Comm Server, June 13, 2005

CISCO IOS Security Configuration Guide

Cisco Safe Blueprint for Small, Midsize, and Remote-User Networks

Switches and VLANS

CISCO – Configuring Port Security, Software Configuration Guide – Release 12.2(31)SG

This page is intentionally blank.

APPENDIX B. FILE EXTENSIONS

This is not a recommendation to enable blocking of active web content, but to be capable of blocking it should it be necessary. The decision to block active content, excluding viruses, should be weighed carefully, as blocking active content will render many websites unusable or difficult to use. Executable files in email attachments that could be blocked include the following:

.abe .cmd .eml .ins .mdb .mst .reg .url .wsf .adp .com .exe
.isp .mde .pcd .scr .vb .wsh .bas .cpl .hlp .js .msc .pif
.sct .vbe .bat .crt .hta .jse .msi .pl .scx .vbs .chm .dll
.inf .lnk .msp .pot .shs .wsc

In addition to this reference, it is recommended to review the Outlook Email Security in the Midst of Malicious Attacks document by NSA.

This page is intentionally blank.

APPENDIX C. BOGON LIST

The IP address ranges indicated below are a static list of bogons that be filtered. It does not contain all unallocated subnets that should be filtered. The list of unallocated subnets change monthly and the administrator should establish a procedure to review IANA's website to get the most current list.

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 ip 172.16.0.0 0.15.255.255 any log	Private Network
192.0.0.192	Deny		access-list 101 deny ip 192.0.0.192 0.0.0.0 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 0.0.128.255 any log	IANA - Reserved 192.0.0.0 - 192.0.127.255
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 255.0.0.0 0.255.255.255 any log	Unallocated / IANA Reserved

This page is intentionally blank.

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	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
INFOCON	Information Operations Condition
INFOSEC	Information Security
INFOWAR	Information Warfare
IOS	Internetworking Operating System
IP	Internet Protocol
IPS	Intrusion Protection System
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 Identifier
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 blank.

APPENDIX E. IPV6 ADDRESSES

The list of addresses were captured from the IANA web site dated 2007/04/04. For current information on IPv6 address space please visit the IANA website.

<http://www.iana.org/assignments/ipv6-address-space>

IPv6 Prefix	Allocation	Reference	Note
0000::/8	Reserved by IETF	[RFC4291]	[1] [5]
0100::/8	Reserved by IETF	[RFC4291]	
0200::/7	Reserved by IETF	[RFC4048]	[2]
0400::/6	Reserved by IETF	[RFC4291]	
0800::/5	Reserved by IETF	[RFC4291]	
1000::/4	Reserved by IETF	[RFC4291]	
2000::/3	Global Unicast	[RFC4291]	[3]
4000::/3	Reserved by IETF	[RFC4291]	
6000::/3	Reserved by IETF	[RFC4291]	
8000::/3	Reserved by IETF	[RFC4291]	
A000::/3	Reserved by IETF	[RFC4291]	
C000::/3	Reserved by IETF	[RFC4291]	
E000::/4	Reserved by IETF	[RFC4291]	
F000::/5	Reserved by IETF	[RFC4291]	
F800::/6	Reserved by IETF	[RFC4291]	
FC00::/7	Unique Local Unicast	[RFC4193]	
FE00::/9	Reserved by IETF	[RFC4291]	
FE80::/10	Link Local Unicast	[RFC4291]	
FEC0::/10	Reserved by IETF	[RFC3879]	[4]
FF00::/8	Multicast	[RFC4291]	

Notes:

- [0] The IPv6 address management function was formally delegated to IANA in December 1995 [RFC1881].
- [1] The "**unspecified address**", the "**loopback address**", and the **IPv6 Addresses with Embedded IPv4 Addresses** are assigned out of the 0000::/8 address block.
- [2] 0200::/7 was previously defined as an OSI NSAP-mapped prefix set [RFC-gray-rfc1888bis-03.txt]. This definition has been deprecated as of December 2004 [RFC4048].
- [3] The **IPv6 Unicast space** encompasses the entire IPv6 address range with the exception of FF00::/8. [RFC4291] IANA unicast address assignments are currently limited to the IPv6 unicast address range of 2000::/3. IANA assignments from this block are registered in the IANA registry: [iana-ipv6-unicast-address-assignments](http://iana.org/assignments/iana-ipv6-unicast-address-assignments).
- [4] FEC0::/10 was previously defined as a **Site-Local scoped address prefix**. This definition has been deprecated as of September 2004 [RFC3879].
- [5] 0000::/96 was previously defined as the "**IPv4-compatible IPv6 address**" prefix. This definition has been deprecated by [RFC4291].

This page is intentionally blank.

APPENDIX F. VULNERABILITY UPDATES

Deleted Vulnerabilities – Many of the following deletions were combined with other vulnerabilities. Most can be found in the new Device Management Section. Duplication was removed in many areas.

- *(NET0280: CAT III) The IAO/NSO will ensure that a documented procedure is in place to validate loaded image files, 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.*
- *(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*
- *(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.*
- *(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.*
- *(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*

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

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

- *(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.*

- *(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.*

- *(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.*

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

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

- *(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.*

- *(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.*

- *(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.*
- *(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.*
- *(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.*
- *(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.*
- *(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.*
- *(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:*
- *(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.*
- *(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.*
- *(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.*
- *(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).*
- *(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.*
- *(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.*
- *(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.*

Modified Vulnerabilities – The modified vulnerabilities further clarify and add detail where necessary. Some modifications were a result of splitting previous vulnerabilities that had multiple checks. **BLUE font highlights the change.**

Section 2

- *(NET0130: CAT III) The IAO/NSO will ensure that all external connections are validated and approved by the CAO and DAA, and SNAP or SCAO requirements are met, and MOA and MOU is established between enclaves, prior to connections.*
- *(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. A static route is the only acceptable route to an AG.*
- *(NET0166: CAT III) The IAO/NSO will ensure the AG network service provider IP addresses are not redistributed into or advertised to the NIPRNet or any router belonging to any other Autonomous System (AS) i.e. to another AG device in another AS.*
- *(NET0180: CAT II) The IAO/NSO will ensure all public address ranges used on the NIPRNet are properly registered with the .MIL Network Information Center (NIC).*
- *(NET0190: CAT III) The IAO/NSO will ensure that workstation clients' real IPv4 addresses are not revealed to the public by implementing NAT on the firewall or the router.*

Section 3

- *(NET1170: CAT III) The IAO will ensure that only firewalls that obtained validation against the DoD Application-Level for Medium Robustness Environments Protection Profile (PP) are placed in the network infrastructure meeting a Common Criteria PP of EAL 4 or greater.*
- *(NET1180: CAT II) The IAO/NSO will ensure that DMZ Architecture is implemented, providing boundary protection for classified and sensitive architectures that interconnect enclaves.*
- *(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 premise router to form the DMZ.*
- *(NET1190: CAT II) The IAO will ensure that firewall assets implemented will have full packet awareness as provided by application-level gateways, hybrid firewalls or a non application-level firewall solution using proxy servers or application-proxy gateways.*
- *(NET1162: CAT II) The IAO will ensure that the firewall policy is in accordance with DoD Instruction 8551.1 and Appendix C.*

- (NET1163: CAT I) *The IAO will ensure that the Enclave perimeter is protected via deny by default policy implemented at the perimeter router or at the firewall, and the site is in compliance with all perimeter filtering defined in the perimeter and router sections of the Network STIG.*
- (NET1250: CAT II) *The FA will ensure the firewall will not utilize any services or capabilities other than firewall software (i.e., DNS servers, e-mail client servers, ftp servers, web servers, etc.), and if these services are part of the standard firewall suite, they will be either uninstalled or disabled.*
- (NET1300: CAT III) *The IAO will ensure administrator logons, changes to the administrator group, and account lockouts are logged.*

Section 4

- (NET0400: CAT II) *The router administrator will ensure neighbor authentication with IPsec or MD5 Signatures are implemented for interior 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 trusted Autonomous Systems.*
- (NET0722: CAT III) *The router administrator will ensure PAD services are disabled **unless approved by the DAA** .*
- (NET0728: CAT III) *The router administrator will ensure DHCP Services are disabled **on premise routers**.*
- (NET0740: CAT II) *The router administrator will ensure HTTP servers are disabled.*
- (NET0810: CAT III) *The IAO/NSO will ensure **the enclave has** two Network Time Protocol (NTP) servers defined to synchronize time.*
- (NET0812: CAT III) *The IAO/NSO will ensure that all internal routers are configured to use the premise router to synchronize time **in an external trusted NTP implementation**.*
- (NET0910: CAT II) *The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in **Appendix C and DoD Instruction 8551.1** for all ports and protocols required for operational commitments.*
- (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 Destination Unreachable** (message number 3) **port unreachable** (code 4), are permitted inbound with the following exception: **Must be denied from external AG addresses, otherwise permitted.***

- (NET0920: CAT II) *The router administrator will bind the ingress ACL filtering packets entering the network to the external interface on an inbound direction.*
- (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.*
- (NET0960: CAT II) *The IAO/NSO will implement tcp intercept features provided by the router or implement a filter to rate limit tcp syn to protect servers from any TCP SYN flood attacks from an outside network.*
- (NET0186: CAT III) *The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.*

Section 5

- (NET0630: CAT II) *The IAO/NSO will ensure an OOB management network is in place for MAC I systems or 24x7 personnel have immediate console access (direct connection method) for communication device management.*
- (NET0652: CAT II) *The IAO/NSO will ensure modems are not connected to the console port.*
- (NET0655: CAT III) *The system administrator will ensure that the device auxiliary port is disabled if a secured modem providing encryption and authentication is not connected.*
- (NET0680: CAT II) *The system administrator will ensure in-band management access to the device is secured using an encryption such as AES, 3DES, SSH, or SSL.*
- (NET0690: CAT III) *The system administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*
- (NET1040: CAT III) *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.*
- (NET1666: CAT II) *The IAO/NSO will ensure that all SNMP community strings and usernames are protected via technology that secures using an encryption such as AES, 3DES, SSH, or SSL.*
- (NET1762: CAT II) *The IAO/NSO will ensure that all in-band sessions to the NMS is secured using an encryption such as AES, 3DES, SSH, or SSL.*

Section 6

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

- (NET0440: CAT II) The IAO/NSO will ensure when an authentication server is used for administrative access to the device, only one account is defined locally for use in an emergency (i.e., authentication server or connection to the device is down).
- (NET0460: CAT I) The IAO/NSO will ensure each user accessing the device locally has their own account with username and password.
- (NET0465: CAT II) The IAO/NSO will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.
- (NET0470: CAT II) The IAO/NSO will immediately have accounts removed from the authentication server or device, which are no longer required.
- (NET0667: CAT II) To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure device management ~~in-band access enforces the following security restrictions:~~ is restricted by two-factor authentication (e.g., Secure ID, DoD PKI, or alternate token logon).
 - ~~— Encryption of management session (FIPS 140-2 validated encryption)~~
 - Auditing
 - ~~— Two factor authentication discussion; reference Section 3.4.3.1.~~
- (NET1020: CAT III) The IAO/NSO will ensure that all attempts to any port, protocol, or service that is denied are logged.
- (NET1021: CAT III) The IAO/NSO will configure all devices to log severity levels 0 through 6 and send log data to a syslog server.
- (NET1286: CAT III) The IAO/NSO will ensure the audit log data is backed up weekly.

Section 9

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

Section 10

- (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 an encryption such as AES, 3DES, SSH, or SSL.
- (NET1800: CAT II) The IAO/NSO will ensure VPNs are established as tunnel type VPNs.

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

Renamed Vulnerabilities – Total of 32

NEW	OLD		NEW	OLD
NET0345	NET1170		NET0949	NET0966
NET0346	NET1180		NET1622	NET0630
NET0365	NET1190		NET1623	NET0645
NET0351	NET1200		NET1624	NET0650
NET0368	NET1162		NET1628	NET0652
NET0369	NET1163		NET1629	NET0655
NET0375	NET1240		NET1635	NET0664
NET0377	NET1250		NET1636	NET0665
NET0378	NET1252		NET1637	NET0670
NET0379	NET1254		NET1638	NET0680
NET0384	NET1260		NET1639	NET0685
NET0390	NET1290		NET1640	NET0690
NET0445	NET0667		NET1645	NET0681
NET0911	NET0980		NET1646	NET0682
NET0912	NET0990		NET1834	NET1625
NET0918	NET1000		NET1837	NET1630
NET0928	NET0186			

New Vulnerabilities – Total of 133

NET0167	NET0445	NET0943	NET1802	NET1930
NET0168	NET0667	NET0944	NET1816	NET1931
NET0186	NET0742	NET0945	NET1822	NET1934
NET0196	NET0744	NET0946	NET1823	NET1935
NET0201	NET0802	NET0947	NET1824	NET1937
NET0270	NET0813	NET0948	NET1826	NET1938
NET0347	NET0897	NET0953	NET1827	NET1940
NET0348	NET0898	NET0954	NET1829	NET1942
NET0355	NET0899	NET0980	NET1830	NET1944
NET0366	NET0900	NET0990	NET1832	NET1945
	NET0901	NET1000	NET1833	NET1950
NET0380	NET0902	NET1022	NET1835	NET1951
NET0381	NET0903	NET1023	NET1836	NET1954
NET0386	NET0906	NET1111	NET1838	NET1960
NET0388	NET0907	NET1113	NET1839	NET1965
NET0391	NET0911	NET1114	NET1850	NET1970
NET0395	NET0912	NET1281	NET1900	NET1975
NET0396	NET0915	NET1287	NET1901	NET1976
NET0398	NET0916	NET1288	NET1905	NET1977
NET0402	NET0918	NET1289	NET1908	NET1979
NET0408	NET0921	NET1299	NET1910	NET1990
NET0412	NET0923	NET1421	NET1911	NET1992
NET0431	NET0924	NET1432	NET1914	NET1993
NET0432	NET0927	NET1433	NET1915	
NET0433	NET0928	NET1441	NET1918	
NET0434	NET0941	NET1621	NET1919	
NET0441	NET0942	NET1647	NET1920	

This page is intentionally blank