NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 8, Release 8

23 January 2015

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

This document is a requirement for all DoD-administered systems and all systems connected to DoD networks. These requirements are designed to assist Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), Network Security Officers (NSOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

Note: The Network Devices and Policy STIGs are written to address pre-JIE (Joint Information Environment) architectures/enclaves. While some of the requirements will carry over into guidance directly addressing JIE architecture, there may be differences between pre-JIE and JIE requirements due to the differences in scope and surrounding infrastructure; therefore the Network Devices and Policy STIGs will not apply to JIE environments. JIE-specific device STIGs are being developed for devices used in the JIE framework. These include:

- Network JIE Router-L3 Switch
- Network JIE L2 Switch
- Network JIE Firewall
- Network JIE IDS-IPS

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil. DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA FSO maintenance release schedule.

2. ASSESSMENT CONSIDERATIONS

2.1 White Papers

The white papers packaged with the Network Infrastructure STIG assist the reader in subject areas without the actual procedures defined in the STIG. Their intent is to assist the reader with illustrations and tables to visualize the need for safeguards in the VMS database, as well as provide a quick glance of specific topics. For example, the Intrusion Detection and Prevention Systems – Security Guidance at a Glance white paper contains specific technology related vulnerabilities for intrusion detection systems (IDS) and intrusion prevention systems (IPS), but does not contain any associated VUL-IDs. As of the writing of this release, the following documents are available:

- *IDPS Systems – Security Guidance at a Glance*
- *Network Access Control – Security Guidance at a Glance*
- *Network Management – Security Guidance at a Glance*
- *Virtual Local Area Network (VLAN) Provisioning – Security Guidance at a Glance*

3. ENCLAVE PERIMETER

An enclave is a computing environment under the control of a single authority with personnel and physical security measures. Enclave terminology used in the STIG and white papers refers to sub-enclave and regional enclave. The sub-enclave reference is intended to describe the sub-enclaves (i.e., base, camp, post, station, etc.). The sub-enclaves are extensions of the private Intranet having connectivity to the enterprise Regional Enclave often termed Network Operations Center (NOC).

3.1 Enclave Protection Mechanisms

Controlling the flow of network traffic between networks employing differing security postures is required. By using Defense-in-Depth practices such as: 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 Information Technology (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 (such as, System Security Authorization Agreement [SSAA]) or the emerging DoD Risk Management Framework (RMF) process.

The perimeter firewall will allow web traffic to pass through to the web application since the IP address and port will likely be open. The reverse web proxy (RWP) will terminate the initial session and validate the destination IP address corresponds to an internal web server. The web content filter (WCF) will check the data for malware using current signatures and then will pass back to the RWP. The RWP should then create a new session between itself and the web server and passes the data it received from the WCF. The web application firewall (WAF) inspects the inbound connection for application protocol and data element problems. The web server will then terminate the connection from the RWP and processes the inbound data. If the request requires an application (A/P) server a new connection is made from the web server to the application server. The A/P server processes the web server request. If the request requires a call to a database (DB) then a new connection is made from the A/P server to the DB server. The DB security gateway inspects the inbound connection for protocol and behavioral problems. The DB then processes the request after terminating the connection from the A/P firewall.

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

The minimum required components are briefly discussed here and depending on 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 required by all medium robust DoD networks.

Sensors should be strategically placed to monitor traditional and wireless traffic. The number of sensors required is dependent of the architecture and its role, sensor capacity limitations, etc. A key requirement is avoiding sensor data overflow, thus multiple sensors may be required in a Regional Enclave. A single sensor may provide the capabilities needed at a local enclave (extension of a Regional Enclave) depending on the architecture and functions the local enclave provides.

If the enclave has an Approved Gateway (AG), then an external IDPS will be required. Additional components in the diagram may be required depending on the design of the enclave. Review appropriate STIGs for details.

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 in detail in the STIG under its appropriate sections.

It is recommended the reader review all the perimeter policies defined in the Network Infrastructure STIG for specific requirements pertaining to the Regional Enclave, DECC, and local enclaves.

Network Test Access Ports (TAPs) may be considered in network designs where promiscuous implementations are implemented. TAPs can create a monitoring access port between any two network devices, including switches, routers, firewalls, and more. TAPs can function as access ports for any monitoring devices used to collect in-line data. Protocol analyzers, Remote Network Monitoring (RMON) probes, IDSs, and other management and security solutions can be connected to the network via TAPs. SPAN is probably a more widely deployment since it is very scalable and is used with inline implementations.

Restricted LAN segments provide client services and backend servers, such as internal Domain Name Service (DNS) with split DNS architecture, backend mail servers, Active Directory Domain Controller (AD DC), file and print servers, File Transfer Protocol (FTP), private Hyper Text Transfer Protocol (HTTP) servers and various proxies. These services are generally located in an Enclave DMZ.

3.2 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.

3.3 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 Secret Internet Protocol Router Network (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 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 Authorizing Official (AO).

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 the SIPRNet. The policy must ensure 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.

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

3.4 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 (CSUs), data service units (DSUs) and demarcation points (DEMARCs) 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 in a locked closet.

3.5 Approved Gateway/Internet Service Provider Connectivity

An Approved Gateway (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. Analysis of DoD reported incidents reveal current protective measures at the NIPRNet boundary points are insufficient. Documented ISPs and validated architectures for DMZs are necessary to protect internal network resources from cyber attacks originating from external Internet sources by protective environments. Direct ISP connections are prohibited unless written approval is obtained from the Global Information Grid (GIG) Waiver Panel or the Office of the DoD CIO who directs the GIG Panel.

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

Any enclave with one or more AG connections will have to take additional steps to ensure 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 Denial of Service (DoS) attack, as well as provide a backdoor into the NIPRNet. The DoD enclave must ensure 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 the protocol used, no protocol will redistribute routes into the AG and 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 CNDSP.

The enclave perimeter requirement for filtering will include USCYBERCOM and Ports, Protocols, and Services (PPS) Vulnerability Assessment (VA) filtering guidelines. 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 the source Internet Protocol (IP) address belongs to the enclave.

3.6 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 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 AO.

3.7 Network Layer Addressing

The method by which cooperating enclaves exchange Internet Protocol, version 6 (IPv6) traffic must be approved in accordance with the DISN connection approval process to ensure compliance with Information Assurance (IA) policies. DoD IPv6 Transition Office (DITO) and ASD-NII has developed a plan for the DoD IPv6 transition to progress through several milestones, each representing increased adoption of IPv6 features. Milestone Objective 1 (MO1) permits the fundamental IPv6 capability needed for limited operation within enclaves. Milestone Objective 2 (MO2) permits a subset of IPv6 features and applications needed for inter-domain networking. MO2 version 2 (MO2v2) permits partial IPv6 functional parity with Internet Protocol, version 4 (IPv4). Milestone Objective 3 (MO3) permits full IPv6 functional parity with IPv4 and includes additional features unique to IPv6. The following enclave network system security components will require examination and modification for IPv6:

- Network Protection: 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: Core routers and switches
- Assurance Devices: HAIPE, encryptors
- Configuration: DNS, Network Address Translation (NAT), Access Control List (ACL), and PPS
- Infrastructure and Services: Dynamic Host Configuration Protocol (DHCP), DNS, network IDS, Network Time Protocol (NTP)

To ensure a successful migration to IPv6, there will be a transitional period when IPv4 and IPv6 are used simultaneously to ensure network connectivity. MO2 will employ a phased approach based on eleven architectures. Reference DITO IPv6 documents on the Army Knowledge Online (AKO) portal for more detail.

3.8 IP Address Registration

The DoD Network Information Center (NIC) assigns blocks of network addresses to local administrators. Non-DoD activities have been assigned networks by the SIPRNet Support Center (SSC) and have been given the domain name .sgov.gov. 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

Neither RFC1918 address space nor NAT are approved to be used on the SIPRNet and must receive DISN Security Accreditation Working Group (DSAWG) approval, if implemented.

3.9 IPv4 Address Privacy

Using the private addressing scheme in accordance with RFC 1918 will require an organization to use 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.

NOTE: If the site has implemented an application-level firewall, hiding of the clients' real address can also be done by enabling the proxies.

3.10 IPv6 Addresses

An IPv6 address contains 128 bits consisting of two 64 bit parts. The left most 64 bits contain the network part (prefix) and the right most 64 bits contain the host part (interface identifier), as shown below. 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 Inter-Domain 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.

2001:0db8:0000::/48 or
2001:db8::/48

Appendix D contains a dated IANA IPv6 address allocation for a quick reference. For current IPv6 allocations, visit the IANA web site identified in Appendix D. Table 3-1 shows some common IPv6 addresses and some addresses that have specific security guidance found in this STIG.

Table 3-1: Well-Known IPv6 Address

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

The NIC will assign blocks of IPv6 network addresses 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 to 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.

Internet Engineering Task Force’s (IETF's) Internet Protocol Next Generation (IPNG) working group has recommended that the address block given to a single edge network, which may be recursively, sub-netted 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).

3.11 Dynamic Host Configuration Protocol Version 4

With an increase in Transmission Control Protocol/Internet Protocol (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 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.

3.11.1 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.

3.11.2 Stateful Autoconfiguration DHCPv6

Currently, many vendors are not prepared for Dynamic Host Configuration Protocol Version 6 (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 (PD) 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.

3.11.3 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 SAs 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 DoS 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, defined in RFC 3756, were present in IPv4 Address Resolution Protocol (ARP) attacks. IPSec Authentication Header (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 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 they 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.

3.12 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.

4. FIREWALL

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. This section identifies and helps 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.

4.1 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 is 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: 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.

4.2 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.

4.3 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.

4.4 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.

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.5 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; and
- User specific controls, including blocking certain content types for certain users.

4.6 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.

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.

Many vendors are providing integrated router, firewall, and IPS/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.

4.7 Content Filtering

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

- An application-level firewall at the perimeter to protect the whole Enclave to include the Security Domains.

- A non application-level firewall at the perimeter (e.g., packet-filter, stateful inspection, deep packet inspection) with a dedicated proxy server or application-proxy gateway protecting every Security Domains.

- A Hybrid firewall at the perimeter to protect the whole Enclave to include the Security Domains capable of application-proxy functionality.

Due to technological advances there are devices, such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or Stateful Inspection firewall, in collaboration with application level proxy devices to service all connections 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.

Data entering or leaving the site must use a proxy or the firewall is configured to implement the content, protocol, and flow control inspections defined below.

- DNS Inspection: Protocol conformance, malformed packets, message length and domain name integrity. Query ID and port randomization for DNS query traffic must be enabled.

- SMTP and ESMTP Inspection: Extended SMTP and SMTP inspection will be configured to detect spam, phishing, and malformed message attacks.

- FTP: FTP is not a recommended file transfer solution. Reference the Enclave STIG for conditional guidance on FTP. The firewall should inspect FTP traffic and drop connections with embedded commands, truncated commands, provide command and reply spoofing, drop invalid port negotiations, and protect FTP servers from buffer overflow.

- HTTP: Inspection will be configured to filter Java applets and ActiveX objects to meet the enclave security policy. Review the security policy with the Information Assurance Officer and look for Java and ActiveX filters if the security policy requires restrictions.

4.8 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 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 and all tunnel endpoints are in a deny-by-default posture. One or the other will satisfy the requirement at the enclave boundary.

4.9 Tunnels

The default stance is that IP tunnels are disabled. This guidance does not recommend whether tunnels need to be disabled or enabled, as that is determined by operational necessity, only that the default position is “disabled”. The threat from tunneling is caused by the fact that tunneled traffic has a complete IP packet encapsulated within the payload of the outer tunnel layer(s). If tunneled traffic enters a network, the inner IP packet may evade the normal scrutiny of firewalls, IDS, or other security measures. Once inside, the tunneled traffic could be de-encapsulated allowing the inner IP packets to be delivered to inside nodes. Any allowed tunnel traffic must be properly filtered and secured.

The default guidance is:

- Do not enable tunnels unless it is part of the planned topology to use the known tunnel.
- Do apply filtering to prevent tunnel traffic from entering the network.

Tunneling capabilities can be available as basic operating system features or from various tool sets or network management software, but they should all be disabled by default in well behaved implementations. The filtering guidance is a backup measure in case any weak implementations accept a tunneled packet despite not being explicitly configured to do so. The IPv4-in-IPv4 specification (RFC 2003), in particular, does not contain strong enough language to require tunnel traffic to be dropped by default, especially when the de-encapsulator and final recipient is one and the same node.

The outer tunneling layer can be IPv4 or IPv6; therefore, some of the actions below are technically IPv4 guidance (e.g. IP4-in-IPv4 tunnels). There is no limit, however, to the number of tunnel layers and an IPv6 packet could be buried several layers deep, and so all tunnels must be filtered in order to preserve security.

Report the detection of all outbound tunnel packets as a security event. Outbound tunnel packets should trigger a security alert. These events are likely due to unauthorized users or malware. L2TP tunneling technologies that must be disabled by default that pose the same threat as IP-in-IP tunneling described above, since they could potentially carry an IPv6 packet. If they are needed, additional guidance for enabling them is contained in the Backbone Transport STIG. The tunneling technologies listed here may be in use in DoD networks today.

The L2TP protocol carries a link layer packet within an outer IP tunneling packet. It is therefore even more likely to evade security scrutiny (IDS, etc.) since the inner IP packet is buried an extra layer deep. Disable any use of L2TP Tunneling - Refer to additional STIG guidelines for enabling L2TP tunneling. If required, L2TPv3 is a more robust implementation using authentication. This guidance recognizes that although L2TP's default port is 1701, it may be configured to use other ports. L2TP must not be configured on any port for the default stance.

There are a number of outdated tunneling schemes that should be blocked to avoid importing IPv6 packets. These must be blocked at the perimeter router or firewall or denied by the deny-by-default policy.

- Drop Source Demand Routing Protocol (SDRP)
- AX.25 tunneling
- IP-within-IP Encapsulation Protocol
- EtherIP protocol
- Encapsulation Header protocol
- PPTP protocol

4.9.1 Tunnel Inner Layer Packet

Once de-encapsulated, the inner IP layer of a tunneled packet is no different than any other IP packet. Therefore, the inner IP layer must be filtered at the tunnel exit point network. In fact some packets are more dangerous, such as attacks against Neighbor Discovery where a required 255 count in the hop limit field could potentially be delivered.

This guidance describes three ways in which the inner IP layer filtering task may be accomplished, depending on the advances in firewall technology. Refer to NSA firewall design considerations for IPv6 section 5.2 for a description of desired firewall filtering capabilities for tunneled traffic. This reference document defines primary filtering as a firewall that can filter the inner source and destination IP addresses of a tunneled packet in a manner similar to filtering source and destination ports of a TCP or UDP packet. Secondary filtering capability is defined to be the ability to fully filter the entire inner IP layer to the same degree an un-tunneled packet is filtered.

The Primary guidance assumes an advanced firewall with the capability to perform both the primary and secondary filtering functions as explained above. Alternative 1 assumes that the firewall can perform only the primary filtering function. Alternative 2 assumes the firewall cannot do either primary or secondary filtering as may be the case with some existing firewall products.

For Alternatives 1 and 2, the de-encapsulation point may be an interior router with the filtering of the inner IP layer performed by a secondary firewall. Additional actions are provided to protect the de-encapsulating node itself from being attacked, since this node is in front of the protective filtering.

4.9.2 Tunnel Endpoints with Explicit IP Addresses

IPv6-in-IPv4 tunnels require explicit configuration (on the tunnel exit point node) of both the tunnel exit point IP address and the corresponding tunnel entry point address. These are the outer IP layer destination and source addresses respectively. Unfortunately, the other three tunnel types (4-in-4, 4-in-6, and 6-in-6) have no such requirement built into the standards. The tunnel exit point address will likely need to be configured for these tunnel types (i.e., nodes are not expected to simply accept tunneling by default) and there may be a configuration option to allow the tunnel entry point address to be declared as well. Administrators should attempt to specify both addresses regardless of the IP versions being tunneled if the capability is available for the implementation.

There are no requirements in the GRE tunnel standards to check or restrict IP addresses of the tunnel end points (outer IP layer), so it is purely up to the software implementer. The tunnel exit point address will likely need to be configured for these tunnels (i.e., nodes are not expected to simply accept GRE tunneling by default) and there may be a configuration option to allow the tunnel entry point address to be declared as well. Administrators should attempt to specify both addresses if the capability is available for the implementation.

This vulnerability description and required safeguard is not applicable to MPLS auto tunnels used in traffic engineering. The following three tunnel types (4-in-4, 4-in-6, and 6-in-6) do not have requirements built into the standards. Tunnel exit points must be filtered to ensure these protocols have a valid destination address. If a destination address is not defined for these protocols, then drop the packets via the deny-by-default tunnel policy.

4-in-4 - protocol number: 0x04 (4)
4-in-6 - protocol number: 0x04 (41)
6-in-6 - protocol number: 0x29 (41)
GRE - protocol number: 0x2F (47)
ESP - protocol (50)

The language in the actions above, such as “Drop any ... packet”, should be modified as appropriate to account for the packets of any legitimate and deliberately chosen mechanisms. However, these deliberate tunnels that do not comply with this policy need to be documented in the SSAA detailing purpose and verification data.

4.9.3 Tunnel Endpoints Verified by Filter

Tunnel endpoints that do not have the same controls as the network perimeter requirements become an unprotect entry point into the enclave. These filtering actions enforce proper tunnel endpoint addresses at the border of the tunnel entry and exit points. Filtering is necessary because implementations may not enforce tunnel addresses in all cases. Filtering is also necessary because GRE tunneling implementations are not required by standards to check or enforce tunnel endpoint addresses.

The filter for the tunnel Entry-point must be defined to permit expected traffic that enters the tunnel. All other traffic must be denied. This filter must contain a permit statement that explicitly permits the tunnel type (protocol) and the source and destination address. The filter for the tunnel Exit-point must be defined to permit the expect traffic that exits the tunnel. All other traffic must be denied. This filter must contain a permit statement that explicitly permits the tunnel type (protocol) and the source and destination address.

4.9.4 Tunnel Endpoints PPSM Compliance

Allowing unknown traffic into the enclave creates high risk and potential compromise by an intruder. Protocols used by applications the PPSM has reviewed and determined to require additional mitigation is necessary to protect the GIG. After determining the final de-encapsulation endpoints, ensure the tunnel implements protocol inspection, filtering and mitigation as defined in the PPS VA reports.

4.10 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.

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.

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.

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 i in the administrator staff is aware of the alert as soon as possible.

The firewall shall immediately display an alert message, identifying the potential security violation and make accessible the audit record contents associated with the event(s) that generated the alert. The message is displayed at the 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 alert may or may not be part of the message displayed; however, the relevant audit information must be available to administrators.

The firewall will display the alert message identifying the potential security violation and make accessible the audit record contents associated with the event(s) until it has been acknowledged. The intent is to ensure 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).

Acknowledging the message could be a single event or different events. In addition, assurance is required that each administrator that received the message also receives the acknowledgement message, which includes some form of reference to the alert, 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 alert.

5. IPSEC VPN

IPSec VPNs enable an efficient and cost-effective method for secure communications across a shared IP infrastructure (i.e., NIPRNet) to provide intranet or WAN connectivity between multiple sites of an enclave; thereby replacing traditional WAN services, such as ATM and frame relay. It also can provide secured remote access services to the telecommuting and mobile workforce. IPSec provides data confidentiality by encrypting packets before transmission. It helps ensure the integrity of the data by verifying the packets have not been altered while in transient. Authenticity of the data is provided by validating the source of the received packets.

IPSec VPN tunnel is created between two VPN gateways or a single gateway and a software client residing on a laptop device. An IPSec VPN gateway can be a router, multi-layer switch, firewall, or a VPN appliance. The gateway also can take on any one of the following roles: peer, server, or client. A peer would be deployed at both ends of the tunnel with neither device having any controlling influence over the other. With the client-server model, the server will push policy to the client. The server will almost always be deployed at the central site or headquarters while the client is either a hardware client (low end firewall or appliance) deployed at a remote site or it is a software client implemented on a mobile worker's laptop.

5.1 Security Association

Before a tunnel between the two end-points can be established, an agreement must be made as to how the tunnel will be secured. The agreement is referred to as a Security Association (SA). An IPSec SA is established using either Internet Key Exchange (IKE) or via manual configuration. When using IKE, the security associations are established when needed and expire after a period of time has lapsed or a volume of traffic threshold has been reached. If manually configured, they are established as soon as the configuration is complete at both end points and they do not expire.

The SA and its corresponding key will expire after the number of seconds has exceeded the configured limit. A new SA is negotiated before the lifetime threshold of the existing SA is reached to ensure a new SA is ready for use when the old one expires. The longer the lifetime of the IKE SA the longer the lifetime of the key used for the IKE session, which is the control plane for establishing IPSec Security Associations. The SA is less secure with a longer lifetime because an attacker has a greater opportunity to collect traffic encrypted by the same key and subject it to cryptanalysis. However, a shorter IKE lifetime causes IPSec peers to have to renegotiate IKE more often resulting in the expenditure of additional resources. Nevertheless, it is imperative the IKE SA does have a finite lifetime.

When using IKE, the Security Parameter Index (SPI) for each SA is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each SA. IKE peers will negotiate the encryption algorithm and authentication or hashing methods, as well as generate the encryption keys. With manual configuration of the IPSec SA, both the cipher key and authentication key are static. Hence, if the keys are compromised, the traffic being protected by the current IPSec tunnel can be decrypted, as well as traffic in any future tunnels established by this SA. If this IPSec

tunnel is compromised, it will remain compromised allowing an attacker to exploit the tunnel at will.

5.2 Authentication

Both IPSec endpoints must authenticate each other to ensure the identity of each by additional means besides an IP address which can easily be spoofed. The objective of IPSec is to establish a secured tunnel with privacy between the two endpoints traversing an IP backbone network. In the case of teleworkers accessing the enclave using a laptop configured with an IPSec software client, the secured path will also traverse the Internet. The secured path will grant the remote site or client access to resources within the private network; thereby, establishing a level of trust. Hence, it is imperative that some form of authentication is used prior to establishing an IPSec session for transporting data to and from the enclave from a remote site.

5.2.1 Shared Secrets

Using shared secrets between two IPSec endpoints is easy to implement but is also easy to compromise. Regardless of the strength of the password, they can be cracked using software tools that are readily available. Furthermore, implementation using shared secrets is not scalable since all VPN gateways and software clients would need to be configured with the shared secrets. In addition, there cannot be a preshared key for every user because the VPN gateway server does not know the client's identity (the IP address is commonly used). Hence, remote users must use a group-based preshared key for authentication. When an individual leaves the group, changing the key must be coordinated with the other users of the group. PKI mitigates the risk involved with group passwords because each user has a certificate.

5.2.2 Certificates

PKI offers a scalable way to authenticate all IPSec endpoints in a secure manner. Every VPN gateway or remote client that needs to participate in IPSec VPN is issued a digital certificate by the Certification Authority (CA). The digital certificate binds the identity information of a VPN gateway (e.g., hostname or IP address) to the device's public key by means of digital signature. This involves the use of public key cryptography algorithms, such as RSA. Based on this binding, any device that trusts the CA certificate, i.e., trusts the signature of the CA, would accept the identity inside the signed certificate. This model enables all VPN gateways and clients that trust the same CA to authenticate each other.

Certificates are issued and signed by a CA. Hence, the signature on a certificate identifies the particular CA that issued a certificate. The CA in turn has a certificate that binds its identity to its public key, so the CA's identity can be verified. The primary role of the CA is to digitally sign and publish the public key bound to a given user or device via a digital certificate. This is done using the CA's own private key, so trust in the user's key relies on trust in the validity of the CA's key. Hence, to establish trust in the certificate of the remote client or peer, the VPN gateway must be configured to validate the peer's certificate with the DoD-approved CA, as well as validate the identity of the DoD-approved CA. If the peer's certificate is not validated, there is

a risk of establishing an IPSec Security Association with a malicious user or a remote client that is not authorized.

Situations may arise in which the certificate issued by a CA may need to be revoked before the lifetime of the certificate expires. For example, the certificate is known to have been compromised. To achieve this, a list of certificates that have been revoked, known as a Certificate Revocation List (CRL), is sent periodically from the CA to the IPSec gateway. When an incoming IKE session is initiated for a remote client or peer whose certificate is revoked, the CRL will be checked to see if the certificate is valid; if the certificate is revoked, IKE will fail and an IPSec security association will not be established for the remote end-point.

5.3 Internet Key Exchange

IKE Phase I establishes the IKE SA using either Main or Aggressive Mode. Both Main Mode and Aggressive Mode accomplish a Phase 1 exchange. Each generates authenticated keying material from a Diffie-Hellman (DH) exchange. Diffie-Hellman is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. IKE uses DH to create keys used to encrypt both the IKE and IPSec communication channels. The process works by two peers both generating a private and a public key and then exchanging their public keys with each other. The peers produce the same shared secret by using each other's public key and their own private key using the DH algorithm. The DH group is configured as part of the IKE Phase 1 key exchange settings. DH public key cryptography is used by all major VPN gateways, supporting DH groups 1, 2, and 5. DH group 1 consists of a 768 bit modulus, group 2 consists of 1024 bit modulus, and group 5 uses a 1536 bit modulus. The security of the DH key exchange is based on the difficulty of solving the discrete logarithm in which the key was derived from. Hence, the larger the modulus, the more secure the generated key is considered to be.

When using Main mode, IKE performs three bidirectional exchanges between peers with six messages. The first exchange (message one and two) during Main Mode between nodes establishes the security policy—that is, the initiator proposes the encryption and authentication algorithms it is willing to use. Diffie-Hellman is then used to generate and exchange (message four and five) a shared secret for encrypting and authenticating the remainder of the IKE Phase I and Phase II.

If pre-shared keys are used for authenticating peers, each IPSec endpoint must find the pre-shared key for its peer by using the source IP address from which it is receiving the IKE packets. If certificate-based authentication is being used, the endpoint will use its private key. The peers will then exchange their identification in messages five and six. Each will send its identification (IP address or hostname) along with a hash of the accepted SA proposal using their key. After the IPSec endpoints have authenticated each other, IKE Phase 2 (Quick Mode) will begin to negotiate the IPSec SA.

Aggressive mode is completed using only three messages instead of the six used in main mode. Essentially, all the information needed to generate the DH secret is exchanged in the first two messages exchanged between the two peers. The identity of the peer is also exchanged in the

first two packets which have been sent in the clear. There are risks to configurations that use pre-shared keys which are exaggerated when Aggressive Mode is used. The entire session may be intercepted and manipulated. An adversary can either use a pre-shared key to impersonate a trusted end-point or client and connect to the protected network, or it can mount a Man-in-the-Middle attack on any new session.

The IKE Phase-2 (Quick Mode) SA is used to create an IPSec session key. Hence, its rekey or key regeneration procedure is very important. The Phase-2 rekey can be performed with or without Perfect Forward Secrecy (PFS). With PFS, every time a new IPSec SA is negotiated during the Quick Mode, a new DH exchange occurs. The new DH shared secret will be included with original keying material (SYKEID_d, initiator nonce, and responder nonce from Phase 1) for generating a new IPSec session key. If PFS is not used, the IPSec session key will always be completely dependent on the original keying material from the Phase-1. Hence, if an older key is compromised at any time, it is possible that all new keys may be compromised. The DH exchange is performed in the same manner as was done in Phase 1 (Main or Aggressive Mode). However, the Phase-2 exchange is protected by encrypting the Phase-2 packets with the key derived from the Phase-1 negotiation. Because DH negotiations during Phase-2 are encrypted, the new IPSec session key has an added element of secrecy.

5.4 Encrypted Tunnel

Encapsulating Security Payload (ESP) is the feature in the IPSec architecture providing confidentiality, data origin authentication, integrity, and anti-replay services. ESP can be deployed in either transport or tunnel mode. Transport mode is used to create a secured session between two hosts. It can also be used when two hosts simply want to authenticate each IP packet with IPSec authentication header (AH). With ESP transport mode, only the payload (transport layer) is encrypted; whereas with tunnel mode, the entire IP packet is encrypted and encapsulated with a new IP header. Tunnel mode is used to encrypt traffic between secure IPSec gateways, or between an IPSec gateway and an end-station running IPSec software. Hence, it is the only secured method to provide secured path to transport traffic between remote sites or end-stations and the central site.

Data Encryption Standard (DES) encrypts data in 64 bit block size and uses effectively a 56 bit key. A 56 bit key space amounts to approximately 72 quadrillion possibilities. Relative to today's computing power it is not sufficient and is vulnerable to brute force attack. Therefore, DES is no longer appropriate for security services. Triple DES (3DES) is simply a construction of applying DES three times in sequence. 3DES with three different keys (K1, K2 and K3) has effective key length is 168 bits. However, the implementer could chose to use the same key two times or even all three times; thereby having an effective key length of 112 and 56 respectively. Based on certain vulnerabilities when reapplying the same encryption three times, using 168 bits has a reduced security equivalent to 112 bits and using 112 bits has a reduced security equivalent to 80 bits.

While there is much debate about the security and performance of Advance Encryption Standard (AES), there is a consensus that it is significantly more secure than 3DES, and in many environments faster. AES is available in three key sizes: 128, 192, and 256 bits, versus the 56 bit

DES. Therefore, there are approximately 1021 times more AES 128-bit keys than DES 56-bit keys. In addition, AES uses a block size of 128 bits—twice the size of DES or 3DES. To ensure the privacy of the IKE session responsible for establishing the security association and key exchange for an IPSec tunnel, it is imperative that AES is used for encryption operations.

5.5 VPN Gateway Deployment

Packets from a remote client destined outbound must be inspected and proxied the same as any other traffic that will egress the enclave. Otherwise, there is the risk the return traffic will ingress the IPSec tunnel could compromise the remote client and possibly the remote LAN. This scenario can exist with a VPN-on-a-stick implementation that allows traffic to U-turn—that is, traffic from the remote site that traverses the IPSec tunnel is immediately forwarded out the same interface towards the NIPRNet and Internet with no upstream firewall. If a remote LAN is breached, the entire enclave could be exposed via the secured tunnel or any other provisioned link between the compromised remote LAN and other remote sites and the central site. Hence, it is imperative that traffic from the remote site that is destined outbound does not bypass the applicable inspection and proxy services deployed for the enclave's perimeter defense.

Deploying the VPN gateway within a DMZ or service network will eliminate any risks associated with U-turn traffic. The traffic exiting the IPSec tunnel leaving the DMZ destined to either the private network or the NIPRNet/Internet will have to pass through the DMZ firewall and therefore be subject to the applicable policy. If the VPN gateway is a firewall, which could be either on or outside the DMZ, review the configuration and verify it is not allowing traffic received from the IPSec tunnel to U-turn back out towards the NIPRNet/Internet. To allow traffic to U-turn, the firewall would have to be configured to NAT for the pool of remote client addresses on the outside interface (PAT the same global address), as well as a configuration statement to allow traffic to egress out same interface in which the IPSec tunnel terminates—most implementations do not allow this by default. If the firewall is configured to allow a U-turn, then there must be another firewall upstream to inspect this outbound traffic or the traffic must be forwarded (policy based routed) towards the firewall or applicable proxy to perform the stateful inspection.

A VPN gateway peer at the remote site provides connectivity to the central or other remote sites belonging to the enclave via an IPSec tunnel across an IP backbone network, such as the NIPRNet. This creates an extension or Intranet for the Enclave using IPSec tunnels in lieu of traditional or legacy WAN services (T carrier, ATM, frame relay, etc.). Unless the remote site has the required enclave perimeter defense (firewall, IPS, deny by default, etc.), it is imperative that all inbound and outbound traffic traverse only the IPSec tunnels or other provisioned WAN links connecting the remote site to other sites belonging to the enclave. In other words, no packets can leak out an external-facing interface as "native" IP traffic into an IP backbone (i.e., NIPRNet, Internet). In addition, the external interface must not receive any traffic that is not secured by an IPSec tunnel or other provisioned WAN links connected to the central or remote site. This not only ensures that inbound and outbound traffic does not bypass the enclave's perimeter defense, but also eliminates any backdoor connection.

6. WIRELESS INFRASTRUCTRE

6.1 Wireless Infrastructure Policy – Applicable To All Wireless Infrastructure Devices

Wireless policy requirements are applicable to all wireless infrastructure systems used in the DoD to connect to DoD networks or are used to store, process, receive, or transmit DoD data. Review Wireless Policy checks for all wireless devices (classified or unclassified) that are used to process, transmit, store, or connect to DoD information or enclave resources. These checks should be reviewed before other wireless equipment specific checks are reviewed.

6.2 WLAN Compliance Requirements

This section applies to DoD WLAN systems (Institute of Electrical & Electronics Engineers, Inc. [IEEE] 802.11) that are owned and/or operated by DoD components and does not apply to the use of commercial, public, or home WLAN systems used for remote connections to DoD networks, which are covered in Section 6.4 of this STIG.

WLANs are generally used as an extension to an existing wired infrastructure. The IEEE 802.11 standard defines the interoperability requirements for WLANs operating in the 2.4 and 5 GigaHertz (GHz) unlicensed bands.

6.2.1 WLAN Network Devices (WLAN Access Points, Controllers, Authentication Servers, & WIDS)

Two types of WLAN Access Points (AP) may be used in a DoD network: Enclave-NIPRNet Connected and Internet Gateway Only Connection. The Enclave-NIPRNet Connected WLAN AP provides a wireless connection to the DoD network for authorized WLAN client devices. The Internet Gateway Only Connection WLAN AP provides a wireless connection only to the Internet for wireless client devices like the iPad, which do not support CAC authentication.

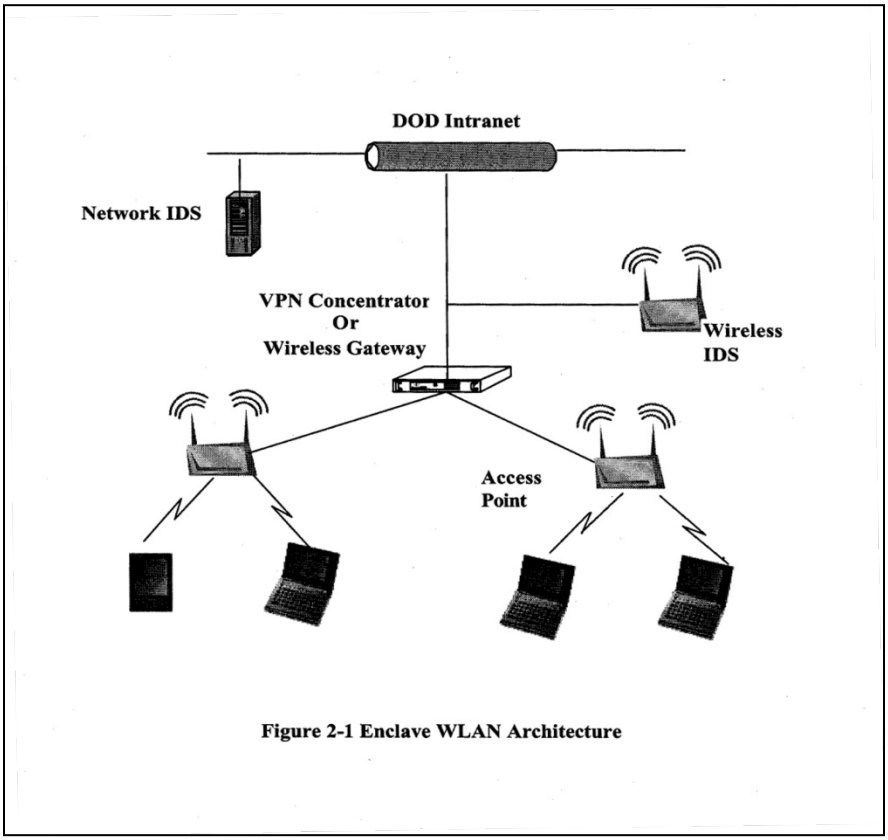
Most enterprise WLAN systems (as opposed to consumer WLAN systems) consist of the following network components:

- WLAN Access Point
- WLAN Controller
- WLAN Authentication Server
- WLAN IDS Sensor (feature may be included in the access point)
- WLAN IDS Server

When creating a WLAN network asset in VMS, select the Computing asset, and then the appropriate asset posture based on the type of WLAN network component being registered. When registering either a “WLAN Access Point” or “WLAN Controller” asset, also add the “Network Appliance” asset posture. When registering a “WLAN Access Point” one of two roles must be selected: “Enclave-NIPRNet Connected” or “Internet Gateway Only Connection”.

Figure 6-1 shows a representative example of a compliant DoD WLAN architecture. The WLAN APs shown in the diagram are examples of Enclave-NIPRNet Connected APs.

Figure 6-1: DoD Intranet



6.2.2 WLAN Network Devices (WLAN Bridges)

A WLAN Bridge is an access point that has been configured to connect to another access point, typically to provide communications between two buildings or sites. A WLAN Bridge is usually configured to not accept connections from WLAN clients.

DoD WLAN Bridge security controls apply to all DoD operated WLAN bridges that provide point-to-point communications between two DoD sites, buildings, or networks. To register a WLAN bridge in VMS, select the Computing asset, and then the WLAN Bridge asset posture. Also, add the "Network Appliance" asset posture.

6.2.3 Classified WLANs

Legacy classified WLAN devices include the Harris Corporation's SecNet 11 and SecNet 54 and the L3 Communications KOV-26 Talon (version 1.1.04 and later). The SecNet 11 is approved to

transmit classified information up to Secret and the SecNet 54 and Talon are approved to transmit classified information up to Top Secret.

The SecNet 11 is an IEEE 802.11b device that operates in the 2.4 GHz frequency band while the SecNet 54 and Talon are IEEE 802.11 b/g devices that operate in the 5 GHz band. The Harris SecNet 11 device uses a proprietary implementation of the IEEE 802.11 standard; therefore, the system may not be discoverable by most wireless intrusion detection systems (WIDS).

National Security Agency (NSA) distributes both classified and unclassified operational keys for the SecNet 11/54 and Talon; therefore, SecNet 11/54 and Talon are available for unclassified WLANs that process sensitive information. Communications Security (COMSEC) accounts are required for organizations that plan to use the SecNet 11/54 and Talon. The three approved WLAN architectures for classified WLAN systems are shown in Figures 6-2, 6-3, and 6-4.

Figure 6-2: LAN Extension

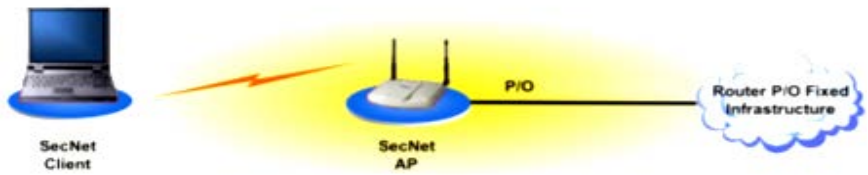


Figure 6-3: Wireless Bridging

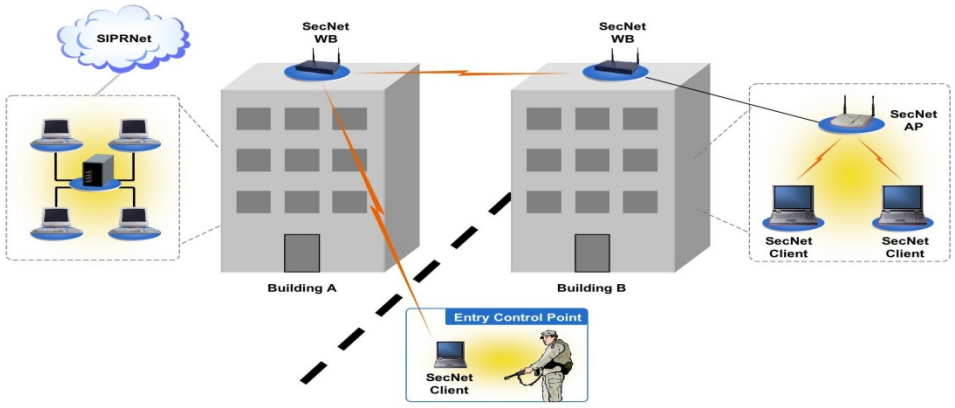
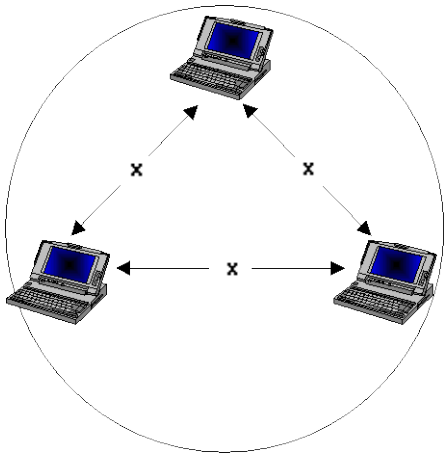


Figure 6-4: Wireless Peer-to-Peer



DoD Classified WLAN security controls apply to WLANs used for processing classified information and/or connecting to the Secret Internet Protocol Router Network (SIPRNet). For Classified WLAN workstations, register the workstation in VMS, and then add the "Harris SecNet 11" or "Harris SecNet 54" or "L3 KOV-26 Talon" asset posture. For the SecNet access point, register the "Harris SecNet 11" or "Harris SecNet 54" asset posture.

NSA recently released a classified WLAN capability package based on the new NSA Commercial Solutions for Classified (CSfC) program. The CSfC program provides the capability for vendors to develop commercial products that can be used to process classified information and then have those products approved by NSA. The technical requirements for a CSfC WLAN system are reviewed using the Campus IEEE 802.11 WLAN Capability Package, which is outside the scope of this STIG. The CSfC WLAN STIG, included with the Wireless STIG, will be used to verify the CSfC based WLAN system has been approved by NSA and the SIPRNet connection approval office, a security review has been completed on the system, required training has been completed, and required procedures are being followed. Appendix A provides procedures for registering a CSfC WLAN system asset in VMS.

6.3 Wireless Metropolitan Area Network (WMAN) Compliance Requirements

DoD WMAN security controls apply to WMAN systems (IEEE 802.16-2004 [formally 802.16d] and 802.16e-2005 [formally 802.16e]) that are owned and/or operated by DoD components and do not apply to the use of commercial WMAN systems for remote connections to DoD networks, which is covered in Section 2.7 of this STIG. The IEEE 802.16-2004 and 802.16e-2005 standards are sometimes referred to as fixed Worldwide Interoperability for Microwave Access (WiMAX) and mobile WiMAX, respectively. WMAN is a telecommunications technology that provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint links (bridge) to portable and fully mobile WMAN subscriber (client) access to Internet services.

WMAN systems are designed for medium range "last mile" connections and are primarily used with the DoD as wireless bridges to connect two sites or buildings. Recently, wireless carriers

have deployed WMAN systems to provide wireless digital broadband services as an alternative to cable, fiber-optic, and cellular Third Generation (3G) systems.

The following WMAN assets should be registered in VMS:

- WMAN Access Points – applies to all DoD operated WMAN network devices that provide access to a DoD network by WMAN subscriber (client device).
- WMAN Bridges – provides point-to-point communications between two DoD sites, buildings, or networks.
- WMAN Subscribers – client devices (such as, PDAs, laptops, etc.) that are used to connect to DoD-owned WMAN networks. Requirements for WMAN subscribers that are used for remote access to DoD networks via public WMAN access points are covered in Section 6.4.

6.4 Compliance Requirements for Wireless Remote Access Connections to DoD Networks

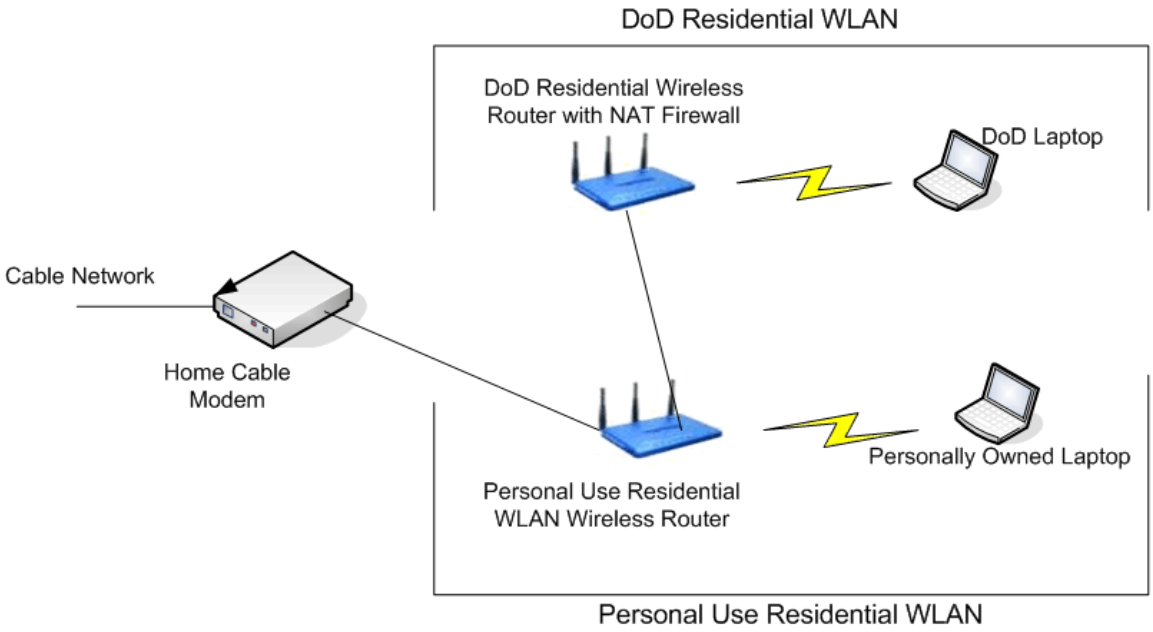
This section applies to any wireless client (e.g., laptop) that remotely connects to a DoD network via a broadband Internet connection provided by a hotel, home, restaurant, airport, or other public wireless access point. The most common wireless technologies used for remote access are WLAN and 3G/4G cellular telephony. The requirements described below are found in the Secure Remote Computing: Remote Access Policy STIG.

Cellular wireless broadband remote access connections are generally considered more secure than public WLAN connections and should be preferred by DoD sites for wireless remote access to DoD networks. WLAN connections from public access points in airports, restaurants, hotels, and other public areas pose significant risks to DoD Information Technology (IT) systems for the following reasons:

- It is very difficult for DoD wireless device users to know if they are connecting to a legitimate wireless access point or a hacker-controlled access point or wireless client acting as an access point.
- After connecting to a hacker-controlled access point, the hacker can download malware on a wireless client before a user or automated tool can block the download.
- A recent study reported over 50% of wireless devices identified during a wireless scan at several U.S. airports to be illegitimate (not part of the airport sanctioned wireless network).
- Connections to cellular femto and pico cells have the same risks as WLAN public hotspots.

Figure 6-5 provides an example of a compliant residential WLAN system used for remote access to DoD networks by a GFMD (i.e., wireless DoD laptop or PDA).

Figure 6-5: Compliant DoD Residential WLAN Architecture



NOTE: It is recommended for each site that allows telework via home wireless systems furnish DoD users with managed DoD residential WLAN equipment. This would allow them to configure, furnish, and monitor the configuration of the DoD residential WLAN equipment.