WIRELESS LAN SECURITY FRAMEWORK ADDENDUM to the WIRELESS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 1

31 October 2005

Developed by DISA for DOD

UNCLASSIFIED

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1 BACKGROUND

Experience has shown that as new technologies emerge and gain popularity, they become a source of new vulnerabilities for which security solutions must be developed. Wireless technologies and devices are a case in point. As these are increasingly used for personal, business, and government communication, it is clear that, unless properly implemented and secured, they can pose significant risks to national security and to non-wireless networking infrastructures.

Among these wireless technologies, wireless local area networking (WLAN or "wireless fidelity" [WiFi]) present both great opportunities and security concerns. To assist in the secure deployment and operation of 802.11 WLAN technologies, the Defense Information Systems Agency (DISA) has created a Wireless Local Area Network (LAN) Security Framework, which is presented in this document. This guidance provides a common conceptual framework to help the Department of Defense (DOD) coordinate acquisition, development, architecture design, and implementation of 802.11 wireless infrastructures connected to the Unclassified But Sensitive Internet Protocol Router Network (NIPRNet).

The framework presented in this document is geared toward developers, system architects, system administrators, and system users and is intended to guide secure design, development, and implementation of WLAN security technologies that comply with relevant DOD policy. This document defines WLAN components needed for a secure WLAN solution and discusses proper implementation.

This document provides a conceptual framework for implementing WLANs securely. To this end, the document provides details concerning WLAN technologies and solutions that enable a secure connection to the NIPRNet. Although the document's content is technical, its presentation is intended to provide readers of varying levels of expertise with sufficient background to understand the topics discussed. In short, this document does not assume that readers have operating system (OS), networking, and security expertise. The intended audience includes the following:

- Government managers (such as chief information officers or senior managers) who are planning to employ a WLAN in their agency
- Systems engineers and architects who are designing and implementing a WLAN for an unclassified environment
- System administrators who are administering, securing, or upgrading a WLAN connected to the NIPRNet

- Security consultants who are performing assessments to determine the security postures of unclassified wireless environments
- Wireless users who are interested in understanding the security risks surrounding WLANs and the mechanisms used to mitigate those risks.

Although this document is intended to provide a good overview of current DOD WLAN security issues, because of the constantly changing nature of the wireless security industry and the threats to and vulnerabilities of these technologies, readers are strongly encouraged to take advantage of other resources for more current and detailed information.

1.2 AUTHORITY

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

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

1.3 SCOPE

This Addendum is designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls for mobile and wireless devices connected to DOD networks.

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) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@disa.mil**.

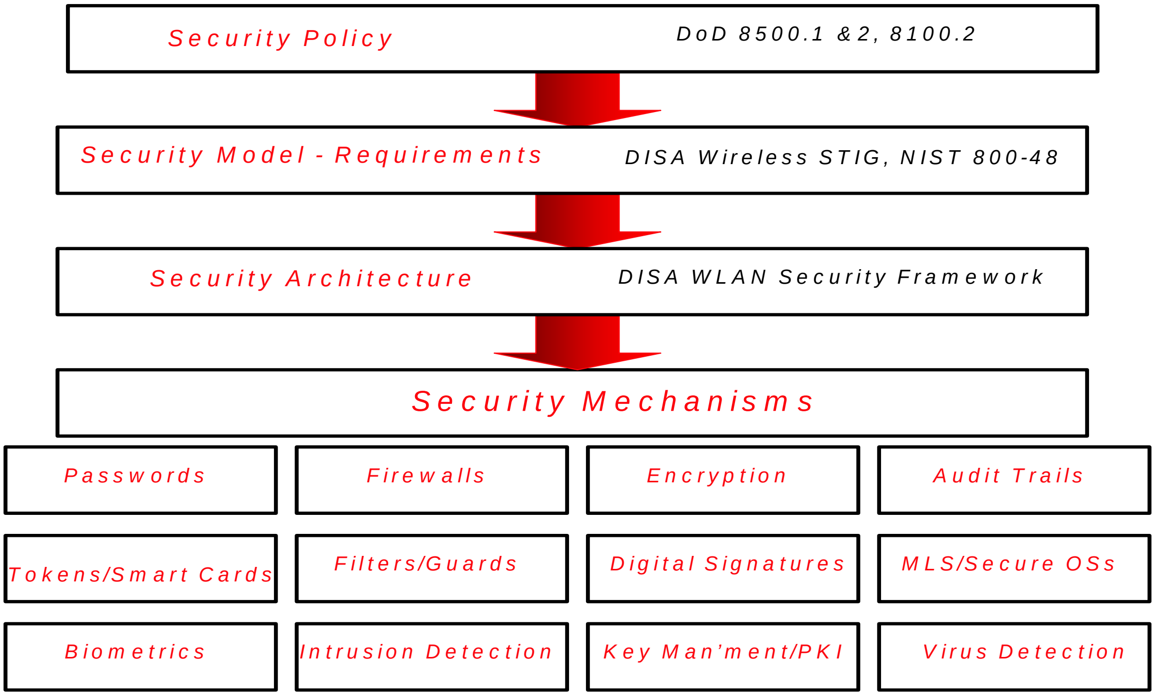
1.5 Document Revisions

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

1.6 Approach

This document follows a standard security engineering approach, in which high-level requirements are dictated by security policy. These requirements are then translated into a conceptual architecture. Once the architecture is defined, specific security mechanisms can be selected. Figure 1-1 depicts this approach and the specific application to the WLAN Security Framework.

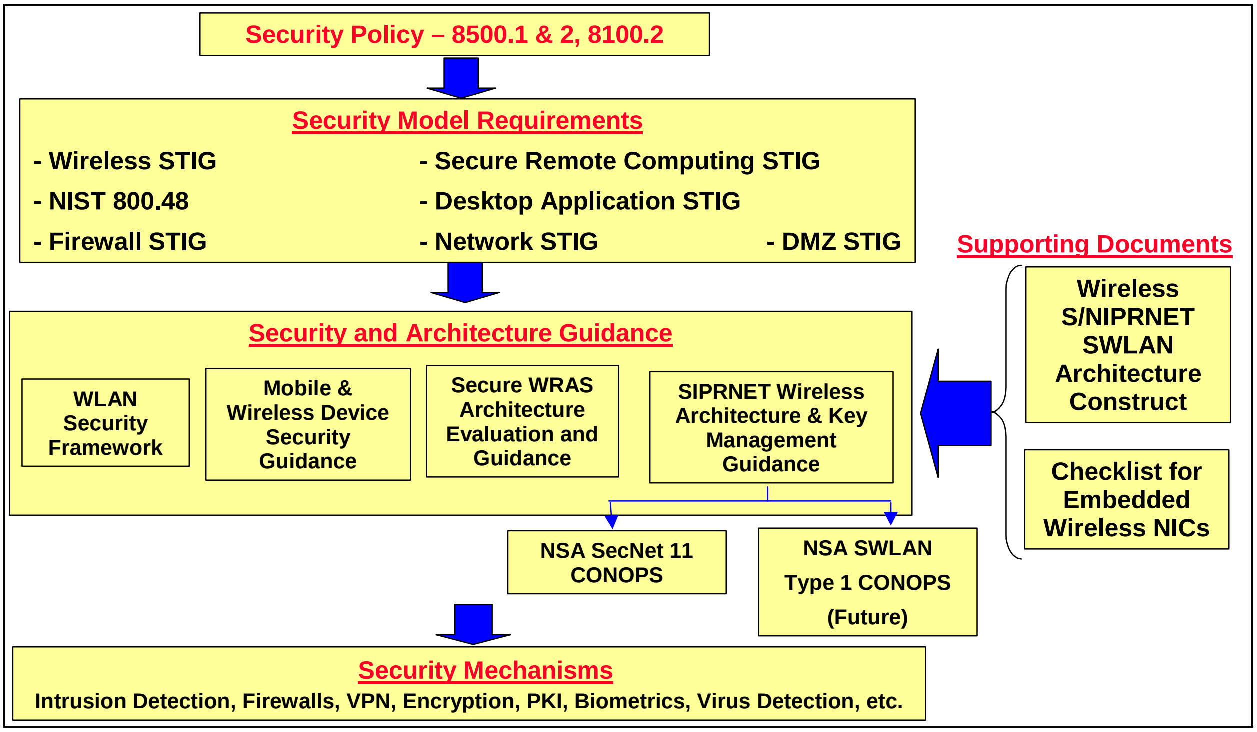
Figure 1-1. Security Engineering Approach to WLAN Security Framework



The policies on which this framework is based include DOD Directive (DODD) 8500.1, DOD Instruction (DODI) 8500.2, and DOD Wireless Security Policy 8100.2. The DISA *Wireless Security Technical Implementation Guide (STIG)* and National Institute of Standards and Technology (NIST) Special Publication 800-48, *Wireless Security of 802.11, Bluetooth, and Handheld Devices,* are used as references to provide specific requirements for defining a secure WLAN architecture. This architecture makes up the WLAN

Security Framework. Figure 1-2 provides an overview of the relationships among the documents relied on in this approach.

Figure 1-2. Security Engineering Approach—Document Relationship Diagram


Security Policy – 8500.1 & 2, 8100.2
Security Model Requirements
- Wireless STIG
- Secure Remote Computing STIG
- NIST 800.48
- Desktop Application STIG
- Firewall STIG
- Network STIG
- DMZ STIG
Supporting Documents
Wireless S/NIPRNET SWLAN Architecture Construct
Checklist for Embedded Wireless NICs
Security and Architecture Guidance
WLAN Security Framework
Mobile & Wireless Device Security Guidance
Secure WRAS Architecture Evaluation and Guidance
SIPRNET Wireless Architecture & Key Management Guidance
NSA SecNet 11 CONOPS
NSA SWLAN Type 1 CONOPS (Future)
Security Mechanisms
Intrusion Detection, Firewalls, VPN, Encryption, PKI, Biometrics, Virus Detection, etc.

The WLAN framework also discusses the functionality of the WLAN security components. DOD entities should be able to use this framework to select the solution that best fits the requirements of their environment and to successfully implement a secure network.

It is expected that DISA and DOD will provide detailed guidance for the configuration of the specific WLAN security products in future STIGs and guidance documentation.

1.7 Document Structure and Use

This document is divided into 10 sections and 2 appendices. The following tables provide an overview of the document and assist in its use. Table 1-1 provides a general synopsis of each section's content.

Table 1-2 guides readers in the use and specific benefits of the various sections of the document.

Table 1-1. Document Roadmap

Section	Title	Description
Section 1	Introduction	Includes the purpose and scope of the Wireless LAN Security Framework.
Section 2	Background	Provides additional background information and a short discussion of threats and vulnerabilities.
Section 3	Policy & Guidance	Highlights the relevant policies and guidance available for reference in implementing a wireless infrastructure.
Section 4	WLAN Security Framework	Discusses the WLAN framework and the four ways in which it can be implemented.
Section 5	Implementation Considerations	Discusses items that must be considered before WLAN design and implementation. Some of these include certification and accreditation (C&A), Common Criteria, scalability and interoperability, and proprietary versus standards-based solutions.
Section 6	Administrative Controls	Focuses on some key administrative controls that must be implemented to adequately secure WLANs.
Section 7	Technical Mechanisms	Discusses some key technical mechanisms that are included in the reference model and that must be considered during design, testing, and implementation of a WLAN.
Section 8	Mobile Device Security	Discusses security steps and features that are critical to the secure use of mobile devices.
Section 9	Future Considerations (802.11i)	Notes a key future consideration in securing DOD wireless networks.
Section 10	Case Studies	Presents case studies describing how wireless LANs are currently being securely deployed in DOD. Each case study relates to one of the four methods of implementing the WLAN framework (presented in Section 4).
Appendix A	Checklists	Provides checklists to help guide procurement and implementation of WLANs.
Appendix B	Acronyms	Provides a list of the acronyms used in the document.

Table 1-2. Document Use

Section	Use	Focus
Section 1 and 2	Read these sections to understand the scope and purpose of the document and to learn about some of the threats and vulnerabilities addressed by this document.	Overview and Background Information
Section 3	Read this section to gain an overview of the policies used in developing the framework.	Policy
Section 4	Read this section to understand the general architecture and components used in the WLAN Security Framework.	Conceptual Architecture
Sections 5 Through 9	Read these sections to gain an understanding of some key implementation considerations, key technical mechanisms, key administrative controls, mobile device security, and future considerations.	Security Mechanisms

Section	Use	Focus
Section 10	Read this section for an overview of some existing WLAN implementations in DOD.	Existing WLAN Implementation
Appendix A	Use the checklists in this appendix as tools in the design and engineering of a WLAN. • The C&A checklist presents the steps that must be taken in the design and implementation of a WLAN to provide a secure system that is approved for use. • Product selection checklists include key components that each security product used in a WLAN must support. • The WLAN Security Checklist, from NIST Special Publication 800-48, provides detailed management, technical, and operational recommendations that should be addressed in any WLAN design and implementation.	Checklists to Facilitate Product Selection and Implementation
Appendix B	Use this appendix as a reference for acronyms used in this document.	Acronyms

2. BACKGROUND

As WLAN technologies have proliferated, significant security-related concerns have emerged about their implementation because of the flawed initial design of the security components of the 802.11 protocol. Despite these concerns, the benefits of WLANs have driven the adoption of this technology in commercial and government arenas.

To effectively implement WLANs in DOD, a WLAN architecture must be designed to address relevant threats and vulnerabilities. With WLANs, as with any wireless communication, attacks based on passive collection and traffic analysis cannot be fully mitigated. This type of attack, however, will not result in data compromise or provide an attacker with access to the network. All attacks that could result in the compromise of data or in unauthorized access *can* be mitigated. Table 2-1 lists common attacks associated with WLANs. This table provides only a high-level view of the attacks and mitigation measures. In general, this framework prescribes use of strong encryption, strong mutual authentication, and other controls that work together to provide layered security.

Table 2-1. Common Attacks on Wireless Networks

Attacks	Comment
Traffic Analysis	Only wireless client and access control device addresses (Media Access Control [MAC] or Internet Protocol [IP]) are visible to an adversary; all other traffic is encrypted.
Passive Eavesdropping	Strong encryption will prevent eavesdroppers from collecting any usable data.
Partial or Known Plaintext Attack (e.g., Wired Equivalent Protocol [WEP] attack)	This is not a concern because in this framework WEP is not used to provide encryption.
Unauthorized Access	This attack is mitigated by strong authentication and Federal Information Processing Standard (FIPS) 140-2 encryption.
Man in the Middle	This type of attack is mitigated by mutual authentication and strong encryption. A successful man-in-the-middle attack is defined by the capture of encrypted data and successful decryption of the data.
ARP Attacks	This attack is mitigated through strong mutual authentication and FIPS-validated encryption.
Replay Attacks	This is mitigated by strong authentication and encryption. In addition, protocols such as Secure Internet Protocol (IPSec), Temporal Key Integrity Protocol (TKIP), and Counter-Mode Cipher Block Chaining (CBC) MAC Protocol (CCMP) have a counter for replay protection built into packets.
Session Hijacking	This is mitigated by strong encryption and authentication mechanisms.
Redirection	Any plaintext IP addresses should be nonroutable.
Denial of Service	Incidence response is key to minimizing the impact of denial-of-service attacks.

3. POLICY & GUIDANCE

This section highlights the relevant policies and guidance available for reference in implementing a wireless infrastructure. These policies were considered in developing, and incorporated into, the WLAN Security Framework.

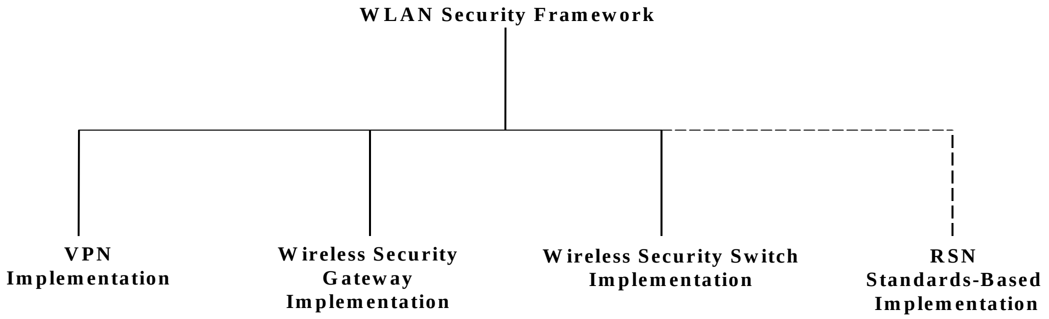
Policy	Description
Wireless STIG	The *Wireless STIG* was published as a tool to assist in the improvement of the security of DOD information systems. The guidance provided in this STIG is authoritative according to DODD 8500. https://iase.disa.mil/documentlib.html#wirelessguid
DODD 8100.2	This directive describes the appropriate use of commercial wireless devices, services, and technologies in the DOD Global Information Grid (GIG).
DODD 8500.1	This directive prescribes the use of information assurance (IA) in a defense-in-depth approach.
DODI 8500.2	This instruction implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of DOD information systems and networks under DODD 8500.1.
DODI 5200.40 (DITSCAP)	Use of the DOD Information Technology Security Certification and Accreditation Process (DITSCAP), available online at http://iase.disa.mil/ditscap/ditsdocuments.html, is required for any new information technology (IT) system. DITSCAP is used to implement policy, assign responsibilities, and prescribe procedures for C&A of IT, including automated information systems, networks, and sites, in DOD. The System Security Authorization Agreement (SSAA) is the key to DITSCAP. The SSAA is used to guide and document the results of the C&A and the implementation of IT security requirements. It resolves several issues, including the critical schedule for the C&A, the budget, security requirements, the functionality of the system, and performance issues.
Mobile Code Policy	This policy categorizes mobile code technologies and restricts their application within DOD on the basis of their potential to cause damage if used maliciously. http://iase.disa.mil/mcp/index.html

4. WLAN SECURITY FRAMEWORK

Effectively securing a WLAN begins with an architecture that incorporates all of the DOD policy-based administrative controls and technical mechanisms discussed in Sections 7 and 8. However, many practical factors, such as scalability and cost, also must be considered during the design process.

The WLAN Security Framework provides four reference implementations that should be used by network designers to ensure that the tenets outlined in Sections 7 and 8 are incorporated in the WLAN design. Further, the practical considerations involved in each implementation are discussed to assist in the decision-making process. This section presents a description of the generic architecture, then outlines the four reference implementations, which are shown below, in Figure 4-1.

Figure 4-1. Framework Taxonomy


WLAN Security Framework
VPN Implementation
Wireless Security Gateway Implementation
Wireless Security Switch Implementation
RSN Standards-Based Implementation

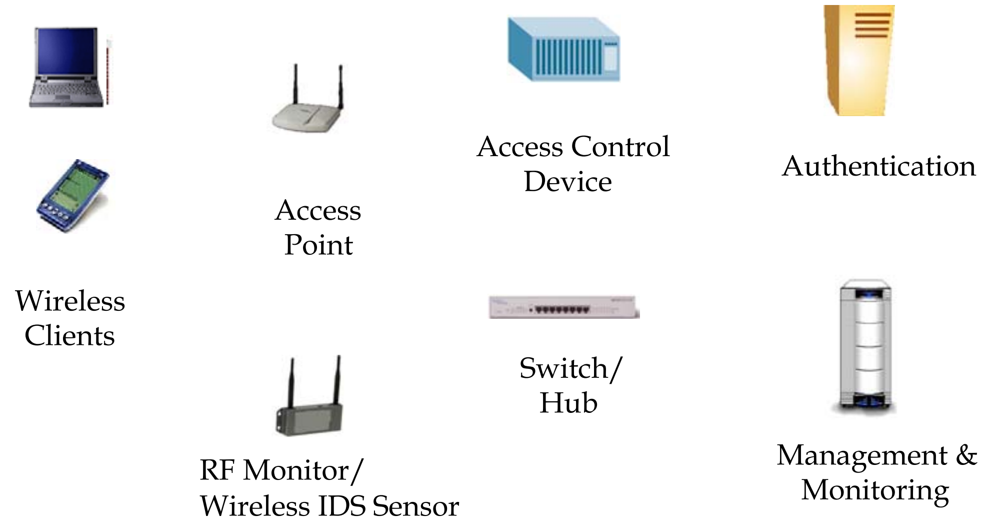
All of the implementations shown in Figure 4-1 have a similar component set and architecture. What distinguishes them from each other is the specific component (referred to as the access control device) that provides a number of essential security features to the architecture. As the figure shows, the access control devices that will be discussed include a virtual private network (VPN) device, a wireless security gateway, a wireless security switch, and a robust secure network (RSN) standards-based device.

The following subsections discuss first the generic architecture, then the four reference implementations (including their benefits and limitations).

4.1 WLAN SECURITY FRAMEWORK ARCHITECTURE

The WLAN framework is the basic architecture that can be used as a model for deploying wireless networks in DOD unclassified environments. A number of network components are needed to implement all of the mechanisms that are critical to securing a wireless network. Figure 4-2 shows the components required to implement the generic architecture. As noted previously, all of the components of this architecture except the access control device are common to all implementations of the WLAN framework.

Figure 4-2. Basic Components



4.1.1 Wireless Client

The wireless client provides the user interface for networked applications (e.g., Web browser, e-mail client), as well as a wireless communication capability, via a wireless network interface card (NIC).

The wireless client must be Common Criteria certified against any existing protection profiles (see Section 5.1). The wireless client will also need to be configured in compliance with all applicable STIGs. STIGs are available for a number of common operating systems and applications. Because wireless clients are available on different types of devices (e.g., notebook computer, personal digital assistant [PDA]), a determination will need to be made as to which STIGs apply to each type of client. In all cases, software installed on wireless clients should be routinely inventoried and assessed for STIG compliance.

The primary encryption mechanism on the wireless client will be software or hardware that provides file system and tunneling encryption capabilities. File system encryption will provide storage security, while tunneling encryption will secure the communication between the client and the network.

The wireless client must be configured with host-based countermeasures, such as a personal firewall, an intrusion detection system (IDS), and virus protection software. These countermeasures will allow the device and the user to detect imminent or active attacks against the wireless client.

For further protection, file and printer sharing functionality must be disabled. There are numerous known attacks that exploit these features, and wireless devices are particularly susceptible to these threats.

Table 4-1 presents a summary of the features and configurations of the wireless client.

Table 4-1. Wireless Client Features and Configuration

Wireless Client Features/Configuration	Required	Recommended
Ensure Common Criteria certification against any existing protection profiles.	✓	
Ensure compliance with applicable STIGs (e.g., OS, applications).	✓	
Use encryption client software (FIPS-140-2 certified) for storage and communication security.	✓	
Enable strong password protection scheme for device and network user login (as instructed in the *Secure Remote Computing STIG* developed by DISA for DOD). https://iase.disa.mil/techguid/stig/src-stig-v1r1-final-021403.doc	✓	
Ensure that two-factor authentication (smartcard) is used when Public Key Infrastructure (PKI)–based Common Access Card (CAC) authentication is required. http://iase.disa.mil/pki/pkim0812.pdf	✓	
Enable the use of biometric reader if available and/or required. https://iase.disa.mil/documentlib.html.		✓
Enable password protection on screen saver.	✓	
Verify that device is used in a physically secure location and is protected against unauthorized use.	✓	
Allow only one NIC to be active on a particular device at any given time.	✓	
Install and run DOD- and National Information Assurance Partnership (NIAP)–approved personal/host-based firewall. http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#firewalls	✓	
Lock out network access during periods of inactivity (when the computer is not in use).	✓	
Block access on high-risk ports as directed by *Network Infrastructure STIG*, Appendix G. https://iase.disa.mil/techguid/stig/network-stig-v5r2-9-29-03.doc	✓	

Wireless Client Features/Configuration	Required	Recommended
Enable firewall logging of suspicious activity and user alerts, including both inbound and outbound connection attempts.	✓	
Obtain configuration and signature file updates from network administrator on a regular basis, as required by Information Assurance Vulnerability Alerts (IAVA). https://iase.disa.mil/IAalerts/iavahnbk.pdf	✓	
Install and enable DOD-approved anti-virus software. http://www.cert.mil/antivirus/av_info.htm	✓	
Install and update latest virus definitions on a regular basis (weekly). Allow Live Updates to DOD servers.	✓	
Enable and run virus startup scan at each boot.	✓	
Verify that OS is STIG compliant. https://iase.disa.mil/techguid/stig/index.html	✓	
Install all of the latest OS security patches and fixes required by IAVAs.	✓	
Install all of the latest application/software security patches and fixes.	✓	
Ensure that media and file encryption is used for all classified information stored on and transmitted from the device.	✓	
Disable sharing of local files, printers, and drives.	✓	
Disable Internet connection sharing	✓	
Verify that FIPS-140-2 certified VPN client is installed and always used in conjunction with remote access service (RAS) connectivity.	✓	
Verify that active VPN connection icon is present for successful connection attempt. Note: The VPN icon may or may not be available, depending on implementation	✓	
Verify that split tunneling is disabled on the VPN client. (All Internet access would go through DOD firewall or proxy server instead of local service provider.)	✓	

4.1.2 Access Point

The AP provides the wireless client with access to the wired network. It consists of a radio interface (to communicate with wireless devices), a wired network interface (to communicate with wired devices), and bridging software (to pass information between the two interfaces).

Most commercially available APs include a number of features that must be securely configured. Normally, these features are managed by means of a Hypertext Transfer Protocol (HTTP) or a Simple Network Management Protocol (SNMP) interface that is password protected. This is convenient during initial setup, but these interfaces should be considered a security risk after that. Therefore, it is a recommended practice to disable all non–cryptographically protected management interfaces (e.g., HTTP) once the AP has been configured. If management access is required or desired on a regular basis, a secure cryptographically protected interface should be used (e.g., Secure Shell [SSH], Hypertext Transfer Protocol, Secure [HTTPS]).

The wireless AP must be Common Criteria certified against any existing protection profiles (see Section 5.1).

The AP should be FIPS 140-2 certified for encrypted communication with the wireless clients. As discussed in the preceding section, this encryption will not satisfy policy requirements but will add a layer of security.

Each AP will have a Service Set Identifier (SSID), a configurable name associated with an AP to identify the wireless network it supports. The SSID is broadcast in plaintext during beaconing and probing—both of which advertise the AP's presence to potential clients—as well as during communication with authorized devices. Therefore, it is easy for unauthorized users within communication range of the AP to capture the SSID. For this reason, the SSID should not be set to a name that provides information about the network the AP services (e.g., Company "A" Wireless Network); this information could provide an adversary with information that would facilitate an attack. Instead, the SSID should be a random string of characters, preferably compliant with DOD network password rules. As an additional measure, the SSID broadcast feature must be disabled.

To perform any attack on a wireless network, an adversary first needs to be within reception range of a wireless device. To minimize such opportunities, AP signal power should be kept as low as possible, with transmission power set to the lowest possible setting. Signal testing will be required to ensure that authorized users and devices can still communicate with the AP at a lower setting.

Finally, it is recommended that 802.11i-enabled APs (when available) be used in any implementation. The 802.11i standard was ratified in July 2004 and will eventually be supported in commercial wireless products. Standard 802.11i provides a major improvement in wireless security, with stronger encryption, authentication, and key management strategies. Table 4-2 provides a summary of AP features and configuration.

Table 4-2. Access Point Features and Configuration

Access Point Features/Configuration	Required	Recommended
Common Criteria certified against any existing protection profiles	✓	
128-bit WEP/WPA capability		✓
SSID beacon mode disabled		✓
Pseudo-random SSID, preferably compliant with DOD network password rules		✓
HTTP/SNMP management access disabled; ensure that only secure management access is available (e.g., SSH)		✓
Transmission power set to lowest possible setting that will meet required signal strength for the service area	✓	
802.11i security capability		✓

4.1.3 Wireless Access Point Management

Wireless AP management is highly recommended for operational and security purposes. Proper administration, configuration, and identification of authorized APs allow proper access control of a SWLAN and provide a mechanism for discovering and identifying unauthorized or improperly configured APs. Monitoring of the information provided by the APs is critical to detection of wireless rogue devices within the SWLAN. Controlling the number of device connections per AP can also optimize network performance and prevent bottlenecks. Load balancing features, such as signal channel tuning, provide a way of minimizing interference and bandwidth restrictions.

4.1.4 Radio Frequency Monitor

The radio frequency (RF) monitor provides a periodic snapshot of the wireless environment, helps identify rogue APs, and/or acts as a wireless IDS for the WLAN. It monitors the RF space (in this case, the 802.11 frequencies) and analyzes communication traffic for notable events in real time. RF monitoring must be performed in at least one of two possible manners: periodic scanning or continuous scanning. Continuous scanning is highly recommended for maximum effectiveness.

The RF monitor should be able to recognize known network attacks (e.g., denial of service, port scans, man in the middle) if a device that provides an IDS capability is used. To enable this recognition, a knowledge base of attack signatures must be stored on, or made accessible to, the RF monitor. Because of the dynamic nature of this information, it is also recommended that the knowledge base be easily updatable (e.g., by software/data download).

The RF monitor should be able to detect rogue APs or other unauthorized devices. A straightforward approach would be to verify the MAC addresses of all wireless devices against an access control list (ACL). However, because MAC address spoofing could circumvent this approach, a more sophisticated mechanism (e.g., certificate-based verification) might be preferable.

Depending on the type of event detected, a network administrator should be notified as quickly as possible once an anomalous event or condition becomes evident. In the case of a network attack or rogue devices, a real-time alert mechanism (e.g., pager) is essential. This immediate notification can be important because there is a small window of opportunity after the event is detected for thwarting the attack and possibly apprehending the attacker. At a minimum, the RF monitor should log all information related to the event (e.g., timestamp, MAC address).

It would be beneficial for the RF monitor to be integrated into an existing, centralized incident response system. It is generally easier and more cost-effective to maintain a centralized system than to employ multiple, independent systems.

The RF monitor must be Common Criteria certified against any existing protection profiles (see Section 5.1). Table 4-3 provides a summary of the features and configuration of the RF monitor.

Table 4-3. RF Monitor Features/Configuration

RF Monitor Features/Configuration	Required	Recommended
IEEE 802.11 signal detection	✓	
Continuous scanning capability	✓	
Attack signature recognition (updatable)	✓	
Rogue AP/client detection	✓	
MAC address ACL verification		✓
Audit logging capability	✓	
Real-time alert mechanism (e-mail, pager, etc.)	✓	
Integration with centralized monitoring and management systems		✓
Network health verification (e.g., interference, slow performance)		✓
Common Criteria certified against any existing protection profiles	✓	

4.1.5 Access Control Device

As its name suggests, the access control device controls access to the network. This functionality may be provided by an integrated network firewall or another mechanism. The device performs its control function by authenticating the wireless client to the network. This process begins with the client's passing its credentials to the access control device during network login. Strong authentication, such as DOD PKI will be used , the device will communicate with an authentication server to determine whether the client credentials are acceptable and then pass the results to the client. Until a client has been authenticated and authorized, the device should not allow traffic from that client to pass onto the wired LAN (or vice-versa).

Once authentication is complete, the access control device will construct the encrypted tunnel with the wireless client through which the session traffic will pass. This process sometimes involves encryption algorithm and protocol negotiation.

The device should have a logging capability for documenting events such as client logins/logoffs, failed logins, and unauthenticated/unauthorized traffic. To prevent session hijacking, the access control device also should time-out sessions that are inactive for 15 minutes (or less if required by local security policy).

The access control device must be Common Criteria certified against any existing protection profiles (see Section 5.1).

Table 4-4 provides a summary of the features and configuration for the access control device.

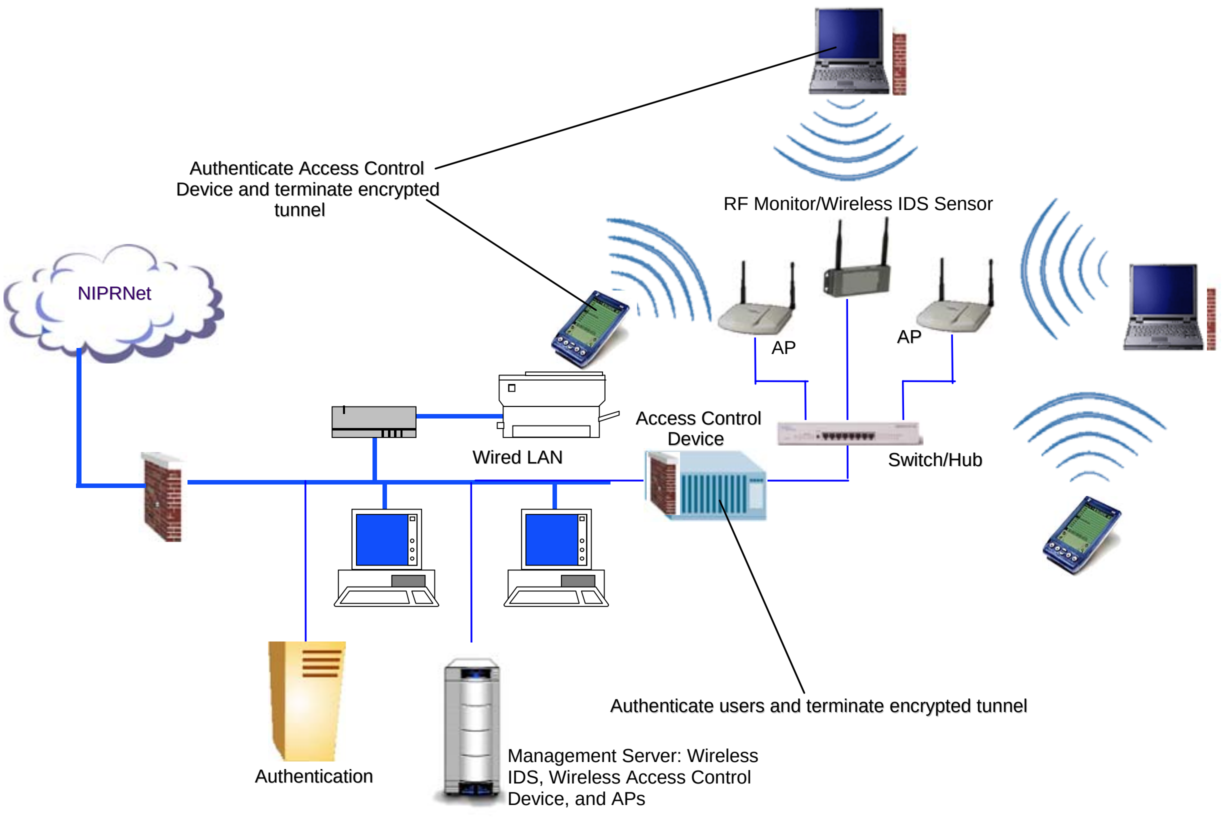
Table 4-4. Access Control Device Features/Configuration

Access Control Device Features/Configuration	Required	Recommended
Common Criteria certified against any existing protection profiles	✓	
Network access control (e.g., integrated firewall)	✓	
Authentication functionality	✓	
Encrypted tunneling capability (FIPS-140-2 certified)	✓	
Audit logging capability	✓	
Session time-out set to 15 minutes (or less if required by local security policy)		✓

4.1.6 Architecture

Figure 4-3 displays the generic architecture for the WLAN Security Framework.

Figure 4-3. Generic Architecture


Authenticate Access Control Device and terminate encrypted tunnel
RF Monitor/Wireless IDS Sensor
NIPRNet
AP
AP
Access Control Device
Switch/Hub
Wired LAN
Authenticate users and terminate encrypted tunnel
Authentication
Management Server: Wireless IDS, Wireless Access Control Device, and APs

A wireless network session will start with the wireless client's establishing a connection with an AP within range. The negotiated session will be 128-bit WEP or WPA enabled. If implemented, the AP will also verify the client's MAC address to ensure that it is authorized to access the network.

At the same time, the RF monitor will detect the presence of the client and the AP and log appropriate audit information (i.e., MAC addresses, date/time detected). If the RF monitor detects any unauthorized MAC addresses, the event will be logged and a system administrator alerted as soon as possible (e.g., by pager or e-mail). This alert mechanism could be accomplished by connecting the RF monitor with the local network operations center. (The switch/hub is not required for any security functions in this architecture; it is simply a pass-through device.)

The client will then authenticate itself to the access control device. The credentials required in this transaction should be either certificate or two-factor based. The access control device will consult the authentication server to verify the user's credentials and to provide authorization details. Regardless of whether the provided credentials are valid, appropriate audit information (credentials, MAC address, date/timestamp) should be logged by the authentication server.

After authentication is complete, an encrypted tunnel will be generated between the access control device and the wireless client. The tunnel will be terminated at those devices and not extended to other devices.

At this point, the wireless client has a secure connection to the internal network and should have access to any resources for which it has been authorized.

For all LAN activity, a network IDS will monitor the network for suspicious traffic (i.e., possible attack scenarios, including port scans, denial of service/SYN floods). In addition, it will verify system integrity (e.g., system file changes) and log any auditable events.

4.2 VIRTUAL PRIVATE NETWORK IMPLEMENTATION

This implementation uses a VPN device as its access control device. VPNs have become a popular technology for securing network traffic over the Internet. They are commonly used for remote user access and network-to-network communication. VPNs support a number of security mechanisms:

- **Tunneling.** Allowing a device (also known as a tunnel endpoint) to transmit packets containing sensitive data across a public, unsecured network encapsulated within another packet for protection, usually via encryption. The outer packet is passed in the clear and contains all of the routing information a public network needs to deliver the packet to the desired network address (another tunnel endpoint). Once the complete packet has been safely delivered to the trusted network device, the outer packet is shed and the inner packet is decrypted and routed to its intended destination.

- **Authentication.** Ensuring that all tunnel endpoints can verify each other's identity. See Section 7.3 for additional information on authentication.
- **Access Control.** Determining what users and devices have permission to access the network, as well as which individual resources should be made available. This determination is usually made on the basis of three factors: the identity of the requesting user and device, the resources requested by the user, and the predetermined access rules.
- **Data Security.** Including strong encryption and data integrity to guard against network attacks, including information tampering and capturing.

VPNs can be implemented in hardware or software using, for example, the IPSec protocol suite.[1]

4.2.1 VPN Device

All of the components discussed in Section 4.1 are applicable to this implementation. A VPN device (which may consist of a VPN gateway or concentrator) will fulfill the role of the access control device. The device must meet all requirements listed in Table 4-5.

Table 4-5. VPN Compliance With Access Control Device Requirements

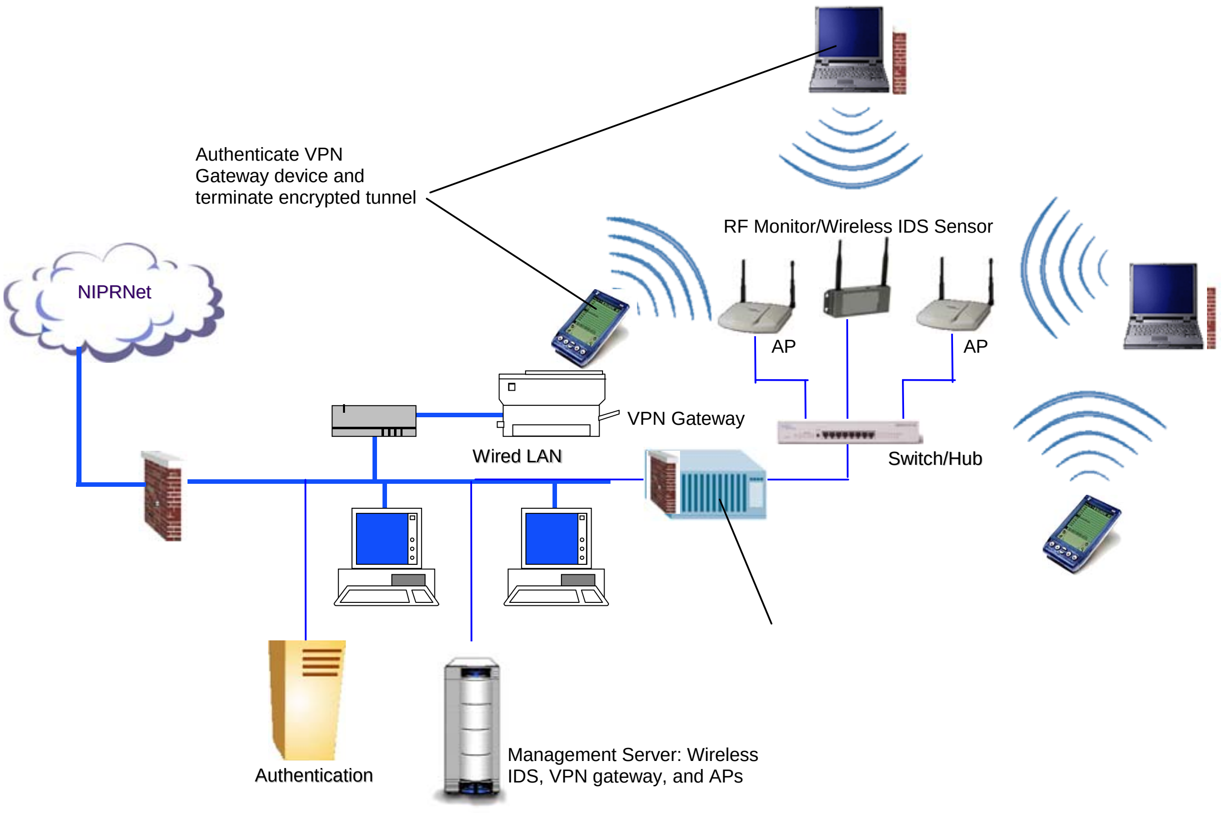
Access Control Device Features/Configuration	VPN Device Features
Common Criteria certified against any existing protection profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	VPN access control. Depending on the specific product chosen, a supplemental network firewall could be required.
Authentication functionality	VPN authentication (IPSec)
Encrypted tunneling capability (FIPS-140-2 certified)	VPN tunneling and data security (IPSec ESP tunneling). Ensure that encryption is FIPS-140-2 certified.
Audit logging capability (DOD 8500.1/2 compliant)	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.2.2 Architecture

Figure 4-4 displays the architecture for the VPN implementation. In this implementation, a VPN tunnel is generated between the wireless client and the VPN device. During tunnel construction, both authentication and encryption algorithms will be negotiated and executed. The tunnel must be terminated at the specific client and VPN devices and not extended to other devices.

[1] IPSec is an Internet Engineering Task Force (IETF) standard for providing secure communication over IP networks.

Figure 4-4. VPN Implementation Architecture


Authenticate VPN Gateway device and terminate encrypted tunnel
RF Monitor/Wireless IDS Sensor
NIPRNet
AP
AP
VPN Gateway
Wired LAN
Switch/Hub
Authentication
Management Server: Wireless IDS, VPN gateway, and APs

4.2.3 Benefits and Limitations

The VPN implementation has a number of benefits. It is very scalable in terms of the number of clients it can service. The only client limit would be vendor-implementation specific. Further, because VPNs are normally implemented at Open Systems Interconnection (OSI) Layer 3 (the network layer), they can support a number of upper layer protocols (e.g., Layer 4, transport protocols: Transmission Control Protocol [TCP], User Datagram Protocol [UDP]) and therefore support a wide variety of network applications.

VPNs should have a relatively low total cost of ownership (TCO). Because VPNs are based on an open standard, a number of vendors have products available. The resulting competitive marketplace should be an advantage to the buyer.

4.3 Wireless Security Gateway Implementation

This implementation uses a wireless security gateway as its access control device. Wireless security gateways have been made available by a number of vendors and provide similar functionality to VPNs (described in Section 4.2) specifically for WLANs. The security mechanisms offered can be a mix of standards- and proprietary-based mechanisms. Depending on the vendor, encrypted tunneling can be provided at different OSI network layers.

Each gateway can support a number of APs, either directly or via switching or hubbing. For further scalability, a number of gateways can be deployed for a single WLAN to provide redundancy, fail-over protection, and seamless roaming. To manage an infrastructure with multiple gateways, vendors usually offer a centralized gateway management server to facilitate administrative tasks.

In this implementation, wireless user devices will need to have a client software package installed to communicate with the gateway. Client software is normally available for a number of devices, including laptops, PDAs, and barcode scanners. Once the package is installed, minimal (if any) configuration is required to use the secure network.

4.3.1 Wireless Security Gateway

All of the components discussed in Section 4.1 are applicable to this implementation. A wireless security gateway will fulfill the role of the access control device. The gateway must meet all of the requirements listed in Table 4-6.

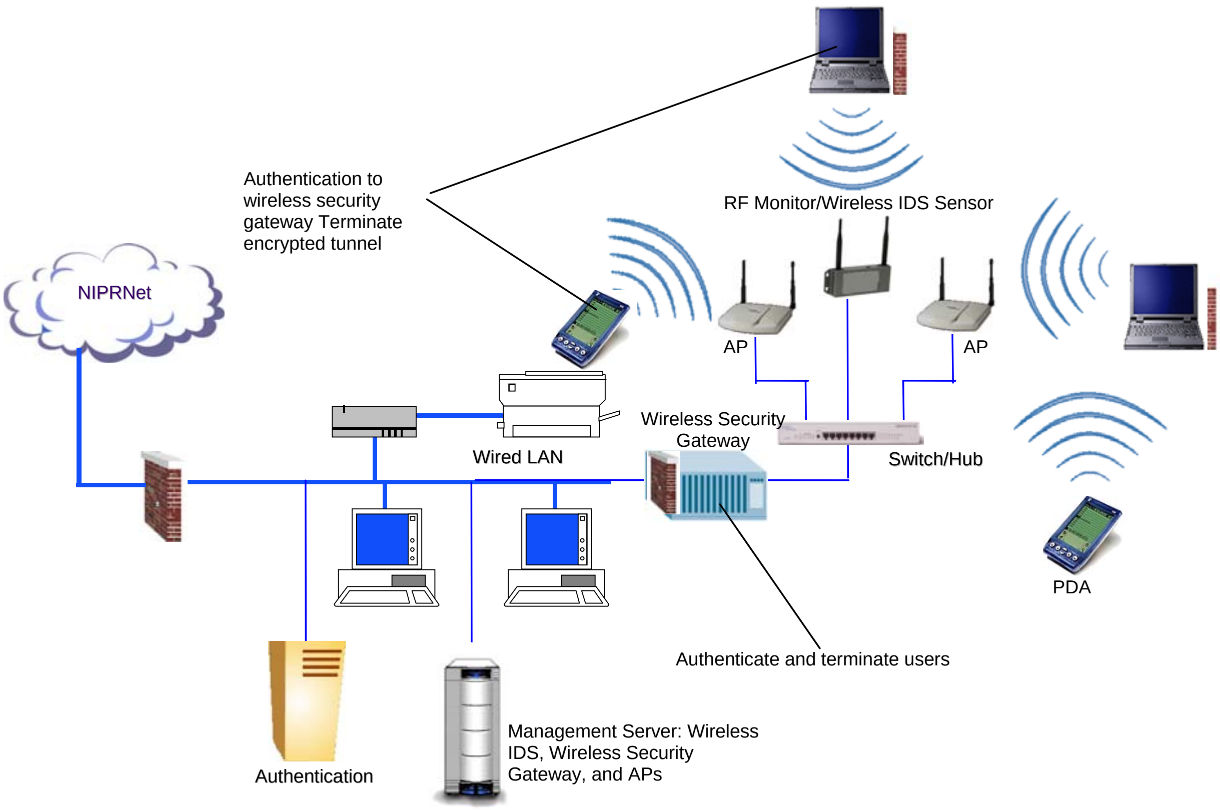
Table 4-6. WLAN Security Gateway Compliance With Access Control Device Requirements

Access Control Device Features/Configuration	Wireless Security Gateway Features
Common Criteria certified against any existing protection profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Vendor-specific. Preferably a standard authentication protocol is used (e.g., Extensible Authentication Protocol [EAP]).
Encrypted tunneling capability (FIPS-140-2 certified)	Vendor-specific.
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.3.2 Architecture

Figure 4-5 displays the architecture for the wireless security gateway implementation.

Figure 4-5. Wireless Security Gateway Implementation Architecture


Authentication to wireless security gateway Terminate encrypted tunnel
RF Monitor/Wireless IDS Sensor
NIPRNet
AP
AP
Wireless Security Gateway
Switch/Hub
Wired LAN
PDA
Authenticate and terminate users
Management Server: Wireless IDS, Wireless Security Gateway, and APs
Authentication

In this implementation, an encrypted tunnel is generated between the wireless client and the wireless security gateway. During tunnel construction, both authentication and encryption algorithms will be predetermined (or negotiated) and executed. The tunnel must be terminated at the specific wireless client and wireless security gateway devices and not extended to other devices.

4.3.3 Benefits and Limitations

The wireless security gateway implementation has a number of benefits and limitations. Among its benefits, most commercially available gateways offer seamless roaming across APs for wireless users. This is a great advantage for mobile users who require a large connectivity area. In addition, multiple gateways can be deployed for scalability and fail-over protection. However, purchasing numerous gateways can be costly.

Gateways are relatively easy to use for wireless clients. Once the network is set up, a wireless user need only authenticate to the network via standard login procedures (user identifier [ID]/password) or certificate (e.g., CAC and personal identification number [PIN]). Once authenticated, the user is abstracted from the underlying security and should have access to all authorized network resources.

One potential limitation of the wireless security gateway relates to interoperability. Depending on vendor implementation, proprietary rather than open standard mechanisms could be used. These proprietary mechanisms might not interoperate with other vendors' systems. If multiple vendors' products will be used in implementing a WLAN, users should ensure that interoperability will not be an issue with this type of implementation.

4.4 WIRELESS SECURITY SWITCH IMPLEMENTATION

This implementation uses a wireless security switch as its access control device. A wireless security switch is similar to a wireless gateway in that it can support multiple APs, either directly or via switching or hubbing. However, a wireless switch contains all of the connection handling functionality that is normally reserved for APs. This allows use of much simpler, smaller, and cheaper APs.

In addition, by moving the connection handling from the AP to the switch, functionality such as load balancing, congestion control, and subnet roaming can be effectively provided.

4.4.1 Wireless Security Switch

All of the components discussed in Section 4.1 are applicable to this implementation. A wireless security switch will fulfill the role of the access control device. The switch must meet all of the requirements listed in Table 4-7.

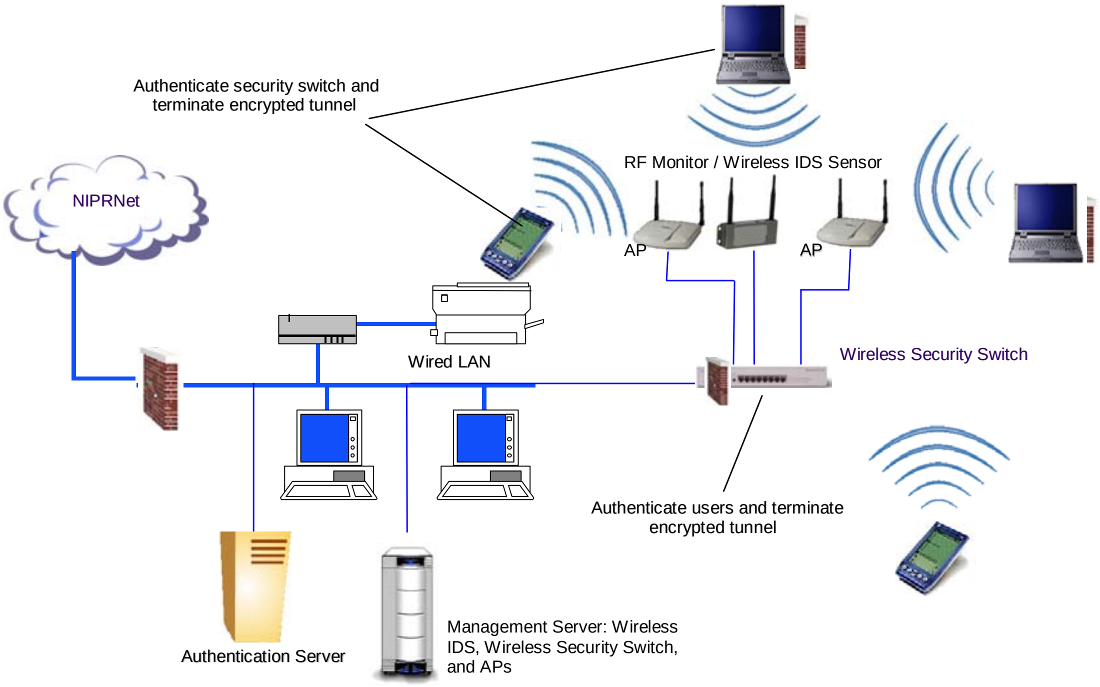
Table 4-7. WLAN Security Switch Compliance With Access Control Device Requirements

Access Control Device Features/Configuration	Wireless Security Switch Features
Common Criteria certified against any existing protection profiles	Some products are certified and some are not. Be sure to verify certification, if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Vendor-specific. Preferably a standard authentication protocol is used (e.g., EAP).
Encrypted tunneling capability (FIPS-140–2 certified)	Vendor-specific.
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.

4.4.2 Architecture

In this implementation, an encrypted tunnel is generated between the wireless client and the wireless security switch. During the tunnel construction, both authentication and encryption algorithms will be predetermined/negotiated and executed. The tunnel must be terminated at the specific wireless client and wireless security switch devices and not extended to other devices. Figure 4-6 displays the architecture for the wireless security switch implementation.

Figure 4-6. Wireless Security Switch Implementation Architecture


Authenticate security switch and terminate encrypted tunnel
NIPRNet
RF Monitor / Wireless IDS Sensor
AP
AP
Wired LAN
Wireless Security Switch
Authenticate users and terminate encrypted tunnel
Authentication Server
Management Server: Wireless IDS, Wireless Security Switch, and APs

4.4.3 Benefits and Limitations

The wireless security switch implementation has a number of benefits, including those associated with other implementations, such as scalability, centralized management, and roaming support. In addition, a unique benefit of this implementation is its support for simple, cheap APs. Because a number of APs are usually required for any WLAN, this could significantly lower TCO.

4.5 802.11I ROBUST SECURE NETWORK STANDARDS-BASED IMPLEMENTATIONS

This implementation uses an RSN-capable AP or wireless switch as its access control device. RSN is a major component of the 802.11i wireless security standard. Specifically, it is a total redesign of the authentication and association mechanisms used in existing 802.11 standards. The IEEE 802.11i amendment was approved and published in July 2004, so vendors will soon begin to provide devices that implement it. However, because the amendment is so new, it is important to note that the following implementation is based on *expected* capabilities of RSN devices.

The RSN capability will be contained in devices at the wireless edge of the network (i.e., APs and wireless switches) rather than devices further inside the WLAN as in the other implementations. Because of the significant changes in the security mechanisms of 802.11i, legacy APs and wireless NICs will not be upgradable to the RSN standard. Rather, new hardware components will have to be purchased.

It is worth noting that the task group responsible for 802.11i made a concerted effort to design it to be compliant with FIPS-140-2. Although RSN by itself will not satisfy the encryption mechanism required by policy, RSN-capable APs and wireless switches will add a layer of security to the overall architecture.

4.5.1 RSN-Capable Access Point or Wireless Switch

All of the components discussed in Section 4.1 are applicable to this implementation. An RSN-capable AP or wireless switch will fulfill the role of the access control device. The device must meet all of the requirements listed in Table 4-8.

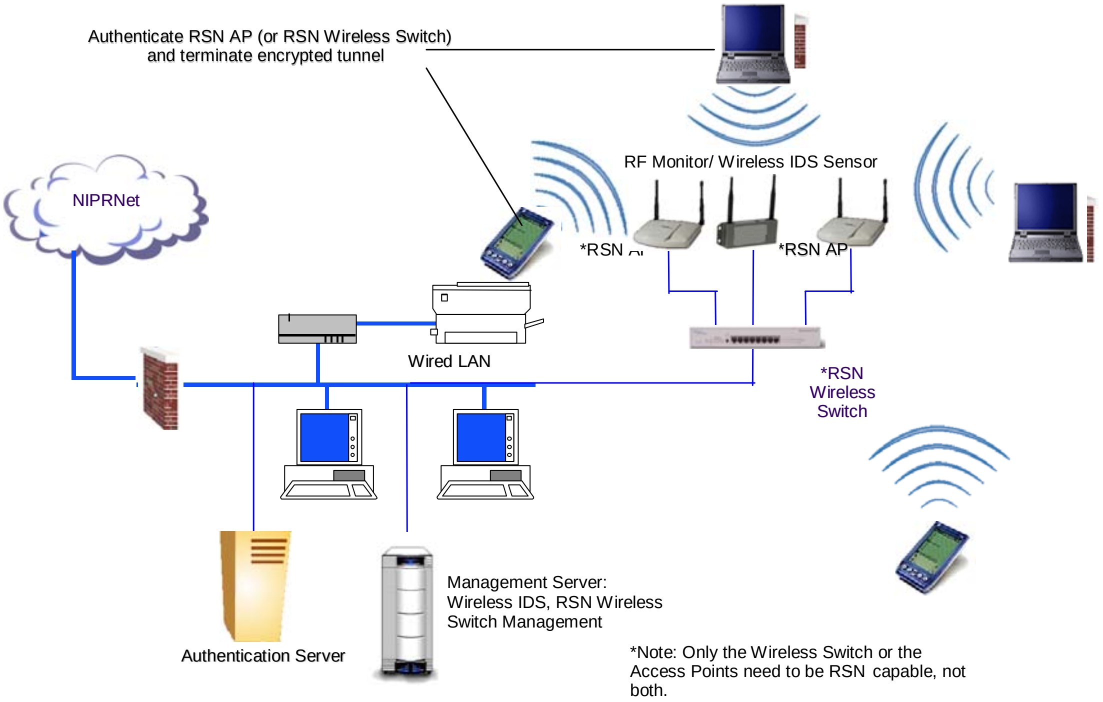
Table 4-8. RSN-Capable Access Point or Wireless Switch Compliance With Access Control Device Requirements

Access Control Device Features/Configuration	RSN-Capable Access Point or Wireless Switch Features
Common Criteria certified against any existing protection profiles	Some products are certified and some are not. Be sure to verify certification if applicable.
Network access control (e.g., integrated firewall)	Vendor-specific. Depending on specific product chosen, a supplemental network firewall may be required.
Authentication functionality	Depends on finalized standard. Preferably a standard authentication protocol is used (e.g., EAP).
Encrypted tunneling capability (FIPS-140-2 certified)	Depends on the finalized standard.
Audit logging capability	Vendor-specific. It is recommended that a fully configurable auditing capability be available.
Perform strict syntactic and semantic analysis of information provided by wireless clients	Vendor-specific. Rigorous testing should be performed to ensure that there are no design flaws. Otherwise, attacks such as buffer overflows may be possible. See Section 4.5.3.

4.5.2 Architecture

Figure 4-7 displays the model architecture for the RSN standards-based implementation.

Figure 4-7. Robust Secure Network Implementation Architecture


Authenticate RSN AP (or RSN Wireless Switch)
and terminate encrypted tunnel
RF Monitor/ Wireless IDS Sensor
NIPRNet
*RSN AP
*RSN AP
Wired LAN
*RSN
Wireless
Switch
Management Server:
Wireless IDS, RSN Wireless
Switch Management
Authentication Server

*Note: Only the Wireless Switch or the Access Points need to be RSN capable, not both.

In this implementation, an encrypted tunnel is generated between the wireless client and the RSN-capable device. During the tunnel construction, both authentication and encryption algorithms will be predetermined/negotiated and executed. The tunnel must be terminated at the specific wireless client and RSN-capable devices and not extended to other devices.

4.5.3 Benefits and Limitations

The RSN-based implementation has a number of benefits. For example, an RSN-capable device should have predominantly standards-based mechanisms, including strong encryption and authentication.

On the downside, it will not be possible to upgrade existing WEP/WPA enabled wireless devices to the RSN standard. Therefore, new APs, wireless switches, and wireless NICs will need to be purchased. Depending on the number of those components needed, this solution could therefore be more costly than the other implementations discussed.

As noted in Table 4-8, the security of the above architecture depends on the RSN device's providing thorough syntactic and semantic analysis of data provided by wireless clients. If the RSN device does not inspect data content, hostile wireless clients could perform buffer overflow attacks on devices on the wired LAN (e.g., the authentication server).

4.6 WRAP-UP DISCUSSION

The reference implementations discussed above provide models for implementing a secure, policy-compliant WLAN. In instances in which VPN components are already purchased and available, it may be best to procure some basic APs and use the available VPN device(s) for access control. FIPS-140-2 certified wireless gateways and switches are relatively new to the marketplace; therefore, they probably will not be found in existing inventory. But they are very scalable and support simple (i.e., cheap) APs. For WLANs supporting a large user base and requiring capabilities such as subnet roaming, these features should be attractive.

Because the 802.11i standard was published only in July 2004, and vendors have yet to supply compliant products, it is difficult to forecast the relative cost factor of the 802.11i RSN standards-based implementation. The marketplace for the new devices should be competitive, particularly for the educated consumer. It appears that RSN-enabled switches will scale less expensively than will RSN-capable APs, especially in WLANs in which a significant number of APs are required. Future revisions of this document will follow the progress of 802.11i devices and their role in a secure, policy-compliant WLAN.

5. IMPLEMENTATION CONSIDERATIONS

This section discusses items that must be addressed and understood before implementation of a wireless LAN. Some major elements among these include the Common Criteria, C&A, policies and procedures, proprietary solutions, and scalability.

5.1 COMMON CRITERIA

The Common Criteria defines general concepts and principles of IT security evaluation and presents a basis for evaluating the security properties of IT products. It also establishes a common basis for expressing IT security objectives, selecting and defining IT security requirements, and writing high-level specifications for products and systems. DOD uses the Common Criteria for procurement only of commercial off-the-shelf products for unclassified use. Using the Common Criteria, DOD develops protection profiles to specify the security properties desired for the product.

According to the policy presented in DODI 8500.2, all IA products must be evaluated and validated in compliance with National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, with the following qualifications:

- If there is a U.S. government protection profile and there are validated products for that protection profile, the Government is restricted to procuring only those products or products that vendors have submitted, before purchase, for evaluation and validation against a Security Target (ST) written to that protection profile.
- If there is a U.S. government protection profile and there are no products for that protection profile, the Government must require, before purchase, that the product be submitted to a NIAP EVP or Common Criteria Recognition Arrangement (CCRA) laboratory for evaluation and validation against an ST written to that protection profile.
- If no U.S. government protection profile exists, the organization must require that the vendor provide an ST that describes the security attributes of the product and submit its product to be evaluated and validated by a Designated Approving Authority (DAA)–approved Evaluation Assurance Level (EAL).

Ideally, only Common Criteria products that are validated against a NIST or a National Security Agency (NSA) protection profile should be used as security components in DOD WLANs.

5.2 CERTIFICATION, ACCREDITATION AND THE CONNECTION APPROVAL PROCESS

C&A is the standard DOD approach for identifying information security requirements, providing security solutions, and managing the security of DOD information systems.

In accordance with DODD 8100.2, wireless devices, services, and technologies that are integrated or connected to DOD networks are considered part of those networks and must be certified and accredited in accordance with DODI 5200.40. For the latest on DOD policies, go to http://www.dtic.mil/whs/directives/. In either implementing a new system using wireless solutions or implementing wireless solutions for a previously certified system, the procedures for accreditation and re-accreditation outlined in the DITSCAP should be followed. The Connection Approval Process (CAP) procedure must also be adhered to in connecting wireless devices to an existing system. DOD agencies can establish a CAP that is specific to their systems. For example, DISA has a CAP specifically for any wired and wireless connection to the Secret Internet Protocol Router Network (SIPRNet) or NIPRNet. Several publications define criteria for the evaluation and validation of a system or product. However, just because a system or product holds a certain rating when it stands alone does not guarantee security when it is installed in a particular environment. The C&A of a system will take into account the system's administration, physical security, installation, configuration mechanisms within the environment, and other security issues. Because software, systems, and environments are continually evolving, C&A of a system should be an ongoing process.

A standard process that entails all criteria should be included as the system is established and implemented. Appendix A provides a checklist that should be followed during the development and ultimately the deployment of the WLAN. Some initial actions include identification of specific personnel positions and development of a security policy. Within this policy, certain duties and parameters should be established to cover the requirements and functionality of the operational environment and how the system will be used. As with any well-thought-out development effort, the C&A and CAP processes will require substantial documentation, including the following:

- Concept of Operations (CONOPS)
- Architecture and design
- Operating procedures
- Network diagrams
- Configuration management documents
- Security incident handling process and procedures.

In addition, various aspects of the system should be tested. Among the tests that will be needed are security test and evaluation (ST&E), penetration testing, and testing of the wireless network connections. All results of these tests should be documented. Following the requirements of C&A and CAP will facilitate the secure deployment of the WLAN.

5.3 Policies and Procedures

Currently DOD is promoting the sharing of vulnerability mitigation strategies throughout the various DOD entities.[2] As a result, policies have been developed to provide a balanced approach to mitigating risks in unclassified and unclassified-but-sensitive environments. DOD policy[3] mandates that all wireless technologies include protection mechanisms, detection and monitoring, response and recovery capabilities, and IA assessment tools and techniques. In addition, the Pentagon[4] and various organizations within DOD have devised policies that both comply with DODD 8500 and include additions relating to the respective environments. It is recommended that each local entity ensure that its local security policy is built on and compliant with DODD 8500.1/2 and DODD 8100.2.

5.4 Proprietary versus Standards-Based Solutions

There are many avenues for deploying and managing secure WLANs. The IEEE established the 802.11 standard so that users could procure interoperable products from multiple vendors to expand their networks. Because the current standards-based solutions have not proved to be secure, vendors have developed a number of proprietary security solutions. However, using proprietary solutions locks users into a single vendor and leaves them at the mercy of that vendor for upgrades and fixes. In addition, these solutions are immature, are not interoperable, are expensive, and can present numerous additional requirements for installation and maintenance.

It is recommended that agencies use tested and validated security mechanisms in network components.[5] Doing so ensures, at a minimum, that experts have documented and verified the security of algorithms and the architecture of the mechanism. Following this practice does not mitigate all implementation-related risk but does ensure that the mechanism's foundation is sound.

5.5 Scalability and Interoperability

The WLAN should be designed for maximum efficiency and availability and should anticipate the growth of the organization. The choice of WLAN solutions will be determined on the basis of the size and geographical distribution of the organization. Among the practical aspects of mechanism deployment that are critical to a solution's effectiveness are scalability and interoperability.

First, the mechanism must be scalable according to the network's needs. For example, user population can be a dynamic characteristic. As the user base grows, the security

[2] Pentagon Area Common Information Technology (IT) Wireless Security Policy.

[3] Department of Defense Instruction (DODI) 8500.2.

[4] See Pentagon Area Common Information Technology (IT) Wireless Security Policy.

[5] NIST Special Publication 800-48.

mechanisms must be able to handle the additional load, such as user accounts and device management. Current requirements might be sufficient for today’s needs; however, advances will soon demand a more intelligent infrastructure that will eliminate the need to add significant infrastructure. The network designer must consider not only conventional requirements but also future needs.

It is also important to implement security devices in a manner that will provide interoperability between devices in the event of network expansion. When considering scalability, agencies must recognize and ensure that networks are flexible, manageable, and standards-based.

5.6 PHYSICAL SECURITY

As network environments become more complex and volatile, it is imperative that organizations address the impending threat of information attacks. Maintaining strong physical security should be a critical part of any IT infrastructure.

Establishing physical security entails consideration of three primary types of control mechanisms: administrative, technical, and physical. If implemented correctly, these mechanisms will help provide a secure environment and prevent theft of network devices and the unauthorized disclosure of information through network attacks.

Administrative and physical controls are similar in that they involve implementing security mechanisms with respect to facility locations and layouts. For instance, agencies must consider the surrounding terrain and such physical deterrents as fencing and gates when installing wireless devices within radio communication range of APs. Placing an AP near a public or unsecured area would not be wise because such placement would give an attacker easier access to network traffic. In mounting APs and antennas, agencies should also take precautions to minimize these elements’ exposure to transmitters and other potential sources of interference.

In addition, unauthorized individuals should be prohibited from having physical access to WLAN devices and cabling, and usage by authorized users should be monitored and logged. Isolated areas that are difficult to monitor should be equipped with remote access monitoring devices staffed by security personnel.

As necessary as these steps are, however, it is important to recognize that physical deterrents provide a minimal level of security and rarely deter attackers. As the sophistication of hacking tools increases, it is not wise to rely on physical security alone to protect wireless networks.

6. ADMINISTRATIVE CONTROLS

Maintaining the security of a WLAN requires constant vigilance. The network should be constantly monitored for behavior that would indicate unauthorized activity. Security administration should be established to protect the network and ensure that all security policies are being followed. The following subsections discuss critical administrative controls that must be implemented in addition to technical mechanisms (discussed in Section 7).

6.1 AUDITING

An auditing capability is an essential component of a WLAN system. In a network, the system must be able to capture network events, also referred to as auditable events (as defined by an administrator), and to log sufficient information for analysis. There are many events that occur on a network that must be captured to ensure that users are accountable for their actions, to verify that the security policies are being enforced, and to serve as investigative tools. Although auditing does not deny an entity access to the network or its resources, it will track activities so that a network or system administrator can assess the type of access that took place, identify a security breach, or warn the administrator of suspicious activity. In implementing the audit functionality, a baseline of current activity must be established and future activity must be measured against the baseline, evaluating any change from preexisting thresholds. The audited events must be analyzed against the level of security risk they present.

In addition to dealing with immediate crises, auditing can point out weaknesses in other technical controls and help the administrator understand changes that need to be made to preserve the necessary security level within the environment.

Audit logs contain a considerable amount of information and must be presented in an organized format. The recorded information can be organized according to system-level, user-level, and application-level events based on administrator-configured actions. The threshold and parameters for the different event types must be configured by an administrator. Moreover, it is not sufficient to simply gather event information; the audit logs must be monitored so that the appropriate responses can be executed.

6.2 MONITORING AND MANAGEMENT

Monitoring and management are important detective mechanisms that identify persons who attempt to gain and succeed in gaining authorized access to the network and the information it contains. These mechanisms are particularly important with WLAN implementations since, because of the nature of RF transmissions, it is fairly easy for attackers to intrude on the medium by which such data traverses the network. Monitoring is one of the technological means of detection that can enhance the security of the wireless link, the client, and the endpoints. Monitoring mechanisms that identify unauthorized activity on a network enable administrators to be proactive with network security. (See Section 4.1.4 for a discussion of wireless IDSs and how they are used to monitor networks.)

An important complement to monitoring, and a key to its effectiveness, is management. In fact, management and monitoring are generally seen as inextricably linked in that it is impractical to have monitoring mechanisms without administrators to assess the reported discovery. For example, if a user fails to log in to a network after a certain (pre-established) number of attempts because he or she is entering an incorrect password, an audit log will result. But this information is of negligible value unless someone views the information and takes the appropriate action. To help ensure effective management, personnel should be designated to manage the information or alerts provided by the security devices.

To make effective use of the monitoring information provided, it will be necessary to identify, collect, and review pertinent log data almost constantly. This level of attention to all servers and equipment on the network is impossible for a network administrator to provide alone. Thus, it is recommended that all WLAN implementations make use of one or more of the several products on the market that facilitate selection and prioritization of the information captured in audit logs.

6.3 INCIDENT RESPONSE

Unauthorized access attempts, denial-of-service attacks, and session hijacking can all have serious impacts on a network. Even when every precaution is being taken to mitigate such risks, WLANs will still be vulnerable to hackers. For this reason, DOD policy recommends that each location implement an incident response protocol system.

Typically on a wireless network, alerts from a monitoring device (such as an RF monitor), alerts from an IDS, or alerts generated from the monitoring of log files are used to detect an attack. Once such an incident has been detected, a brief time frame is available to respond to the incident, including determining the source and possibly capturing the attacker. Therefore, it is essential that agencies establish a functional response system, and perform routine operational maintenance to control and mitigate risks. This response should begin with the monitoring device’s advising an administrator, via pager, mobile phone, etc., of the event in real time. For further assistance, please contact JTF-GNO, the source for incident response support at http://www.cert.mil/misc/mission.htm .

7. TECHNICAL MECHANISMS

The importance of technical security mechanisms in countering threats to WLANs is reflected in DOD policy, which in some instances, mandates use of such means. Specific technical mechanisms that must be considered before implementing a WLAN, as well as the underlying DOD policy, are described in the following subsections.

7.1 RF MONITORING

The robustness and integrity of a WLAN depend on the ability of the network administrator to troubleshoot problems, respond to misconfiguration, and plan for future implementations and upgrades. Because of the complexity of WLANs and the numerous components needed to deploy a WLAN securely, accomplishing these tasks requires that network administrators be able to effectively, constantly monitor all network security components.

There are two types of RF monitoring (the form of monitoring used on WLAN systems): one involves physically driving or walking around certain areas, equipped with a sniffer to detect the presence of WLANs; another, more effective type is surveying wireless devices and client machines by using sensors strategically placed at the various components of the WLAN. In the latter type of monitoring, the sensors report back to a central monitoring or management console.

7.1.1 Policy

DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG), states—

> In Section 4.1.4, "Measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources."
>
> In Section 4.6, "The DOD Components shall actively screen for wireless devices. Active electromagnetic sensing at DOD or contractor premises to detect/prevent unauthorized access of DOD information systems shall be periodically performed by the cognizant DAA or Defense Security Service office to ensure compliance with the DITSCAP ongoing accreditation agreement..."

By helping mitigate attacks, such as denial-of-service, man-in-the-middle, and identity theft attacks, RF monitoring will satisfy the above policy requirements, protecting the network, not only from outside sources, but also from friendly sources.

7.1.2 Implementation

When an RF monitoring scheme is employed, it should contain the necessary mechanisms to provide a real-time network survey. The use of stationary or mobile sensors will allow detection of rogue APs, ad hoc networks, and unencrypted traffic. RF monitoring can also provide the following:

- Monitoring of off-hours traffic
- Mitigation of denial-of-service attacks
- Identification of hardware failure, network interference, slow connection speeds, and network misconfiguration.

Continuously surveying the airwaves in and around the facility housing the WLAN will allow for constant monitoring of a system's components, assisting in the prevention and detection of attacks.

7.2 ENCRYPTION

Attacks against wireless networks are often directed at the wireless link or the means of data transmission. There must be an effective way to protect information as it is stored on media or transmitted through network communication paths. The ultimate goal of encryption is to hide information from unauthorized individuals and to provide some degree of integrity protection. Although most encryption algorithms can eventually be cracked, revealing the protected information, if an attacker has enough time, motivation, and resources, a realistic goal is to make the time required to break the algorithm so long that it is unrealistic to execute a brute force attack.

The WEP protocol, which is used to secure the link between a wireless client and an AP, was originally designed to provide security for WLANs; however, its implementation was flawed. In recognition of these deficiencies, the WiFi Alliance, in conjunction with IEEE, created WPA as an interim solution that is interoperable with and strongly enhances wireless security. WPA uses TKIP to improve data encryption. Although WPA-TKIP still uses the RC4 algorithm (the algorithm on which WEP is based), it changes temporal keys every 10, 000 packets and with proper key management. However, WPA-TKIP is not approved for government uses because it is not FIPS-140-2 compliant.

WPA is forward compatible with the IEEE 802.11i security specification. The 802.11i Working Group has also included Advanced Encryption Standard (AES) CCMP (AES-CCMP) as a part of its standard. This solution is expected to be validated by FIPS-140-2 and usable by DOD. In the interim, DOD must use other encryption solutions, such as IPSec VPNs or wireless security gateways providing FIPS-validated encryption.

The foundation for any cryptographic system is key management (the care and distribution of cryptographic keys). If cryptographic keys are not properly protected from unauthorized persons, any cryptographic solution will fail to meet its objective. Thus, in deploying a WLAN, distribution and management of keys must be addressed. Some solutions will use preshared keys; others will have a central key management infrastructure, such as a PKI. Both scenarios have strengths and weaknesses. Use of preshared keys creates a challenge in key distribution and key protection. A key management infrastructure such as a PKI solves many of these key management and protection problems but requires a complex infrastructure. Because protection is generally the paramount concern in a DOD WLAN, consideration should be given to using the DOD PKI when feasible and appropriate.

7.2.1 Policy

DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG), states—

> In Section 4.1.2, "Encryption of unclassified data for transmission to and from wireless devices is required. Exceptions may be granted on a case-by-case basis as determined by the designated approving authority (DAA). At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 or FIPS PUB 140-2, Overall Level 1 or Level 2, as dictated by the sensitivity of the data…. Encrypting unclassified voice is desirable. PEDs shall use file system encryption. Individual exceptions may be granted on a case-by-case basis as determined by the DAA."
>
> In Section 4.4, "When unclassified wireless local area networks (WLANs) are used to support joint operations, IPSec virtual private network (VPN) technology shall be used and encrypted per subparagraph 4.1.2."

As noted above, DOD policy requires that all encryption algorithms and protocols comply with FIPS-140-2. This is currently significant because, as noted, neither the WEP encryption scheme available in most 802.11 products nor WPA-TKIP is FIPS-140-2 compliant. WEP's flaws are well documented, and tools that crack WEP are readily available via the Internet. Therefore, WEP encryption alone will be insufficient to satisfy the encryption requirement.

7.2.2 Implementation

The framework presented in this document uses FIPS-140-2 compliant algorithms, such as AES or Triple Data Encryption Standard (3DES). With NSA approval of key mechanisms and implementation, all key lengths used in AES (i.e., 128, 192, 256) are adequate to protect classified information up to the Secret level. (Top Secret information requires key lengths of 192 or 256.[6]) AES or 3DES encryption will also be used for transmitting unclassified information because this information can be critical to the performance and operation of organizations and its compromise can have significant impacts.

Organizations can choose whether to use Network Layer 2 encryption, Layer 3 encryption, or both for their wireless networks. In the future, most organizations will probably migrate to the IEEE 802.11i Layer 2 solution due to its standards-based approach to security.

[6] CNSS Policy No. 15, FS-1 June 2003

7.3 IDENTIFICATION & AUTHENTICATION

For a network to be protected against unauthorized users, identification and authentication (I&A) mechanisms must be implemented. Many mechanisms are now available to provide identification, authentication, and authorization when an individual connects to a WLAN. Authentication solutions include username and passwords, smart cards, biometrics, and PKI. Strong two-factor mutual authentication will provide access control to the wired network and prevent man-in-the-middle attacks. Users connecting to the wireless network must first authenticate to the wireless network itself. In this case, the user authenticates to an AP or to some form of security gateway. Once successful authentication to the wireless network is complete and the connection is encrypted, authentication to network resources must also take place. This may include authentication to a Microsoft domain. For user-level authentication, certificate-based (e.g., PKI) or two-factor authentication is recommended.

A PKI enables users of a nonsecure public network to securely and privately exchange data through the use of a public and a private cryptographic key pair. The PKI provides for a digital certificate that contains the public key and can identify an individual or an organization that can store and revoke the certificates, if necessary.

Security token devices can also be used for strong authentication. The token device and the authentication server need to be synchronized to be able to authenticate the user. This method is called two-factor authentication because the token device will present the user with a sequence of characters to be entered into the computer along with an additional password.

In a wireless environment, mutual authentication must be used to prevent attackers from masquerading as an AP or security gateway. Mutual authentication mitigates the risk that an attacker could masquerade as an AP or a wireless gateway to accept and establish a connection with a wireless client. An example of mutual authentication is using DOD PKI certificates. Success in this type of attack could allow the attacker to access data on the client or upload hostile code. If authentication and authorization methods are properly implemented, the attacker could not employ user credentials or brute force to establish a connection to the wired network. (Note: An attacker who inserts himself or herself in the middle of a wireless connection but does not decrypt traffic or overcome the authentication scheme is not considered a more serious threat than an attacker with an antenna and a wireless sniffer.)

7.3.1 Policy

The main DOD policy documents related to I&A are DODD 8100.2 and DODD 8500.1.

DODD 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG), states—

> In Section 4.1.1, "Strong authentication, non-repudiation, and personal identification is required for access to a DOD information system (IS) in accordance with the DOD public key infrastructure (PKI) policy established by DOD Chief Information Officer (CIO). Identification and Authentication (I&A) measures shall be implemented at both the device and network level. Voice does not require DOD PKI I&A."

DODD 8500.1, Information Assurance, 24 October 2002, states—

> In Section 4.1, "Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DOD information systems in accordance with 10 U.S.C. Section 2224…"
>
> In Section 4.2, "All DOD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets…"
>
> In Section 4.8.2, "The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DOD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DOD-approved external certificate authority or other mechanisms approved in accordance with DOD policy."

In addition, several revised memorandums have established requirements for the use of PKI in network logon. These memorandums present instructions for use of PKI in DOD unclassified networks.

Department of Defense (DOD) Public Key Infrastructure (PKI) Memorandum, 12 August 2000, requires the following:

> *Enabling of Networks and Applications*: DOD unclassified networks shall be enabled for hardware token, certificate-based access control no later than October 2002, with organizations beginning this migration in December 2000, when Class 3 certificates on CACs will be available. Unclassified networks hosting mission-critical systems shall migrate to certificate-based access control using Target Class 4 tokens no later than December 32, 2003. Further guidance on enabling applications will be provided in a separate memorandum. Hardware token-based access control to classified networks is encouraged, and requirements for classified networks in this area will be provided in future guidance pending further study of technical and resource issues.

Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DOD) Memorandum, 17 May 2001, states—

> It is DOD Policy that:
>
> 4.1. In accordance with [the 12 August 2000 memorandum]:

> 4.1.1. All DOD unclassified networks that authenticate users, except as specified in 4.1.2, shall be PK-enabled for Class 3 hardware token, certificate-based access control conditional with the following:
>
> a. Availability of commercial certificate-based access control applications compatible with the network operating system; and
>
> b. DOD PKI issuance of access control application compatible certificates on hardware tokens (e.g., CACs) to all users of given network.
>
> Unclassified networks hosting Mission Category I systems…shall be given highest priority.
>
> 4.1.2. Unclassified DOD networks whose user communities belong predominantly to personnel categories not required to receive DOD PKI certificates in accordance with the 12 August 2000 memo] e.g., retirees, dependents, academia, are exempt from 4.1.1.

Public Key Infrastructure (PKI) Policy Update Memorandum, 21 May 2002, states—

> Certificate issuance and other [12 August 2000 and 17 May 2001 memo] requirements impacted by the revised RAPIDS fielding schedule and/or directed for completion by October 2002 are included in the following table along with revised implementation dates:

Applicable Policy	Existing October 2002 Requirement	Adjusted Milestone Date
[12 August 2000 memorandum, 17 May 2001 memorandum 4.1]	PK-enable DOD unclassified networks for hardware token, certificate-based access control	October 2003

DOD has established the use of hardware token, certificate-based access control in the form of the CAC. In addition, as stated in the PKE memorandum cited above, all DOD unclassified networks that authenticate users, unless specifically excepted by waiver, shall be public key (PK)–enabled. For many WLANs, PKI has also been deployed to provide added security.

7.3.2 Implementation

Current policy is that DOD PKI must be used to identify and authenticate users as they log onto networks. This neither requires nor prohibits that authentication to the WLAN device use DOD PKI digital certificates. Although authentication methods that do not incorporate DOD PKI can be used for accessing the WLAN, DOD PKI is mandated for use in identifying users as they log onto DOD networks.

In a wireless network environment, the requirements outlined in current DOD policy memorandums would be satisfied if the user authenticated to the network using a digital certificate on the user’s CAC, even if the user’s wireless device used a different technology to authenticate itself to the wireless AP. Nevertheless, it is recommended that the CAC be used for a single sign-on authentication to the WLAN and network resources (user logon). The DOD PKI policy memorandums require the incorporation of public key technology into Web application authentication and e-mail signature and encryption. Therefore, a network infrastructure that includes wireless components that will be used by individuals to access e-mail and Web servers must make it possible for those users to use their CACs to perform certificate-based authentication, digital signature, and encryption, even if the device logon or network logon is not yet using digital certificates.

Mutual authentication is necessary in a wireless environment to prevent attackers from masquerading as an AP or a security gateway.

Note: Protected Extensible Authentication Protocol (PEAP) and Lightweight Extensible Authentication Protocol (LEAP) are not recommended as authentication mechanisms. There are known man-in-the-middle attacks that cannot be mitigated when using PEAP. PEAP's flaws are based on limitations in the PEAP protocol. LEAP's vulnerabilities might be fixable by the vendors implementing this protocol; if this is, in fact, achieved, LEAP could again become an authentication option.

8. MOBILE DEVICE SECURITY

Wireless devices have been recognized as improving the mobility of DOD infrastructures; however, they are also commonly regarded as the weakest link in WLANs. As the popularity and feasibility of wireless devices grow, so does the number of users remotely accessing DOD networks. This growth has significantly broadened network boundaries, opening the door to numerous risks and possible attacks.

To help protect against such threats, it is imperative that an added layer of security be implemented on the mobile devices that may be used to access the network. Such security measures include personal firewalls, encrypted hard drives, and software virus protection.[7] This section covers the security components required for wireless devices remotely accessing the network, including PDAs, smart phones, text-messaging devices, and laptops.

8.1 COUNTERMEASURES

Mobile devices are exposed to most threats inherent in a wireless environment. Attackers can identify and directly attack mobile devices. Because such attacks can have serious impacts, which extend beyond the device into the WLAN itself, security mechanisms must be implemented to mitigate risks. Host-based countermeasures include use of hardware and software solutions to facilitate securing a wireless environment and mitigate the risks associated with wireless networking. Software countermeasures include proper AP configuration, which consists of operational and security settings, software patches and upgrades, authentication, and IDS. Hardware solutions include access control devices such as VPNs, wireless gateways, and wireless switches.

8.1.1 Authentication

When implemented correctly, authentication solutions provide a reliable way of ensuring that network access is available to authorized users only. DOD policy requires that personal identification be given for access to the network and that authentication measures be implemented at the device level in addition to the network level.[8] Required solutions include the use of usernames and passwords (with required password characters stipulated), password expiration, and minimum password length.

8.1.2 Personal Firewalls

Personal firewalls are software-based solutions that reside on a client's machine and are either client managed or centrally managed. Client-managed versions are best suited to low-end users, because individual users are able to configure the firewall themselves

[7] DISA, *Secure Remote Computing STIG.*

[8] DOD Directive 8100.2, 4.1.1.

and may not follow specific security guidelines. Although personal firewalls offer some measure of protection, they do not protect against advanced forms of attack. Depending on the level of security required, agencies may still need additional layers of protection.

Even though personal firewalls generally must be supplemented by other protective means, they do provide added protection against rogue APs that can be easily installed in public places. Personal firewalls are now considered a requirement on all remote access devices that are accessing a DOD system.[9]

8.1.3 Encryption

Encryption software can be used to protect the confidentiality of sensitive information stored on handheld devices and mirrored on the desktop personal computer. The information on add-on backup storage modules should also be encrypted and the modules securely stored when not in use. The added security provided by encryption establishes an extra layer of defense that further protects sensitive information stored on handheld devices. Unless the data is unclassified on a publicly available web site, all data is sensitive per 8500.2 and therefore must be FIPS 140.2 validated.

8.1.4 Virus Protection

DOD policy recommends the use of anti-virus software for all handheld devices. Virus applications should enable users to perform routine automatic scanning of e-mails and data files. Each DOD entity with independent wireless security policies should ensure that all remote devices contain the most recent vendor-supported anti-virus software. This software must be configured to ensure that the user will be prompted to update the virus signatures on a continuous 14-day basis.

8.2 POLICY

According to DOD 8100.2 wireless devices shall not be used or brought into a classified environment. This policy also emphasizes that wireless devices are not to be used to store, transmit, or process information where classified information is electronically stored.

In addition, *DOD 8100.2,* Use of Commercial Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG), states—

> In Section 4.2, "Cellular/PCS and/or other Radio Frequency (RF) or Infrared (IR) wireless devices shall not be allowed into an area where classified information is discussed or processed without written approval from the DAA in consultation with the Cognizant Security Authority (CSA) Certified TEMPEST Technical Authority (CTTA)."

[9] DISA, *Secure Remote Computing STIG.*

In Section 4.3, "Wireless technologies/devices used for storing, processing, and/or transmitting information shall not be operated in areas where classified information is electronically stored, processed, or transmitted unless approved by the DAA, in consultation with the CSA CTTA. The responsible CTTA shall evaluate the equipment using risk management principles and determine the appropriate minimum separation distances and countermeasures."

In Section 4.5, "DAAs shall ensure that wireless personal area network capability is removed or physically disabled from a device unless FIPS PUB140-1/2-validated cryptographic modules are implemented…."

In Section 4.8, "PEDs that are connected directly to a DOD-wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly while directly connected."

In Section 4.9, "Anti-virus software shall be used on wireless-capable PEDs and workstations that are used to synchronize/transmit data. The network infrastructure shall update anti-virus software for all applicable PEDs and their supporting desktops from a site maintained by the Defense Information Systems Agency."

9. FUTURE CONSIDERATIONS (802.11I)

Products compliant with the IEEE 802.11i standard (ratified July 2004) are available and provide strong, standards-based Layer 2 protection for wireless networks. However, there are currently no such products that are also FIPS-140-2 certified. Once products are available with both certifications, they should be strongly considered for securing wireless networks in an unclassified environment.

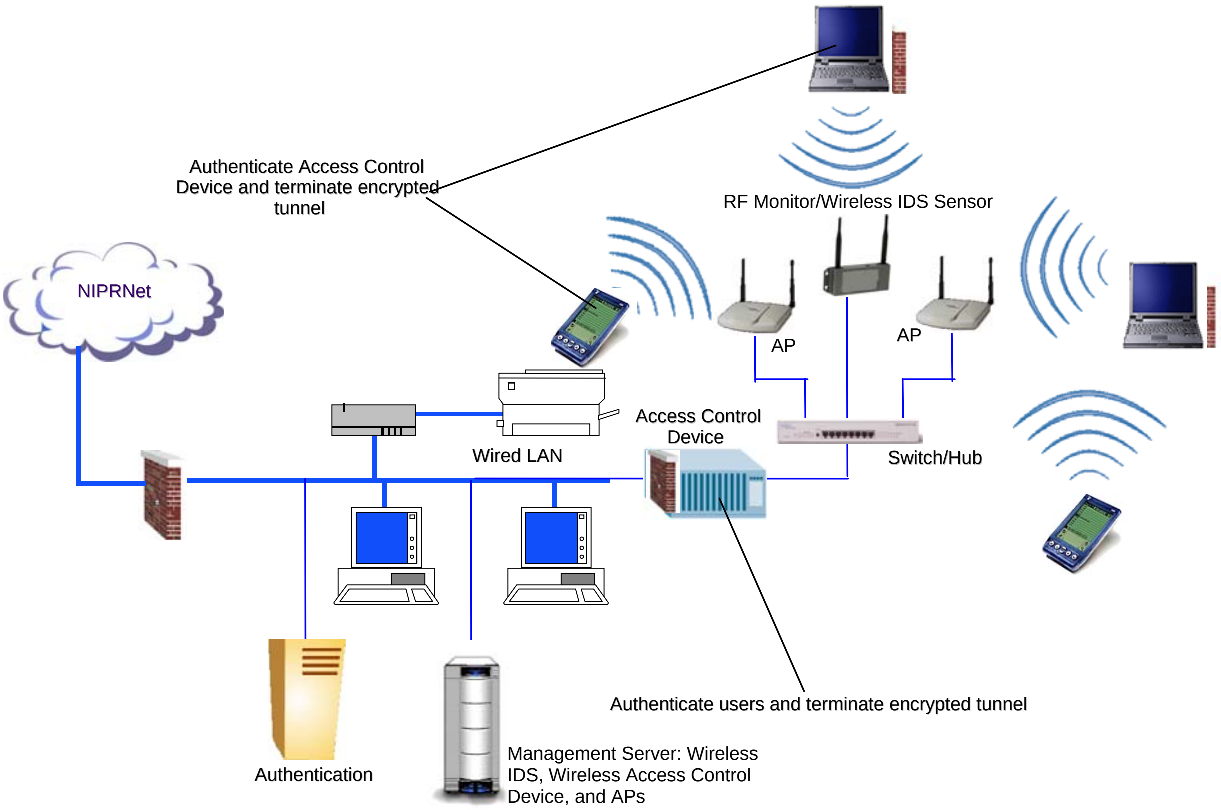
10. CASE STUDIES

Wireless networks have been implemented in various DOD settings to increase user mobility and productivity. This section provides case studies (i.e., descriptions of specific implementations) based on survey data received from DOD entities, healthcare providers, and private organizations.

Although these WLAN solutions vary according to network requirements and organizational needs, the general WLAN security architectures are similar. The general implementation, shown in Figure 10-1, is similar across all solutions and has been discussed throughout the previous sections of this document.

The selection of specific WLAN security components is based on several factors, such as cost, user capacity, and the physical environment. Regardless of which components are selected, if they are implemented properly, an adequate level of security can be provided.

Figure 10-1. Generic Wireless Security Solution


Authenticate Access Control Device and terminate encrypted tunnel
RF Monitor/Wireless IDS Sensor
NIPRNet
AP
AP
Access Control Device
Switch/Hub
Wired LAN
Authenticate users and terminate encrypted tunnel
Authentication
Management Server: Wireless IDS, Wireless Access Control Device, and APs

All of the case studies described within this document include FIPS-140-2 compliant encryption components.

10.1 ORGANIZATION A: DOD MEDICAL HEALTH SERVICES

10.1.1 Overview

The healthcare market has seen a tremendous increase in the demand for patient quality assurance, ranging from accidental death prevention to elevated levels of privacy assurance. Many healthcare facilities have deployed wireless networks, providing physicians and hospital staff with remote access to patient records. This access enables real-time patient monitoring, resulting in better patient care. However, the implementation of wireless applications also has opened the door to security challenges, including intrusions and network attacks. Such attacks threaten patient privacy and underscore the urgency of the Federal Health Insurance Portability and Accountability Act (HIPAA) requirement that all hospitals implement security measures to protect patient information, including wirelessly transmitted data.

The need to guard patient records is even more critical in DOD, where patient information can also be a source of human intelligence.

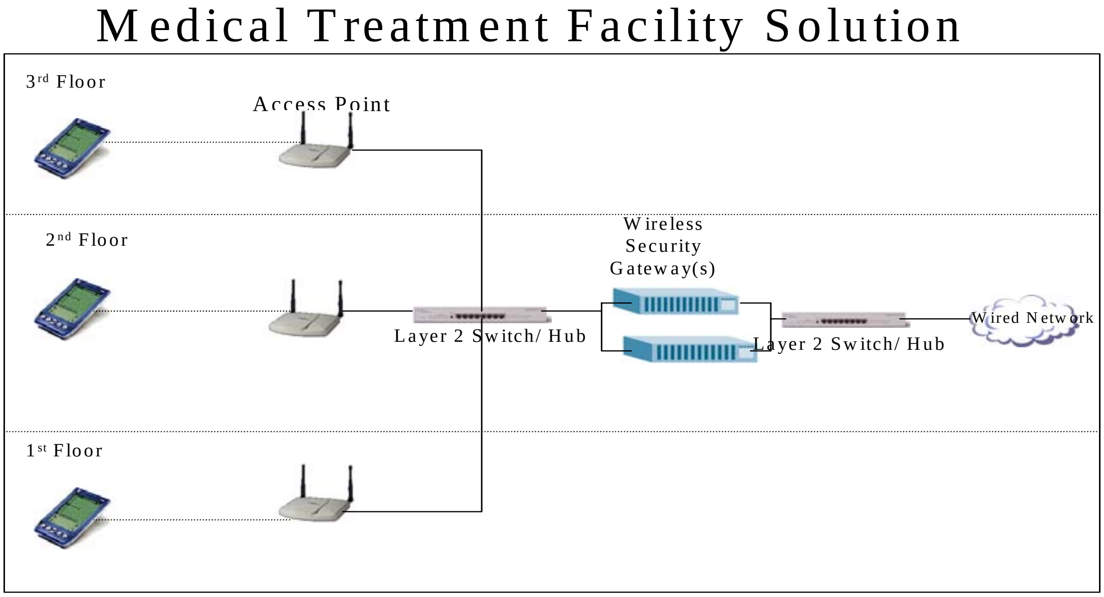
10.1.2 Solution

Within the DOD Medical Health Services unit, a strategic approach has been taken to secure the medical networks and wireless communications in various hospitals and medical centers. The security products used have been compliant with healthcare and government standards mandated by NIST and DOD.

At one treatment facility, wireless barcode scanners were used to read patient wristbands that corresponded to patient charts and medications. The barcode scanners were connected by serial ports to tablet or laptop personal computers configured with 802.11 NICs. The 802.11b APs were placed throughout the facilities and directly wired to a virtual local area network (VLAN) through a network switch/hub. Connected to the switch were two wireless security gateways, acting as a primary and a backup, which were configured to a “fail-over” mode. The two devices functioned as a bridge between the main IT network and the encrypted VLAN.

In this instance, the access control server, identified in Figure 10-2, manages device and user authentication. The control server manages the security gateways and can be tied in to future policy servers, i.e., Remote Access Dial-in User Server (RADIUS) and NT domain.

Figure 10-2. Medical Treatment Facility Solution



10.1.3 Benefits

Health services within DOD have benefited from the implementation of this secure wireless system. Physicians and hospital staff now have the ability to receive real-time information across a secure wireless network that ensures patient confidentiality.

10.2 ORGANIZATION B: SECURE COMBAT INFORMATION SYSTEM

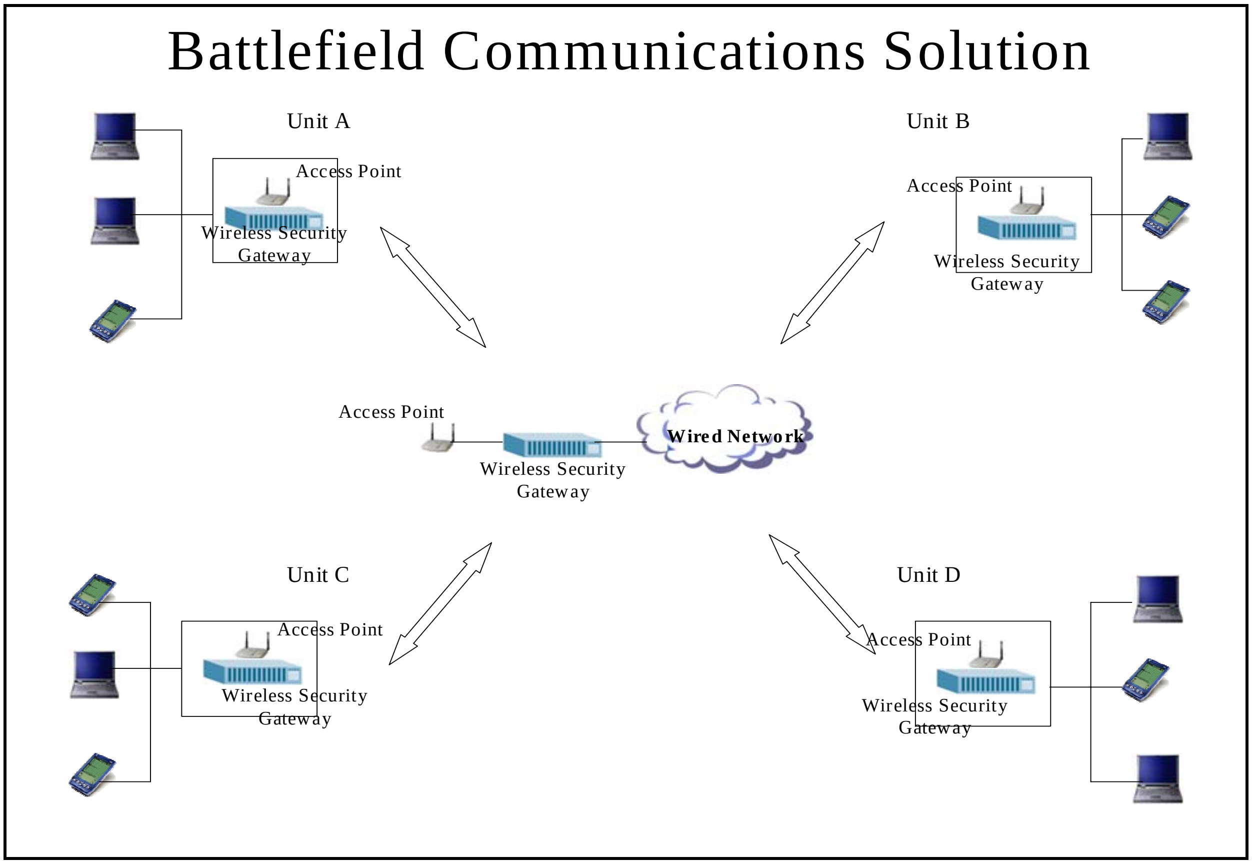
10.2.1 Overview

The military has improved its communication system by implementing wireless technology. This has reduced message travel time on the system, which benefits personnel with real-time information.

10.2.2 Solution

In this solution, FIPS-140-2 validated wireless security gateways were deployed to secure the tactical WLANs supplying military personnel with real-time information. Battlefield operations are generally outfitted with multiple tactical units, including strategically placed warehouses, command facilities, and artillery units. Each tactical unit has been outfitted with personal computers and/or wireless handheld devices that have been configured to authenticate to corresponding APs. At this point, users/devices are identified for authentication, and data packets are encrypted. The data is then passed from the gateway through an AP to a shared AP on the network side. Traffic is then routed from the network AP to a security gateway that decrypts the data on the wired network. The general outlines of this solution are displayed in Figure 10-3.

Figure 10-3. Battlefield Communications Solution


Battlefield Communications Solution
Unit A
Access Point
Wireless Security Gateway
Unit B
Access Point
Wireless Security Gateway
Access Point
Wireless Security Gateway
Wired Network
Unit C
Access Point
Wireless Security Gateway
Unit D
Access Point
Wireless Security Gateway

The security device deployed in this instance has provided a wide assortment of security and implementation features. The wireless gateway was selected mainly because of its ease of use and scalability. In this instance, the gateway also has the capability of providing three levels of authentication, including device, user, and network authentication.

Data packets traveling between the handheld devices or personal computers and the APs are WEP encrypted. Although WEP is typically used to encrypt information between wireless APs and NICs, the vulnerabilities of WEP-enabled APs are well known and recognized within DOD. Because WEP encryption algorithms have not been FIPS-140-2 validated and do not meet the minimum government policy requirements, AES algorithms have been implemented as reinforcement to encrypt the data packets traveling between the individual tactical units and the wired network by way of the wireless gateway device.

10.2.3 Benefits

By implementing a secure wireless LAN, tactical units have increased their mobility and decreased concern about physical boundaries when positioned on the battlefield. Military personnel have thus been able to eliminate the time-consuming method of using messengers to relay messages between multiple units; instead, personnel now receive real-time information.

10.3 ORGANIZATION C: ENGINEERING LOGISTICS CENTER

10.3.1 Overview

Warehouses play a vital role in military/defense processes, providing such essential services to military and civilian entities as shipment processing, packaging, and inventory maintenance. It is therefore imperative that such warehouses maintain efficient procedures to minimize inaccuracies, and that they maintain planned production levels.

Traditionally, procedures have consisted of workers' manually capturing and logging data. However, this method is cumbersome, time-consuming, and vulnerable to human error. To provide leaner, more efficient processing, warehouse management centers throughout the military have reconfigured their systems to implement secure wireless solutions; this has allowed manual operations to be replaced by automated tracking technologies.

10.3.2 Solution

Warehouse workers are now using portable data terminals (PDT) with barcode scanning capabilities to scan items that require processing within the warehouse. A client is embedded in each PDT and assigned a device ID that is registered on the wired-side access control server (ACS). Each user is assigned to only one PDT; however, a PDT can support multiple users. The WLAN server also serves as a platform for the ACS, which monitors and controls the applications supplied by the wireless gateway.

The client software (which corresponds to the wireless security gateway) encrypts the captured data, which then travels to APs strategically placed throughout the warehouse, by means of 802.11b communication. The prior solution operated at a proprietary frequency of 900 megahertz; the system has now been standardized at 2.4 gigahertz, in accordance with government policy. The APs are connected to the WLAN switches by TCP/IP communication and CAT-5 cabling. Information is routed through the wireless security gateway, with the data packets encrypted by AES 192-bit algorithms before they travel between the clients (APs) and the gateway. The data is decrypted once it reaches its destination.

10.3.3 Benefits

The use of bar-coding and wireless collection terminals has increased productivity and decreased errors incurred in logging information. Ideally, this mechanism will be implemented throughout the warehouses in DOD. This would represent a beneficial, high-impact implementation of emerging wireless technologies to enhance production levels and significantly cut costs.

10.4 ORGANIZATION D: DEFENSE COMMISSARY AGENCY

10.4.1 Overview

The Defense Commissary Agency manages more than 200 stores and distribution centers worldwide and has been using wireless technologies for some time. The need for increased attention to security protocols for these technologies became evident when hackers began penetrating the firewalls and compromising the DOD network. By penetrating the system, hackers were able to view patrons' sensitive information, such as credit card data, addresses, and driver's license information. During this time, WEP encryption was used to encrypt data traveling between the client and the APs. Since then, WEP has been judged as not meeting minimum government standards and has been deemed inadequate by NIST.

10.4.2 Solution

Within the majority of its locations, the Defense Commissary Agency has begun deployment of secure wireless networks. Commissary employees are now using handheld barcode scanners equipped with client software to perform remote price checks and real-time adjustment of inventory.

APs are placed throughout each store and distribution facility. These APs correspond to handheld terminals (loaded with client software) and wireless point-of-sale registers. The APs are routed to a VLAN on the RF/secure side of the security device via CAT-5 cabling. The security device has a nonsecure connection to the store router, which operates on a separate LAN with a different IP address block. The wired portion of the store is connected to a second router port and uses a different address block. Centralized management servers were implemented on the network to control store security devices at each location. The devices are identified and authenticated through each server by MAC addresses.

The current system meets all government requirements and is FIPS-validated, featuring 3DES and device authentication on the ACS.

The agencies are currently deploying a wireless IDS and centralized management technology. This system will consist of passive RF sensors tied in to the wired portion of the store network. The sensors report back to centralized management appliances.

Each user will be required to authenticate using a user ID and password before gaining access to the LAN/WAN. This added feature will be implemented with the development of a wireless edge authentication system. There also are plans to install routers at each commissary location.

10.4.3 Benefits

Because commissary employees now have access to an 802.11b secure wireless network, they are able to ensure patrons' privacy while maintaining a high level of service and production quality.

APPENDIX A. CHECKLISTS

Checklists are valuable tools in the design and engineering of new information technology systems, such as wireless local area networks (WLAN). This appendix includes three types of checklists that may be of use:

- A certification and accreditation (C&A) checklist that presents steps that are necessary for the design and implementation of a secure WLAN that is approved for use
- A series of product selection checklists that present key components that each security product used in a WLAN must support
- A WLAN Security Checklist, reproduced from the National Institute of Standards and Technology (NIST) Special Publication 800-48, that provides detailed management, technical, and operational recommendations that should be addressed in any WLAN design and implementation.

A.1 Certification, Accreditation, and Connection Approval Checklist

The following checklist presents the steps that must be taken during the design and implementation of a WLAN to achieve a secure system that is approved for use.

Certification, Accreditation & Connection Approval Process	
Use DOD Instruction 5200.40, DITSCAP, December 1997; DOD 8510.1-M, DITSCAP Application Manual, July 31, 2000; and this checklist when implementing a new system using wireless solutions or when implementing wireless solutions to a previously certified system. http://iase.disa.mil/ditscap/ditsdocuments.html	
1. Identify the following personnel: • Designated Approving (Accrediting) Authority • Certification Authority (CA) • User Representative • Information Assurance Officer (IAO)	
2. Develop a security policy	
3. Determine accreditation goals and objectives A. Determine security mode of operation 1. Determine data sensitivity and classification levels 2. Determine user clearance levels 3. Determine user authorizations B. Determine the accreditation boundary (what is being reviewed, certified, and accredited) C. Determine which mission assurance category the system falls within (see DOD Instruction 8500.2, February 2003)	
4. Define the proposed operational environment and how the system will be used	
5. Develop a CONOPS for the system	
6. Develop architecture and design documents, including system specifications	
7. Develop administrator and user manuals	
8. Develop operating procedures	

Certification, Accreditation & Connection Approval Process	
9. Develop network diagrams	
10. Develop configuration management documents	
11. Develop a security incident handling process and procedures	
12. Complete DOD 8510.1-M, Appendix 2 checklists • Complete system architecture analysis • Complete software, hardware, and firmware design analysis • Complete Network Connection Rule compliance analysis • Complete integrity analysis of integrated products • Complete system design document • Complete life-cycle management analysis • Complete vulnerability assessment • Complete ST&E checklist • Conduct penetration testing • Determine COMSEC protective measures • Conduct system management analysis • Perform a site accreditation survey • Evaluate the contingency plan • Conduct risk management review	
13. Develop/update the SSAA and appendices in accordance with DOD 5200.40	
14. Test the wireless network's • Connection to end-user devices, access points, and connection to other systems • Compliance with wireless security checklist requirements • Compliance with wireless STIG requirements	
15. Document results of test, including vulnerabilities	
16. Finalize SSAA and appendices	
17. Submit SSAA to DAA for approval	
18. Modify the security policy as appropriate	
19. Submit for NIPRNet connection A. Contact the NIPRNet Product Manager or the NIPRNet Customer Service Representative to obtain information regarding the NIPRNet and procedures for connection to the network. Questions regarding the CAP and waiver process should be directed to the NIPRNet CAP Manager. Points of contact: NIPRNet Product Manager (C) (703) 882-0158, (D) 381-0158 brewera@ncr.disa.mil NIPRNet Customer Service Representative (C) (703) 882-0159, (D) 381-0159 ncgoughb@ncr.disa.mil NIPRNet CAP Manager (C) (703) 882-0133, (D) 381-0133 o'haram@ncr.disa.mil B. Access the CAP Web site, located at http://cap.nipr.mil/index.cfm, and click YES for Agreement to Monitor. C. Select CAP Registration, which will take you to http://cap.nipr.mil/capweb/cap_insert/capformpage1.cfm D. Select "Submit a new CAP" E. Register the user with the Network Information Center and identify his or her point of contact (POC) for Domain Name Service at the NIC Web page: http://www.nic.mil or call 1-800-365-3642/703-676-1051.	

A.2 Product Selection Checklists

The following checklists include key components that each of the security products used in a WLAN must support. These checklists, initially presented in Section 4 of this framework, are consolidated here for clarity and convenience.

Wireless Client Features/Configuration	Required	Recommended
Ensure Common Criteria certification against any existing protection profiles	✓	
Ensure compliance with applicable STIGs (e.g., operating system, applications)	✓	
Ensure that wireless NIC is 128-bit WEP/WPA capable.		✓
Ensure that wireless NIC is IEEE 802.1x and/or 802.11i capable (if available).		✓
Use encryption client software (FIPS-140-2 certified) for storage and communication security.	✓	
Employ personal firewall	✓	
Employ intrusion detection system (IDS)		✓
Use virus protection	✓	
Ensure that file/printer sharing disabled.	✓	

Access Point Features/Configuration	Required	Recommended
Common Criteria certified against any existing protection profiles	✓	
128-bit WEP/WPA capability		✓
SSID beacon mode disabled		✓
Pseudo-random SSID, preferably compliant with DOD network password rules		✓
HTTP/SNMP management access disabled; ensure that only secure management access is available (e.g., SSH).		✓
Transmission power set to lowest possible setting that will meet required signal strength for the service area	✓	
802.11i security capability		✓

RF Monitor Features/Configuration	Required	Recommended
IEEE 802.11 signal detection	✓	
Continuous scanning capability	✓	
Attack signature recognition (updatable)	✓	
Rogue access point/client detection	✓	
MAC address ACL verification	✓	
Audit logging capability	✓	
Real-time alert mechanism (e-mail, pager, etc.)	✓	
Integration with centralized monitoring and management systems		✓
Network health verification (e.g., interference, slow performance)		✓
Common Criteria certified against any existing protection profiles	✓	

Access Control Device Features/Configuration	Required	Recommended
Common Criteria certified against any existing protection profiles	✓	
Network access control (e.g., integrated firewall)	✓	
Authentication functionality	✓	
Encrypted tunneling capability (FIPS-140-2 certified)	✓	
Audit logging capability	✓	
Session time-out set to 15 minutes or less (per local security policy)		✓

A.3 NIST Special Publication 800-40 Wireless LAN Security Checklist

The following Wireless LAN Security Checklist, from the NIST Special Publication 800-48, provides users and implementers with detailed management, technical, and operational recommendations that should be addressed as a part of any WLAN design and implementation.

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Ensure that the client NIC and access point support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue access points do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8.	Complete a site survey to measure and establish the access point coverage for the agency.	✓		
9.	Take a complete inventory of all access points and 802.11 wireless devices.	✓		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	✓		
11.	Locate access points on the interior of buildings instead of near exterior walls and windows as appropriate.	✓		
12.	Place access points in secured areas to prevent unauthorized physical access and user manipulation.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Technical Recommendations				
13.	Empirically test access point range boundaries to determine the precise extent of the wireless coverage.	✓		
14.	Make sure that access points are turned off when they are not being used (e.g., after hours and on weekends).	✓		
15.	Make sure that the reset function on access points is being used only when needed and is invoked only by an authorized group of people.	✓		
16.	Restore the access points to the latest security settings when the reset functions are used.	✓		
17.	Change the default SSID in the access points.	✓		
18.	Disable the broadcast SSID feature so that the client SSID must match that of the access point.		✓	
19.	Validate that the SSID character string does not reflect the agency’s name (division, department, street, etc.) or products.	✓		
20.	Ensure that access point channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
21.	Understand and make sure that all default parameters are changed.	✓		
22.	Disable all insecure and nonessential management protocols on the access points.	✓		
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WPA, AES encryption feature.	✓		
24.	Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (access point or hub to access points).	✓		
27.	Install anti-virus software on all wireless clients. http://www.cert.mil/antivirus/av_info.htm	✓		
28.	Install personal firewall software on all wireless clients.	✓		
29.	Disable file sharing on wireless clients (especially in untrusted environments).	✓		
30.	Deploy MAC access control lists.		✓	
31.	Consider installation of Layer 2 switches in lieu of hubs for access point connectivity.	✓		
32.	Deploy IPsec-based VPN technology for wireless communications.	✓		
33.	Ensure that the encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	✓		
34.	Fully test and deploy software patches and upgrades on a regular basis.	✓		
35.	Ensure that all access points have strong administrative passwords.	✓		
36.	Ensure that all passwords are being changed regularly.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		✓	
38.	Ensure that the “ad hoc mode” for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.	✓		
39.	Use static IP addressing on the network.		✓	
40.	Disable Dynamic Host Configuration Protocol (DHCP).		✓	
41.	Enable user authentication mechanisms for the management interfaces of the access point.	✓		
42.	Ensure that management traffic destined for access points is on a dedicated wired subnet.	✓		
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of access points.	✓		
Operational Recommendations				
44.	Configure SNMP settings on access points for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	✓		
45.	Enhance access point management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	✓		
46.	Use a local serial port interface for access point configuration to minimize the exposure of sensitive management information.		✓	
47.	Consider other forms of authentication for the wireless network, such as RADIUS and Kerberos.		✓	
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		✓	
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
51.	Enable use of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.	✓		
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
53.	Designate an individual to track the progress of 802.11 security products and standards (Internet Engineering Task Force [IETF], IEEE, etc.) and the threats and vulnerabilities with the technology.		✓	
54.	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		✓	
55.	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	✓		
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	✓		

APPENDIX B. ACRONYMS

3DES	Triple Data Encryption Standard
ACL	Access Control List
ACS	Access Control Server
AES	Advanced Encryption Standard
AP	Access Point
C&A	Certification and Accreditation
CA	Certificate Authority
CAC	Common Access Card
CAP	Connection Approval Process
CBC	Cipher Block Chaining
CCMP	Counter-Mode CBC MAC Protocol
CCRA	Common Criteria Recognition
CIO	Chief Information Officer
COMSEC	Communications Security
CONOPS	Concept of Operations
CSA	Cognizant Security Authority
CTTA	Certified TEMPEST Technical Authority
DAA	Designated Approving Authority
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DOD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EVP	
FIPS	Federal Information Processing Standards
GHz	Gigahertz
GIG	Global Information Grid
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol, Secure
I&A	Identification and Authentication
IA	Information Assurance
IAO	Information Assurance Officer
IAVA	Information Assurance Vulnerability Alert
ID	Identifier
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Secure Internet Protocol
IR	Infrared
IS	Information System
IT	Information Technology
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control or Message Authentication Code
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIPRNet	Unclassified But Sensitive Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OS	Operating System
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PDT	Portable Data Terminal
PEAP	Protected Extensible Authentication Protocol
PED	Portable Electronic Device
PIN	Personal Identification Number
PK	Public Key
PKE	Public Key Enabling
PKI	Public Key Infrastructure
POC	Point of Contact
PUB	Publication
RADIUS	Remote Access Dial-in User Service
RAS	Remote Access Service
RF	Radio Frequency
RSN	Robust Secure Network
SIPRNet	Secret Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SSAA	System Security Authorization Agreement
SSH	Secure Shell
SSL	Secure Sockets Layer
SSID	Service Set Identifier
ST	Security Target
ST&E	Security Test and Evaluation
STIG	Security Technical Implementation Guide
SWLAN	Secure Wireless Local Area Network

TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
U.S.C.	U.S. Code
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WEP	Wired Equivalent Protocol
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access
WRAS	Wireless Remote Access Service