State of Kansas

Interim
Wireless Local Area Networks
Security and Technical
Architecture

October 6, 2005

Prepared for

Wireless Policy Committee

Prepared by

Results
TECHNOLOGIES GROUP

Revision Log

DATE	Version	Change Description	Author
10/06/05	1.1	Initial Draft	RTG Consulting
04/27/06		Approved by ITEC as part of the WLAN Policy 7500	

Table of Contents

WLAN Security 1
Wireless Security Goals 1
WLAN Security Mechanisms 1
Securing the Control Channel and User Channel between the Access Point and the Access Controller 2
802.11i Authentication and Encryption 3
802.1x Port-based Authentication 3
The 802.1x Authentication Process 5
WLAN Authentication 6
Access to Business Class Networks 6
Access to Guest Networks 7
Login Procedure for Guest Access 7
WLAN Intrusion Protection 8
Wireless Security Threats 8
Detection, Classification and Protection 8
Wireless Intrusion Protections 9

WLAN Security

WLANs allow greater flexibility and portability than wired local area networks (LAN). With the advent of inexpensive WLAN access points and routers designed for small and home office use, wireless users can roam from office environments within secure enterprise environments to public Internet access areas, to their own home wireless network.

WLANs offer four primary benefits:

- **User Mobility** - Users can access files, network resources, and the Internet without having to physically connect to the network with wires. Users can be mobile yet retain high-speed, real-time access to the enterprise LAN.
- **Rapid Installation** - The time required for installation is reduced because network connections can be made without moving or adding wires, or pulling them through walls or ceilings, or making modifications to the infrastructure cable plant.
- **Flexibility** - WLANs can be installed and removed in locations as necessary. Users can quickly install a small WLAN for temporary needs such as a conference, trade show, or standards meeting.
- **Scalability** - WLAN network topologies can easily be configured to meet specific business needs and can scale from small networks to very large networks that enable roaming over a broad area.

However, with the advantages that wireless technology brings to the State of Kansas, it also brings inherent security vulnerabilities. Wireless networks are attractive targets for all types of unauthorized access attempts. From casual users looking for free access to the Internet, to malicious intruders looking to gain unauthorized access to confidential information on wireless clients and State owned applications, robust security mechanisms are needed to protect the information assets of the State.

Wireless Security Goals

The three basic security services defined by IEEE for the WLAN environment are as follows:

- **Confidentiality –** only authorized user have access to the network. The network should provide protection against unauthorized users, security threats, disclosure of sensitive information, intruders masquerading as authorized users.
- **Integrity** - ensure that messages are not modified in transit between the wireless clients and the access point in an active attack. “Is the data coming into or exiting the network trustworthy—has it been tampered with?”
- **Availability** – ensure that the wireless network and the resources accessed by authorized users are available when needed. Protection against attacks and intruders that can initiate denial of service attacks, and other threats that affect network availability.

WLAN Security Mechanisms

To meet the stated security goals of confidentiality, integrity, and availability, the State of Kansas will implement the current state of the art security mechanisms for wireless local area networks, including 802.11i authentication and encryption.. Security mechanisms will be deployed in the wireless local area network in the following areas:

- Security of the Control Channel and User Channel between Access Points and the Access Controller

- Secure authentication of the wireless user to the network with 802.11i authentication and encryption when accessing State agency networks
- Captive Portal authentication for Guest Access
- Segregation of wireless network traffic in the wired network through Virtual LANs
- Intrusion Protection – preventing unauthorized users and access points from connecting to the network or intercepting wireless transmission of authorized users.
- Single sign-on capability leveraging existing authentication databases

Securing the Control Channel and User Channel between the Access Point and the Access Controller

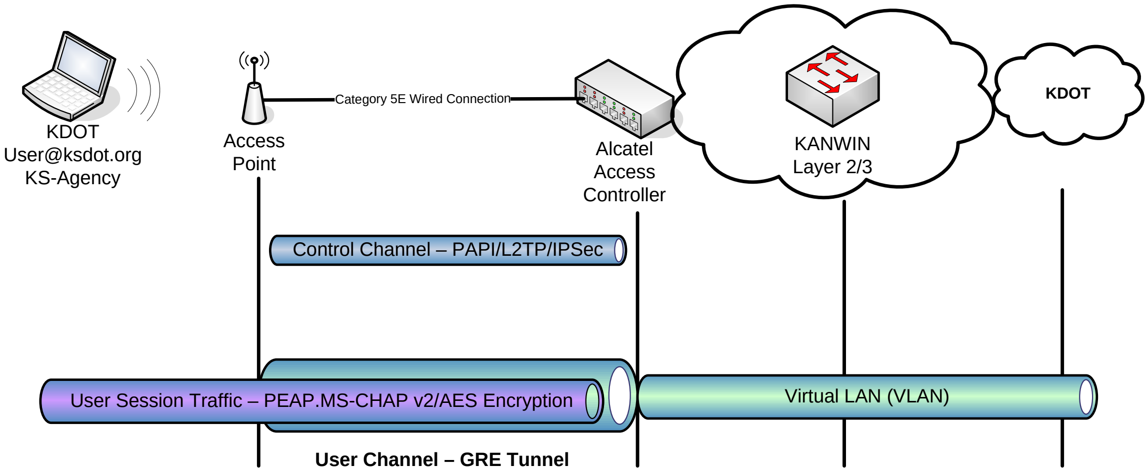
KDOT
User@ksdot.org
KS-Agency
Access Point
Category 5E Wired Connection
Alcatel Access Controller
KANWIN Layer 2/3
KDOT
Control Channel – PAPI/L2TP/IPSec
User Session Traffic – PEAP.MS-CHAP v2/AES Encryption
Virtual LAN (VLAN)
User Channel – GRE Tunnel

Figure 1 - Control Channel and User Channel Security

When securing WLAN traffic in the State network, two distinct communications channels must be secured:

- The Control Channel: the control channel provides the communications path between the Access Point and the Access Controller for management and control traffic. Configuration information and management information passed between the Access Point and Access Controller is transported over the Control Channel.

  Alcatel uses a combination of proprietary and standards based protocols to secure the control channel. Propriety Access Protocol Interface (PAPI) between the Access Controller and the Access Point. PAPI is encapsulated in L2TP over IPsec.

- The User Channel: User session traffic is carried over the User Channel. The user channel is secured by encapsulating data packets in an IP Generic Routed Encapsulation (GRE) tunnel. The user channel is secured from the wireless user all the way to the access controller by default. The encryption of all wireless traffic is terminated and managed by dedicated Crypto hardware. All 802.11 packets from wireless users are encapsulated in the tunnel by the AP and sent to the Access Controller, providing a separation of user wireless traffic from control channel traffic.

802.11i Authentication and Encryption

Also known as WPA2, 802.11i is a newly ratified standard that replaces the existing static WEP encryption technology, which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The 802.11i architecture contains the following components:

- **802.1X port-based authentication,** which provides authentication to devices attached to a LAN port. 802.1x authentication establishes a point-to-point connection, preventing access from that port if authentication fails. 802.1x is based on the EAP, Extensible Authentication Protocol. Several EAP-types can be used including EAP-TLS, EAP-TTLS, and protected EAP (PEAP).
- **Robust Security Network (RSN):** RSN improves upon WiFi Protected Access by replacing the key rotation of Temporal Key Integrity Protocol with the more secure Advanced Encryption Standard (AES).
- **AES encryption** to provide confidentiality, integrity and origin authentication. AES encryption is the strongest encryption available for non-military applications. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. AES is also referred to as FIPS-197 by the National Institute of Standards and Technology (NIST).

The 802.11i standard allows AES encryption to be implemented in software, so adapter cards, clients and APs can support AES through new drivers or firmware. **Be aware that many older wireless clients, in particular PDAs, may not have the necessary processing power to support AES encryption.** Implementation of 802.11i will require existing users to upgrade older hardware that does not support 802.11i. WPA2 is backward compatible with WPA.

Windows Operating Systems Requirements for 802.11i

Microsoft Windows XP, Service Pack 2 support 802.11i authentication and encryption. Users who have XP service pack 1 installed may also upgrade to support 802.11i, with the wireless rollup update. Microsoft also provides 802.1X clients for Windows 2000, service pack 3, through updates.

Microsoft support for 802.11i using Windows 9x and NT 4.0 is limited. Users of older equipment and Windows operating systems may require the installation of a third party client such as Funk Software’s Odyssey client, or install a wireless NIC supporting 802.11i.

Users of personal digital assistants may also require the installation of a third party clients to support 802.11i.

802.1x Port-based Authentication

Authenticator

An authenticator is a LAN port that enforces authentication before access is allowed on the network. In the Kansas State WLAN, the Alcatel Access Controller serves the role of the authenticator.

Supplicant

The supplicant is the LAN port that requests access to the network. In the wireless network environment, the supplicant is the logical LAN port on the wireless network interface adapter, in conjunction with the software client. The supplicant can be provided by the laptop or PDA vendor, or may be a third party supplicant (client) that can be used to augment functionality for older devices. Funk software's Odyssey client is an example of a third party 802.1x supplicant.

Authentication Server

The authentication server verifies the security credentials of the supplicant, which are passed to it by the authenticator. In the State of Kansas WLAN, the authentication server function will be provided by RADIUS servers. For agencies that are Microsoft Windows based, RADIUS functionality can be provided by Windows Server 2000 or 2003 platforms using the Internet Authentication Service (IAS) feature. For agencies that are Novell based, RADIUS, the recommended RADIUS platform is Funk's Steel Belted RADIUS or Odyssey server platforms.

Extensible Authentication Protocol (EAP)

The 802.1x standard specifies the use of Extensible Authentication Protocol (EAP) as the standard authentication mechanism. EAP provides flexibility in the implementation of 802.1x by supporting several EAP types including EAP-TLS, EAP-TTLS, and PEAP. EAP protocols allow for an open ended exchange of authentication messages between the access client (supplicant) and the access server (authenticator).

A security vulnerability of EAP, however, is that the authentication exchange, unless specifically protected, is passed in clear text. EAP-TLS and EAP-TTLS provide encrypted protection of the EAP exchange, but require certificates be installed on the access client and the access server. PEAP (protected EAP), also encrypts the EAP exchange, via TLS, but requires a certificate on the access server only. No client software is required on the client devices.

PEAP

The State of Kansas will deploy 802.1x port based authentication using protected EAP (PEAP) with MS-CHAPv2.

PEAP authentication protects MS-CHAPv2 in a two stage process:

1. An initial EAP exchange establishes an encrypted Transport Layer Security (TLS) tunnel between the wireless client (supplicant) and the authenticator (Access Controller).
2. After the TLS tunnel is established, a second EAP exchange, using MS-CHAPv2 mutually authenticates the wireless client to the network.

   MS-CHAP v2 is a password-based, challenge-response, mutual authentication protocol that uses the Message Digest 4 (MD4) and Data Encryption Standard (DES) algorithms to encrypt responses. Without PEAP MS-CHAPv2 is susceptible to offline dictionary attacks that could determine the challenge-response handshake parameters. As part of that exchange, the wireless client authenticates the certificate of the authenticator (RADIUS) server.

The 802.1x Authentication Process

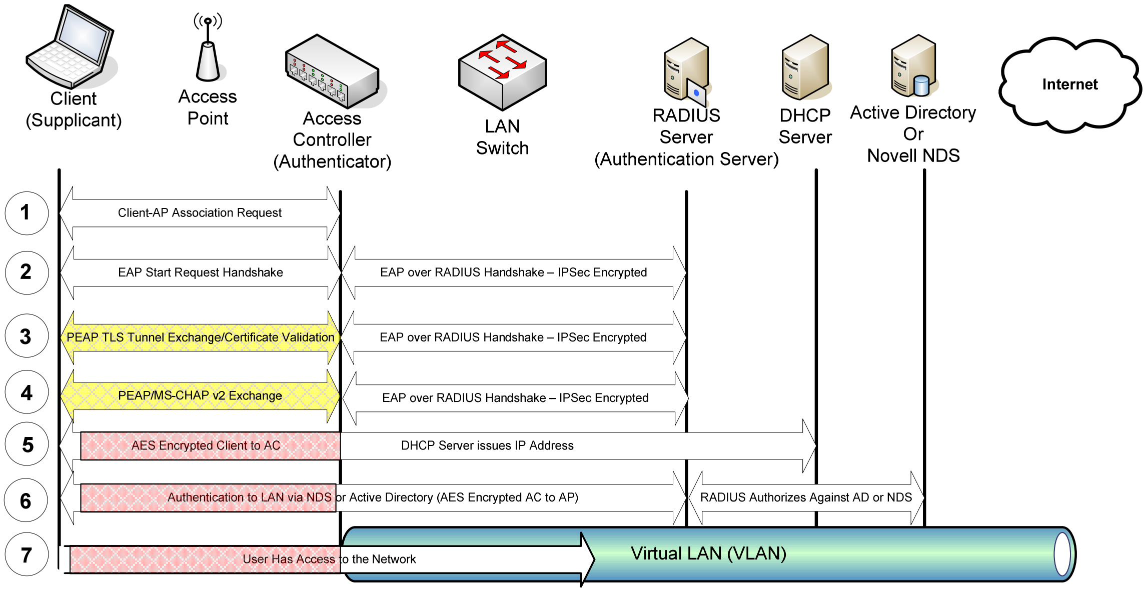
Client
(Supplicant)
Access
Point
Access
Controller
(Authenticator)
LAN
Switch
RADIUS
Server
(Authentication Server)
DHCP
Server
Active Directory
Or
Novell NDS
Internet
1
Client-AP Association Request
2
EAP Start Request Handshake
EAP over RADIUS Handshake – IPSec Encrypted
3
PEAP TLS Tunnel Exchange/Certificate Validation
EAP over RADIUS Handshake – IPSec Encrypted
4
PEAP/MS-CHAP v2 Exchange
EAP over RADIUS Handshake – IPSec Encrypted
5
AES Encrypted Client to AC
DHCP Server issues IP Address
6
Authentication to LAN via NDS or Active Directory (AES Encrypted AC to AP)
RADIUS Authorizes Against AD or NDS
7
User Has Access to the Network
Virtual LAN (VLAN)

Figure 2 - 802.11i Security

1. The client sends a request for association to the AP. Association 4-way handshake sequence completes.
2. EAP Negotiation. The client sends a request for security negotiations to the Access Controller via the AP. The Access Controller then forwards the request to the RADIUS server for authentication. Upon successful negotiation, a TLS connection is established.
3. PEAP Negotiation. Client initiates TLS tunnel with the RADIUS server. RADIUS certificate is validated by the client.
4. PEAP/MS-CHAP v2 negotiation. The client and AC negotiate MS-CHAP v2 handshaking encrypted by TLS. **802.1x authentication is complete**.
5. A DHCP request for an IP address is issued by the client. The DHCP server issues the IP address.
6. Logon request is authenticated and authorized via RADIUS, RADIUS validates the request with Microsoft Active Directory or Novell NDS. User role, including VLAN assignment is granted by RADIUS.
7. User has access to the internal network through assigned VLAN.

WLAN Authentication

Two logical wireless local area networks will be established for use by the State of Kansas.

- Business Class Network – using the service set identifier (SSID) KS-Agency, will be available to State employees, legislators and other authorized users. Users of the Business Class Network must be authorized at the Agency level in conformance with State and Agency security policy.
- Guest Network – using the KS-Guest SSID, will provide WLAN access to vendors, lobbyists, and other visitors who have a business need to access the Internet. Guest users will provide minimal identification to hosting agencies for access.

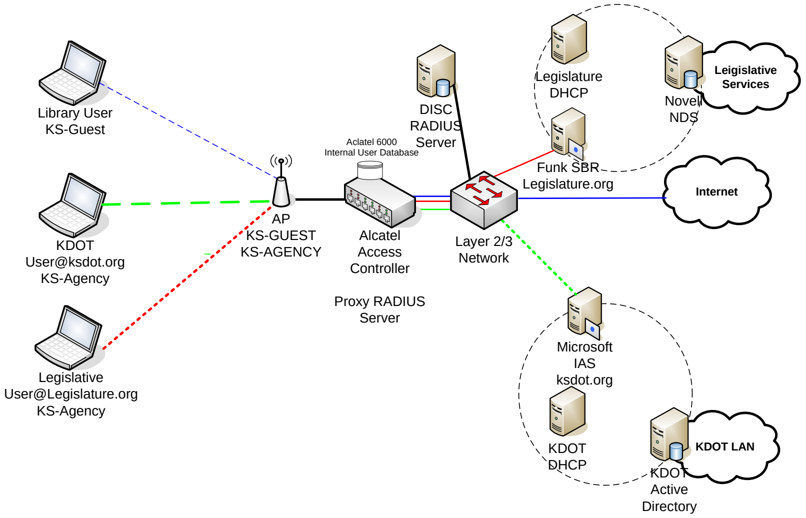

Figure 3 - RADIUS Authentication for Business Class Networks

Access to Business Class Networks

Access to the enterprise WLAN for the State of Kansas will be authenticated via RADIUS servers and proxy RADIUS to identify the user by agency, and direct the authentication request to the appropriate authentication server. The authentication process will work as follows:

1. After associating with the KS-Agency SSID, and authenticating at Layer 2 via 802.1x, the user will be presented with a login screen, prompting them to enter their user id and password. The format of the user id is the user name appended with the domain name of the agency.

   For example:

   KDOT User: username@ksdot.org
   Legislative User: username@las.state.ks.us

2. The request is passed to the Alcatel Access controller which is configured as a RADIUS client with proxy RADIUS capabilities. The RADIUS client on the Alcatel access forwards all requests to the appropriate RADIUS server.

   KDOT requests are forwarded to the KDOT RADIUS server

Legislative requests are forwarded to the Legislative Services RADIUS server

3. The Agency RADIUS server processes the logon request and passes the user id and password to the Agency's user authentication database; Microsoft Active Directory in the KDOT example, and Novell NDS in the Legislative Services example.

4. The user authentication database (Active Directory or Novell NDS) authenticates the user and the request is passed back to the Agency's RADIUS server.

5. The Agency RADIUS server assigns the user to an Agency user role (i.e. KDOT or LAS) that is also defined in the Alcatel access controller. The Agency user role assigns the user session to the appropriate VLAN and assigns an IP address via the Agency's DHCP server to the session and the user's laptop computer.

6. The user now has access to the Agency (KDOT or Legislative Services) network and the Internet.

Access to Guest Networks

Per State WLAN policy, "Guest" users are defined as visitors (vendors, lobbyists, citizens) to the State Capitol or State office buildings that need to access the WLAN in order to conduct business with the State.

- All Guest users will be required to identify themselves to the hosting agencies and be granted access to the WLAN Guest network (KS-Guest SSID).
- Hosting agencies will then grant access to the network through Guest user ids and passwords. Requirements may vary by agency or be centrally mandated by DISC. User ids and passwords may be stored on the internal user database of the Alcatel Access controller, or may be located on an external user database, centrally controlled by DISC or controlled at the Agency level.

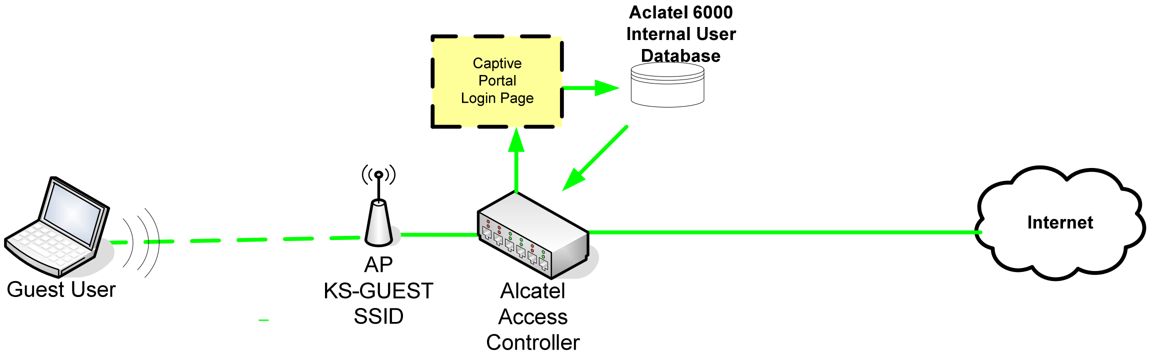

Figure 4 - Guest Access Login Procedure

Login Procedure for Guest Access

Guest access will not be secured by 802.11i authentication and encryption. Once authenticated by the Captive Portal, network traffic is open and unsecured. The Guest login sequence follows:

1. The Guest User associates with the KS-Guest SSID.
2. The user opens a web browser.
3. The browser request for the user's home page is redirected to the Captive Portal screen configured in the Alcatel controller.
4. The user is requested by the Captive Portal screen to read and agree to the Acceptable User policy and enter id in one of two modes.

   a. User email address
   b. Guest User id and password provided by the hosting agency.
5. The user id is authenticated by the internal user database of the Alcatel Access Controller.
6. The web page is redirected to the user's home page on their browser.
7. Access to the Internet is now available.

WLAN Intrusion Protection

Wireless Security Threats

WLANs allow greater flexibility and portability than wired local area networks (LAN). With the advent of inexpensive WLAN access points and routers designed for small and home office use, wireless users can roam from office environments within secure enterprise environments to public Internet access areas, to their own home wireless network.

However, those advantages are accompanied by increased security threats. The traditional definitions of perimeter security no longer apply when wireless networks are integrated into existing enterprise networks. The State WLAN will be an attractive target for unauthorized access attempts which can take the following forms:

- **Probing** – tools that allow attackers to discover network resources (APs, SSIDS, etc). The first step in launching an attack.
- **Surveillance** – tools that record network traffic, allowing attackers to gain needed information about users and the network including user ids, passwords, and other sensitive information.
- **Impersonation** – using the information gathered by probing and surveillance tools, attackers set up wireless clients or unauthorized access points with the identity of valid users and access points to gain access to the network, or gather additional information about authorized wireless users.
- **Rogue Access Points** – Unauthorized access points that connect to the network. Typically installed by employees to ports in the wired networks, allowing non-secure connections into the networks.
- **Denial of Service (DoS) Attacks -** that prevent or inhibit authorized users from accessing the network. DoS attacks can block network access completely or severely degrade network performance and client system performance.
- **Ad Hoc Networks** (peer-to-peer wireless networks) – allow one wireless laptop computer (or other device) to communicate directly with another laptop computer without connecting to the WLAN network. Non-secure Ad Hoc networks can provide unauthorized access to sensitive information on laptop computes and unauthorized access into the WLAN network through an Ad Hoc laptop that is authorized to access the WLAN.
- **Client Intrusion –** an attack on an authorized wireless client (laptop or PDA) in order to gain access to the WLAN network.
- **Network Intrusion –** an attack launched against the network using exposed vulnerabilities in order to gain unauthorized access to the network.

Detection, Classification and Protection

To mitigate these threats, the State of Kansas will implement the Wireless Intrusion Protection (WIP) features of the Alcatel WLAN platform. The WIP module is a software module that configures Alcatel Access Points as Air Monitors (AMs). The WIP module performs the following monitoring and mitigation tasks.

- Intrusion Detection – The potential rogue device or intrusion is detected
- Intrusion Classification – the device or threat is classified as dangerous or benign
- Intrusion Protection – Based on the classification, the threat is contained by block or disconnecting wireless associations with devices that are launching the attacks.

  The Alcatel intrusion protection system has the ability to dynamically shut down or contain many intrusion attempts dynamically based on pre-configured security policies. Other threats result in alerts being generated to the network administrators for further action. .

Wireless Intrusion Protections

The Alcatel Access controller provides the following intrusion protection capabilities for the threats previously listed:

- **Rogue Access Points** – the system has the ability to identify rogue access points and prevent them from connecting to the network. The system can also prevent authorized users from associating with rouge access points.
- **Denial of Service –** the system can detect rate analysis DoS attacks and Fake AP attacks
- **Network Intrusion –** the system can detect and prevent Man-in-the-Middle attacks, MAC spoofing, station disconnection (de-associate), EAP Handshake analysis, sequence number analysis, AP impersonation, signature detection, and Ad hoc network detection intrusions and vulnerabilities.
- **Mis-configured Devices** – the system can detect mis-configured APs and wireless clients that pose security vulnerabilities to the network. These include weak encryption configuration, and wireless bridging on wireless clients.
- **Impersonation** – the system can detect the presence of Honeypot APs that are impersonating authorized access points, and can verify the identification of network interface cards by organizationally unique identifiers (OUIs) that validate the identity of a network interface card by the manufacturer.

When these threats are detected by the IPS, the system can based on pre-configured policy, shut down the intrusion attempt, and/or prevent the rogue AP, or offending client from associating with the State WLANs.