

BlueSecure™ Wireless IDS (WIDS)

The BlueSecure™ WIDS is integrated into the BlueSecure Access Points and is used to find and contain Rogue APs and a host of WLAN® DoS and spoofing attacks that threaten the security of your network.

As with the BlueSecure Access Point, the BlueSecure WIDS works in conjunction with vWLAN® and Bluesocket Controllers to provide wireless intrusion detection for enterprises.

Dual-Radio, Multi-purpose 802.11 a/b/g/n Radios

The BlueSecure WIDS uses the BlueSecure AP's dual-band radios supporting 802.11 a/b/g/n in a plenum-rated housing with fixed omni-directional antennas. They support 802.3af Power over Ethernet (PoE) for operation without available AC power.

Zero Touch, Plug-and-Play Deployment

BlueSecure WIDS is completely plug-and-play, requiring no manual configuration. The WIDS can be directly attached to any existing Ethernet switch or IP router, and across any subnet boundary. Once connected, BlueSecure WIDS associate to a vWLAN® appliance or BlueSecure Controller, which automatically configures each BlueSecure WIDS based on the configuration set by the administrator. Network administrators can configure and manage multiple WIDS deployments from a central location.

Low Bandwidth Requirements on the Uplink

The BlueSecure WIDS contains an analysis engine which pre-processes wireless data before it sends it to the controller thereby minimizing the uplink bandwidth requirement. The analyzed data is also sent on a secure channel between the WIDS and the vWLAN® appliance or BlueSecure Controller.

Rogue Containment

The Bluesecure WIDS performs rogue containment not only on rogue APs, but also on rogue stations. Stations can be added to a white list to prevent authorized clients from being contained.

RF Alarm Definitions

The BlueSecure™ WIDS detects over 52 RF alerts in the system, which helps customers understand the state of their wireless network and also inform them of potential threats to their network.

Alarm Type

Adhoc SSID same as AP

AirJack Attack

Airsnarf Attack

AP Broadcasting Multiple SSID

AP Channel Change

AP Denied Association

AP Denied Authentication

AP Down

AP in WDS Mode

AP Low Signal Strength

AP Overloaded

AP Restarted

Description

A mobile station in Adhoc mode is using an approved AP SSID.

Airjack is a toolset that allows attackers to inject fake 802.11 packets in order to gain network access or create a DoS attack.

Airsnarf is an open source tool that creates an AP with a configuration similar to hotspots in an attempt to lure clients.

The AP is broadcasting multiple SSIDs. This can indicate a spoof attempt

The Access Point has changed channels.

An authorized AP denied an association request from client.

An authorized AP denied client access due to authentication failure.

The AP is down.

AP is operating in WDS (bridge) mode.

An AP with low signal strength is detected by BAP sensor.

An overloaded AP refuses new clients from associating with it.

The AP has restarted.

Email us at
vWLAN@bluesocket.com

bluesocket®



BlueSecure™ Wireless IDS (WIDS)

Alarm Type	Description
AP spoof attempt	An attempt to spoof an authorized access point was detected. This could be indicative of a spoofing attack.
AP SSID Changed	An AP has changed its SSID, if this was not authorized then there is a possible spoof in progress.
AP Using Default SSID	The Access Point is using its factory default SSID. This may indicate a mis-configured AP and it should be changed to an SSID appropriate to the installation.
AP Using Hotspot SSID	An AP is using a hotspot SSID.
ASLEAP Attack	ASLEAP is a tool that exploits a weakness in CISCO proprietary LEAP protocol.
Authorized AP Down	An authorized Access Point can no longer be heard by the sensor. This may indicate that the AP has failed or been Removed from service.
Broadcast Attack	Many attacks use broadcast disassociate or deauthenticate frames to disconnect all users on the network, either to redirect them to a fake network or to cause a Denial of Service attack or disclose a cloaked SSID.
Channel with Excess Error	This alert is generated if clients retransmit packets excessively on a given channel.
Channel with too many APs	Too many APs are using the same channel.
Client Association Change	Client has changed its association to a different Access Point. This might be due to a Rogue AP in the vicinity.
Client BSSID Changed	Mobile station has changed its BSSID.
Client Limit	Maximum client limit per AP has been reached. Could be due to a MAC spoofing client or real network density increase.
Client Rate Support Mismatch	Specified mandatory data rate in Probe Request does not match with the values advertised by the AP.
Client To Rogue AP	An authorized client is connected to a rogue AP.
Client with Excess Retransmission	This alert is generated if a client retransmits its data packet.
Deauthentication Flood	An attacker is conducting a Denial of Service (DoS) attack by flooding the network with 802.11 de-authentication frames in an attempt to disconnect users from Access Points. This can result in a Denial of Service (DoS) attack.
Dictionary Attack	This attack is aimed as finding out the password and/or hashing function used in user authentication.
Disassociation Traffic	This alarm indicates that a client is continuing to send traffic within 10 seconds of being disassociated from an AP.
Duration Attack	An attacker sends 802.11 frame with 0xFF in the duration field. This forces other mobile nodes in the range to wait till the value reaches zero. If the attacker sends continuous packets with huge durations, it prevents other nodes from operating for a long time, results in an Denial-of-Service attack.
EAPOL ID Flood	Attacker tries to bring down an AP by consuming the EAP Identifier space (0-255).
EAPOL Logoff Storm	An attacker floods the air with EAPOL logoff frames. It may result in Denial of Service to all legitimate stations.
EAPOL Spoofed Failure	Spoofed EAP failure messages detected.
EAPOL Spoofed Success	Spoofed EAP success messages detected.
EAPOL Start Storm	An attacker floods the air with EAPOL start frames. It may result in Denial of Service to all legitimate stations.
Fata-Jack Attack	A Fata-jack device sends an authentication failure packet to a mobile node to prevent the client from getting any WLAN services.



BlueSecure™ Wireless IDS (WIDS)

Alarm Type

Description

Hotspotter Attack	Hotspotter Attack is an open source tool that passively monitors 802.11 Probe Requests from mobile stations and compares them with common hotspot SSIDs. If there is a match the attacker acts as an AP with the same SSID to fool the mobile station to provide its authentication credential.
Invalid Deauthentication Code	Unknown deauthentication reason code. Some access points and drivers can not handle improper reason codes.
Invalid Disconnect Code	Unknown disassociation reason code. Some access points and drivers can not handle improper reason codes.
Invalid Probe Response	An Access Point has responded to a client probe with a 0-length SSID, which is an invalid response which has been shown to create a fatal error with some client cards. This could be a faulty AP or an attacker specifically crafting the packet to disrupt the network.
Link Test	Some Lucent/Orinoco/Proxim/Agere products provide link testing capability which could use network bandwidth.
MSF Broadcom Exploit	MSF-style poisoned exploit packet for Broadcom drivers, this can be used for client hijacking.
MSF D-Link Exploit	MSF-style poisoned 802.11 rate field in beacon for D-Link driver, this can be used for client hijacking.
MSF Netgear Exploit	MSF-style poisoned 802.11 over-sized options beacon for Netgear driver attack, this can be used for client hijacking.
Netstumbler Probe	Netstumbler is a wireless network scanning tool. This could be the precursor to a more serious attack
Network Probe	A Client is probing the network looking for a wireless AP, but is not connecting. Many wireless cards and operating systems (i.e. Windows XP) do this by default in an attempt to automatically find Access Points, but this could be an operational issue indicating a misconfigured client because it cannot associate
Possible AP Spoof	A BSS timestamp mismatch in beacon or probe frames is likely to indicate an attempt to spoof the BSSID or SSID of an AP.
Rogue Ad-Hoc Client	A rogue client in Ad-Hoc mode has been detected.
Rogue AP	A Rogue AP has been detected. Check that this is not a newly installed Access Point or an AP belonging to a nearby organization.
Rogue Client	A rogue client has been detected.
Rogue Client To AP	A rogue client is connected to an authorized AP.
Spoofed MAC Address	A spoofed MAC address has been detected. If you are using any MAC-based authentication/ access control, the user may be attempting to bypass this protection or hijack another user's session.
SSID too long	SSID length exceeds 32 bytes which is larger than allowed by the 802.11 standard. This is indicative of a SSID handling exploit.
Turbo Cell Mode	Turbo cell is a proprietary solution to support higher data rates. This alert shows that a specific AP is in this mode.
Unapproved Manufacturer	A device is from an unapproved manufacturer.
Using Unauthorized SSID	An authorized client is using an unauthorized SSID.
Wellenreiter Probe	Wellenreiter is a wireless network scanning tool
WEP Disabled	An AP is not using WEP encryption.
WEPWedgie Attack	WEPWedgie is an open source tool for determining 802.11 WEP keys and injecting traffic with the stolen key.

