

What is IPsec?

IP Security is a standard for protecting traffic over the Internet. It was not designed to protect wireless LANs.

What is 802.1x?

802.1x is designed for simple port-based authentication on wired networks. It does not provide any data privacy.

What is WPA/WPA2 (802.11i)?

WPA/WPA2 is designed for easy interoperability, not robust and flexible security. It is off-the-shelf security bundled with newer Wi-Fi equipment.

WIRELESS SECURITY DECISION FACTORS

	IPsec	Fortress Technologies	802.1x	Fortress Technologies	WPA / WPA2	Fortress Technologies
Flexibility	<ul style="list-style-type: none"> May require changes to subnets, DHCP and other LAN components TCP/IP network only 	<ul style="list-style-type: none"> Transparent to network; no subnetting required; use same DHCP/static addresses Configurable Three Factor Authentication™ 	<ul style="list-style-type: none"> Requires RADIUS server even if back-end authentication uses another directory Inflexible user authentication Unable to use in point-to-point environments 	<ul style="list-style-type: none"> Works with common back-end directories (RADIUS, LDAP, NT) Many authentication options Can be used for WLAN and point-to-point applications (802.11, 802.16, etc.) 	<ul style="list-style-type: none"> Requires RADIUS server even if back-end authentication uses another directory Inflexible user authentication 	<ul style="list-style-type: none"> Works with common back-end directories (RADIUS, LDAP, NT) Many authentication options Can be used for WLAN and point-to-point applications (802.11, 802.16, etc.)
Encryption	<ul style="list-style-type: none"> Relying on layer 3 encryption exposes IP addresses Does not protect broadcast or multicast traffic 	<ul style="list-style-type: none"> Encryption at layer 2 protects all data beyond the MAC header Protects broadcast and multicast traffic Protects the network, data and device 	<ul style="list-style-type: none"> No privacy Authentication only — typically paired with WEP/WPA 	<ul style="list-style-type: none"> Strongest commercially available protection with government proven track record Choice of DES, 3DES, or AES-128/192/256 	<ul style="list-style-type: none"> Limited choice of RC4(WPA) or AES-128(WPA2) 	<ul style="list-style-type: none"> Strongest commercially available protection with government proven track record Choice of DES, 3DES, or AES-128/192/256
Authentication	<ul style="list-style-type: none"> Limited options impose inflexible authentication schemes No device level authentication 	<ul style="list-style-type: none"> Three Factor Authentication™: Access ID, Device ID, user name and password Device authentication allows device policies to be enforced Choice of authenticators to deploy 	<ul style="list-style-type: none"> Allows use of weak EAP methods Vulnerable to password-guessing DoS attacks 	<ul style="list-style-type: none"> Three Factor Authentication™ Model eliminates use of vulnerable EAP-types All credentials encrypted with session key, eliminating vulnerabilities 	<ul style="list-style-type: none"> Allows use of weak EAP methods Vulnerable to password-guessing DoS attacks WPA2 — Unproven, new to market 	<ul style="list-style-type: none"> Three Factor Authentication™ Model eliminates use of vulnerable EAP-types All credentials encrypted with session key, eliminating vulnerabilities
Mobility	<ul style="list-style-type: none"> Limited capabilities 	<ul style="list-style-type: none"> Seamless roaming between subnets 	<ul style="list-style-type: none"> n/a 	<ul style="list-style-type: none"> Seamless roaming between subnets 	<ul style="list-style-type: none"> Not supported in the standard 	<ul style="list-style-type: none"> Seamless roaming between subnets
Ease of Use	<ul style="list-style-type: none"> Difficult to deploy and administer Large applications can slow devices 	<ul style="list-style-type: none"> Easy to install and manage "Set & Go" 	<ul style="list-style-type: none"> Difficult to deploy and administer 	<ul style="list-style-type: none"> Easy to install and manage "Set & Go" 	<ul style="list-style-type: none"> Difficult to deploy and administer 	<ul style="list-style-type: none"> Easy to install and manage "Set & Go"
Total Cost of Ownership	<ul style="list-style-type: none"> HIGH Management costs drive higher expense 	<ul style="list-style-type: none"> LOW High choice. High flexibility Works with a variety of networks, devices, directory services, RFs Simple, effective provisioning of new users and devices 	<ul style="list-style-type: none"> MEDIUM Inflexible Upgrades require overhaul of older, existing access points 	<ul style="list-style-type: none"> LOW High choice. High flexibility Works with a variety of networks, devices, directory services, RFs Simple, effective provisioning of new users and devices 	<ul style="list-style-type: none"> MEDIUM Inflexible Upgrades require overhaul of older, existing access points 	<ul style="list-style-type: none"> LOW High choice. High flexibility Works with a variety of networks, devices, directory services, RFs Simple, effective provisioning of new users and devices

SECURITY METHOD

Fortress Technologies Security System

- Complete wireless LAN security solution providing privacy, authentication and access control
- Easy to deploy and centrally managed

- Protects the data, network and device
- Supports legacy, current and future devices
- Requires no change to network or directory services

Fortress Security Gateways

Fortress Secure Gateways offer a greater range of options for easily integrating secure wireless and mobility for existing enterprise infrastructure. By providing a fast and simple means of securing any vendor's wireless network and wireless devices, Fortress Secure Gateways allow customers to protect current and future network investments without worrying about forklift upgrades of their APs or needing to add proprietary wireless switches to their network.

Visit www.fortresstech.com for more information

CORPORATE HEADQUARTERS
Fortress Technologies, Inc.
4023 Tampa Road, Suite 2000
Oldsmar, FL 34677
PHONE: 1 (888) 4PRIVACY or
1.888.4PRIVACY (477-4822)



FORTRESS SECURITY SYSTEM

Secure Gateways	AF2100	AF7500	AF8500
Form Factor	· Compact design · Small, ruggedized, durable · 25 Mbps encrypted throughput	· Enterprise-scale · 1U rack-mount · 75+ Mbps encrypted throughput	· High-performance · Enterprise-scale · Rack mounted chassis(1U) · +150 Mbps encrypted throughput
Dimensions HxWxD in (mm)	1.75x8.5x6 (45x216x152)	1.75x17x12 (45x432x305)	1.7x16.8x12.2 (45x426x334)
Weight	2.6lbs (1.2kg)	7.5lbs (3.4kg)	12.32lbs (5.6kg)
Connections	3 RJ45 10/100 Ethernet, 1 serial	3 RJ45 10/100 Ethernet, 1 serial	· 2 RJ45 10/100/1000 · 1 RJ45 10,100 Ethernet, 1 serial
Power Supply	External AC/DC power adapter	International 120/240 VAC	International 120/240 VAC
Cooling	Fanless heat-sink chassis	2 exhaust fans	3 exhaust fans
Operating Temperature	0° C ~ 60° C	0° C ~ 35° C	0° C ~ 45° C
Storage Temperature	-10° C ~ 70° C	0° C ~ 60° C	-20° C ~ 70° C
Relative Humidity (Non condensing)	5% ~ 95%	10% ~ 90%	5% ~ 95%
Safety and Emissions	CE, FCC and UL	CE, FCC and UL	CE, FCC and UL

Comprehensive Secure Device Support

<i>Enterprise Devices</i>	Windows	CE, CE.Net	Palm*	DOS	Linux
<i>PCs, Laptops, Tablets</i>	●	●		●	●
<i>PDA's</i>		●	●		
<i>Specialized Devices</i>	Windows	CE, CE.Net	Palm	DOS	Linux
<i>Acute Network Technologies</i>		●			
<i>AirSpeak</i>		●			
<i>Neoware</i>		●			
<i>TeleVideo</i>		●			
<i>Wyse</i>		●			
<i>Ruggedized Devices</i>	Windows	CE, CE.Net	Palm	DOS	Linux
<i>HHP</i>		●		●	
<i>Intermec</i>	●	●		●	
<i>LXE</i>	●	●		●	
<i>Psion-Teklogix</i>	●	●		●	
<i>Symbol</i>		●	●	●	

*For Tungsten™ C

Fortress System Components Secure Gateways

AF2100, AF7500 & AF8500 – provide security between wireless devices, users and network infrastructure. All critical security operations – encryption, authentication, data integrity checking, key exchange, and data compression – are optimized to minimize hands-on management. It also provides secure service for multiple access points simultaneously and scales for various architectures.

Secure Client - enables devices to securely communicate with the network and peer to peer. Only authorized devices are allowed access. This lightweight software client supports the widest ranges of devices and operating systems.

Management and Policy Server (MaPS) – provides a centralized management and administration platform for security services and policy management. MaPS facilitates easy control and access to configuration and operational information for thousands of gateways and tens of thousands of users across enterprise LANs and remote facilities.

The Fortress product solution is represented by a global, diverse network of authorized distributors, value-added resellers and system integrators.

