Fortinet Secure Wireless LAN

A FORTINET SOLUTION GUIDE

www.fortinet.com

Introduction to Wireless Security

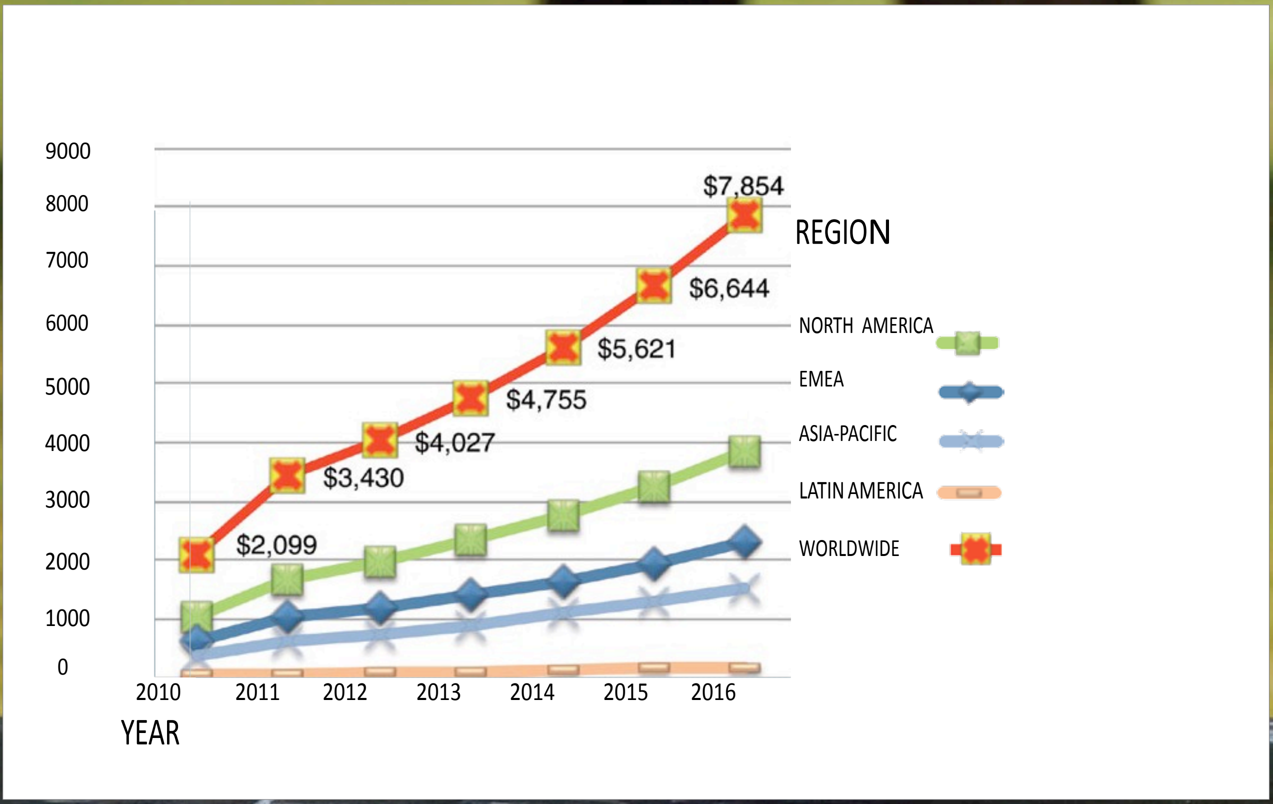
Broad adoption of IEEE 802.11n has created a complex wireless landscape with proliferating mobile devices and applications. It is no longer sufficient to treat all wireless users and applications alike. Threats from social media networks and mobile malware provide a compelling need to deploy and enforce granular WLAN control policies. Fortinet offers the only business-grade wireless solution in the industry today, which addresses these myriads of challenges:

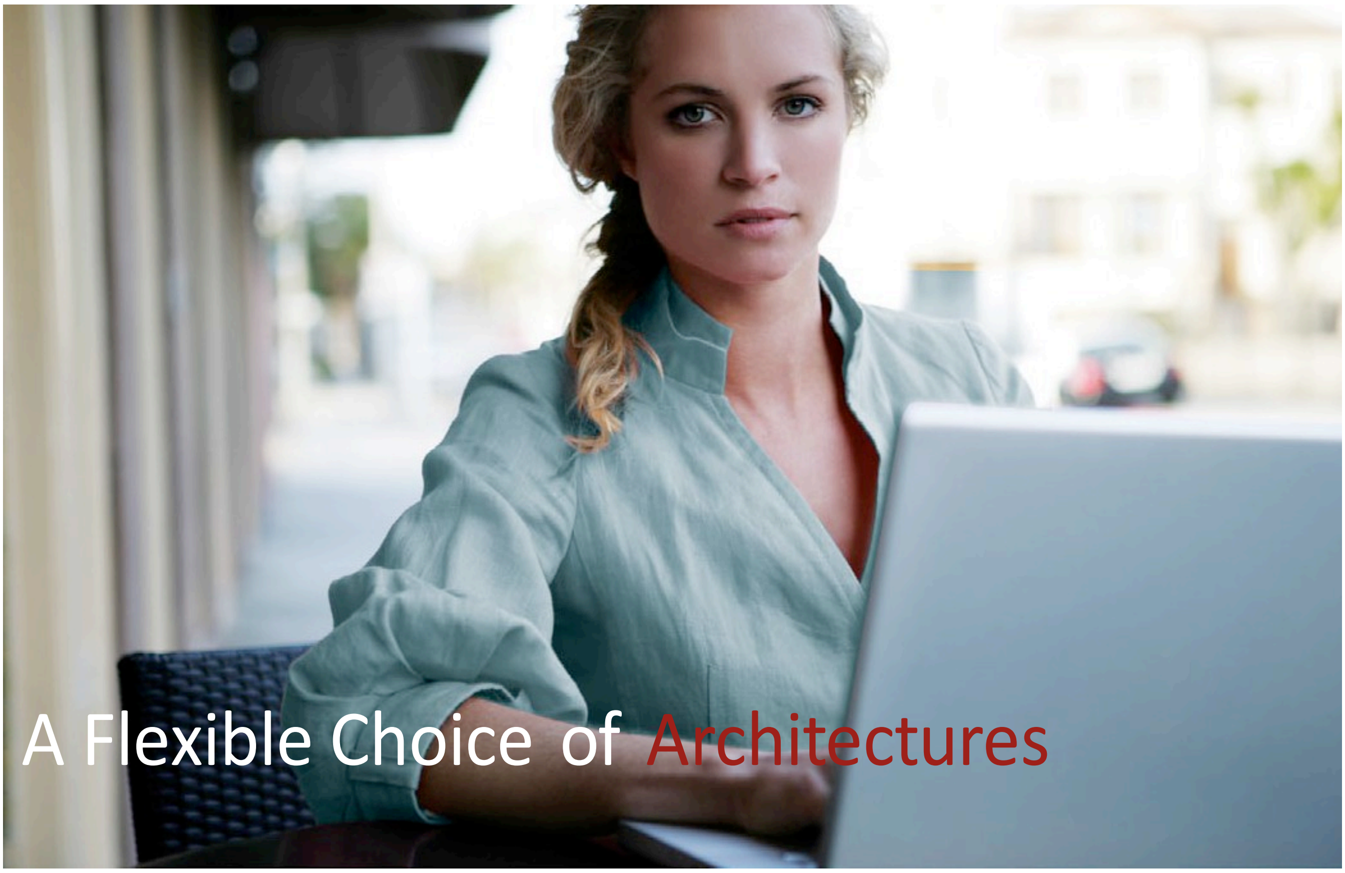
- Identifies business applications and controls their usage n Applies full UTM policies to both wired and wireless data n Brings maximum productivity with fair-use enforcement n Empowers identity-driven policies without complexity
- Introduces simplicity via single pane of glass management
- Provides deployment flexibility with low TCO

Growth of Wireless LANs

The increasing popularity of mobile devices and the need for cost reduction are driving Wireless LAN (WLAN) adoption. Analysts have forecast that spending on enterprise WLAN equipment will rise from $3.4 billion in 2011 to $7.9 billion in 2016, representing a 18.4% CAGR. In addition, organizations have embraced a wireless edge design to drive down the cost associated with edge switches and wiring.

The ratification of the IEEE 802.11n wireless standard is the catalyst for new enterprise adoption since the new standard provides better coverage and fivefold performance increase over legacy wireless outperforming wired Fast Ethernet LANs. This results in a more widespread adoption of WLANs, resulting in a more pronounced need for network application services, such as WLAN network management and security.





A Flexible Choice of Architectures

There are two leading Wi-Fi architectures today. One is called “Thick APs” and the other is referred to as “Thin APs.” The use of a thick or thin AP Wi-Fi architecture depends on the service needs.

Thick AP refers to a wireless access point or Wireless Termination Point (WTP) that autonomously switches packets between wired and wireless domains. Each Thick AP is a standalone device responsible for authentication, encryption and applying access control policies. Each Thick AP requires independent management, or management via a centralized network management application. All-in-one, Thick APs are ideal for locations such as small office or retail shops requiring smaller service area.

A Thin AP provides the same features as a Thick AP, but in a distributed fashion to provide greater service area. The Thin AP simply passes wireless network traffic to the switch/controller, performing few complex tasks locally. This capability will enable all the Thin APs to delegate all the authentication, security processing, channel assignment, transmitter power level and rogue AP detection to the centralized wireless LAN controller which decreases management complexity and reduces overall cost of deployment. As the size of service area increases, you can deploy additional Thin APs and connect them to the existing Controller. Thin APs require a centralized wireless controller for management, and are ideal for locations requiring greater coverage and capacity than a single Thick AP can deliver.

The Need for Comprehensive Wireless LAN Security

Independent of the type of architecture used for access points, WLANs face many threats that strong authentication and link encryption do not address. Because wireless is a shared medium, it is more prone to malicious attacks such as de-authentication broadcasts, evil twin access point (AP) / Honeypot. Also, it is possible for one user’s high usage of application traffic to reduce the bandwidth available to all other users. Therefore you need to implement the same protection mechanisms, that you deploy ubiquitously on your WAN gateway, on your wireless LAN as well. Also, in response to these threats, regulators and standards bodies like the PCI Security Standards Council have created wireless data protection requirements. Failure to comply with those standards can result in significant penalties and/or loss of customer trust due to exposure of protected data.

An End-to-End Security Architecture

There is one policy for how data should be treated in your organization, and that policy provides controls according to who the user is, what applications they are using, and even what device they are using. This requires instituting the 'single pane of glass' management view across wired and wireless resources, as mentioned earlier.

The opportunity here is for greater consolidation of networking elements, providing simplicity and scalability through deployment flexibility with low cost of ownership.

Sometimes piecemeal solutions work when money is no object. In reality, budgets are limited, resources are scarce and networks evolve over-time. It is typically unavoidable that WLAN is an overlay solution, in the sense that it is added to the rest of the network, though this doesn't prevent it being able to behave as though were a designed piece from inception. Given the limitation of power budget and rack space in corporate networks, wireless solutions must avoid adding a large burden. For example, in a truly business- grade WLAN; the controller may be the existing firewall or UTM device already installed in the network. These devices are designed to handle large amount of information and therefore there is reserve processing and storage capacity that may be utilized by the business-grade WLAN. Utilizing existing installed base of network devices inadvertently reduces cost and complexity and lends itself to a more scalable architecture.

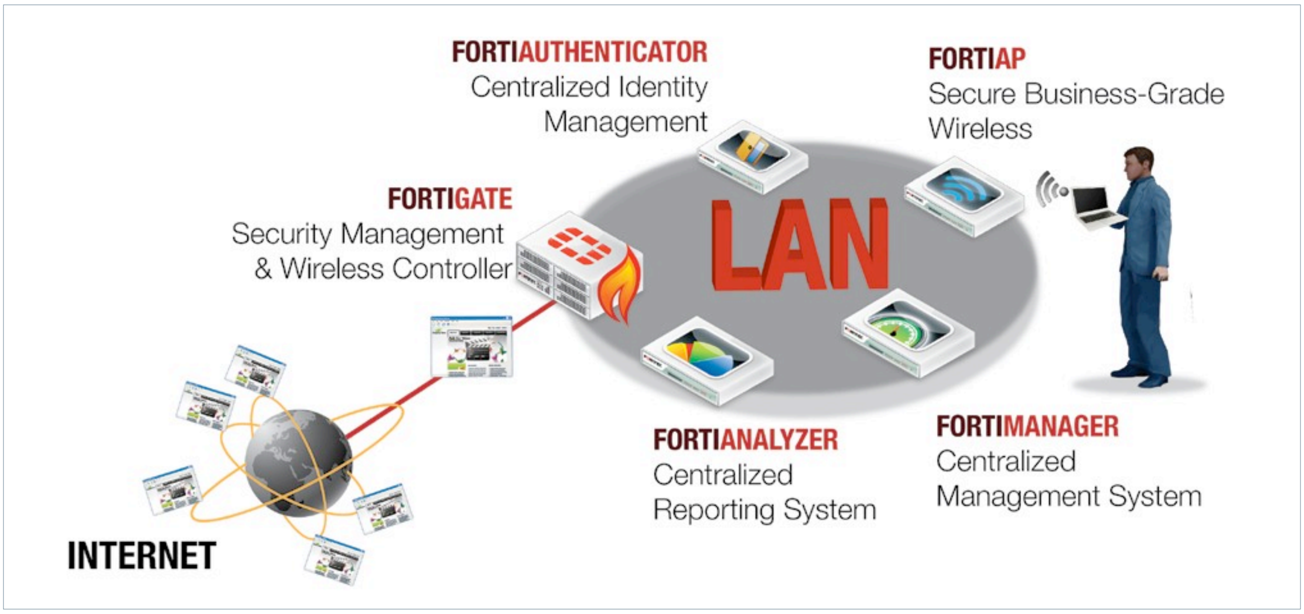
Fortinet's Secure WLAN Solution

As described previously, Fortinet's Secure WLAN solution simplifies the LAN connectivity/security for both wired and wireless networks. It is based on 4 key pillars:

- Firewall and application policies
- User Management
- Logging and reporting
- Configuration and provisioning

The Fortinet Secure WLAN solution is represented Fig 1. It is a combined set of products circulated around the FortiGate and the FortiAPs, which are the core products. Based on the size of the network and architecture FortiAuthenticator, FortiAnalyzer and FortiManager products complement the core products for delivering a full and comprehensive solution.

Figure 1: Fortinet Secure WLAN Solution


FORTIAUTHENTICATOR
Centralized Identity Management
FORTIAP
Secure Business-Grade Wireless
FORTIGATE
Security Management & Wireless Controller
LAN
FORTIANALYZER
Centralized Reporting System
FORTIMANAGER
Centralized Management System
INTERNET

Core Products

FortiGate and FortiAPs are the core products of the Fortinet Secure WLAN Solution.

FortiGate Network Security Platform: Security Management + Wireless Controller

The FortiGate consolidated security platforms can act as wireless controllers, significantly reducing the cost and complexity of deploying secure WLANs. FortiGate platforms enable the integration of both wired and wireless traffic into a single management console, giving you a “single pane of glass” management interface of your network.

FortiGate platforms provide complete content protection against network, content, and application-level threats. These high-performance, low-latency devices ensure that your network security does not become a network bottleneck. FortiGate platforms incorporate sophisticated networking features, such as high availability (active/active, active/passive) for maximum network uptime, and virtual domain (VDOM) capabilities to provide multi-tenant support for subscriber-based environments or greater internal segmentation of data for policy compliance.

FortiWiFi is a FortiGate, ranging from the FortiWiFi-20C to the FortiWiFi-81CM. The FortiWiFi security appliances with Thick AP capabilities,. These Thick AP devices offer a range of performance and features, including high-speed 802.11n support and WAN communications via optional wireless broadband access and dial-up modems.

The FortiWiFi consolidated security platforms deliver comprehensive enterprise-class protection for smaller locations at an affordable price. They make it easy to protect smaller locations, branch offices; customer platforms’ integrated set of essential security technologies, you can deploy a single device that protects all of your applications and data. The simple per-device pricing, integrated management console, and remote management capabilities significantly reduce the costs associated with deploying and managing complete content protection.

Each FortiWiFi model is capable of broadcasting up to seven SSIDs or Virtual Access Points (VAPs) enabling multi-tenant environments in a single device. Each VAP appears a separate virtual interface on the FortiWiFi device, enabling the application of separate firewall and user policies to the traffic.

FortiAp Wireless Access Point Solutions: Secure Wireless

FortiAP wireless access points are enterprise class, controller-managed devices that extend FortiGate® consolidated security functions to your wireless networks. Each FortiAP access points tunnels all of its traffic to the wireless controller integrated into FortiGate platforms, providing a single console to manage both wired and wireless network traffic.

FortiAP wireless access point solutions provide increased visibility and policy enforcement capabilities while simplifying your overall network environment. They employ the latest 802.11n-based wireless chip technology, offering high-performance wireless access point with integrated wireless monitoring and support for multiple virtual APs on each radio. FortiAPs work in conjunction with the feature-rich family of FortiGate controllers to provide a fortified wireless space that delivers complete content protection. FortiGate controllers centrally manage radio operation, channel assignment, and transmit power, which further simplifies your deployment and management requirements.

FortiAuthenticator Two Factor Authentication: Centralized Identity Management

FortiAuthenticator is a centralized user authentication and management service providing various methods of validating the true identity of a user before allowing the access to the requested service making the solution ideal for deployment within small to medium enterprises. Authentication methods include local LDAP and RADIUS or integration with an existing directory service. These methods can be incremented with either time or certificate based two-factor authentication.

FortiAuthenticator will provide as well the self-user registration capabilities and is also available as a Virtual machine (VM).

FortiAnalyzer Logging & Reporting: Centralized Reporting System

FortiAnalyzer platforms integrate network logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout your network. They provide organizations of any size with centralized security event analysis, forensic research, reporting, content archiving, data mining, malicious file quarantining and vulnerability management. Centralized collection, correlation, and analysis of geographically and chronologically diverse security data from Fortinet appliances and third-party devices deliver a simplified, consolidated view of your security posture.

The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

FortiAnalyzer is available as an appliance and as a Virtual Machine (VM).

FortiManager Centralized Management: Centralized Management System

FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure. Whether deploying several or thousands of new devices and agents, distributing updates, or installing security policies across managed assets, FortiManager appliances drastically reduce management costs and overhead. Device discovery, group management, auditing facilities, and the ability to manage complex mesh and star VPN environments are just a few of the timesaving features that FortiManager appliances offer. Complemented by the FortiAnalyzer™ centralized logging and reporting appliance, FortiManager provides a comprehensive and powerful centralized management solution for your organization.

FortiManager appliances can scale to manage thousands of Fortinet devices and agents. Groups of devices and agents, along with their administrators, form the FortiManager concept of Administration Domains (ADOMs). Within an ADOM, an administrator has the ability to create policy packages, folders, and objects that can be shared between all the FortiGate devices in the local ADOM. In the Global ADOM of FortiManager, global policies and objects can also be assigned and applied to sub ADOMs. Whether you are managing one or one thousand ADOMs, FortiManager appliances always provide effective and efficient management of your Fortinet assets.

FortiManager is available as an appliance and as a Virtual Machine (VM).

Why Select Fortinet for Secure WLAN?

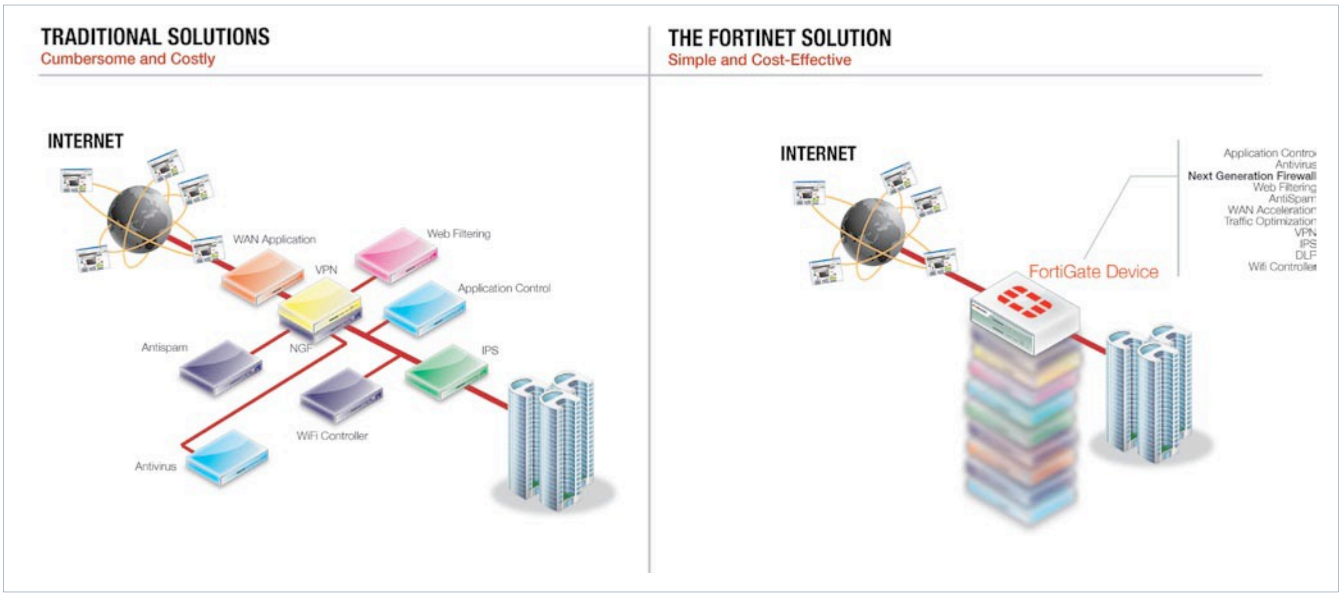
Fortinet is the only vendor providing a full and comprehensive solution delivering

- **Highest security**
  Thanks to its FortiGate platform, Fortinet is recognized by IDC as the worldwide #1 on the UTM (Unified Threat Management) market and by Gartner as the leader in their UTM Magic Quadrant. As the FortiGate platform is at the core of the secure wireless LAN solution, it provides the highest level of security, integrity and management on both the wire and wireless LAN areas. Fig 2.

- **Right sized solution for your deployment**
  The broad range of FortiGate, FortiAuthenticator, FortiAnalyzer and FortiManager platforms (all available in a virtual form factor), ranging from low-end towards mid-range and high-End, enable our customers choosing the right solution based on their needs.

- **Simplified Management**
  Many vendors are offering a secure wireless LAN solution by adding products from different third party suppliers. This brings complexity in terms of configuration, interoperability, troubleshooting and keeps increasing the TCO. Fortinet is dramatically reducing all of these thanks to its different platforms.

Figure 2: How The FortiGate Platform Simplifies And Unifies All Aspects Of Security



Conclusion

The Fortinet secure wireless LAN solution delivers the integrated, consolidated security every organization needs to fortify their wireless network security. FortiGate, FortiWiFi and FortiAP security platforms add layers of security to wireless traffic without affecting performance or increasing costs. You can quickly and easily add core security services such as application control, antivirus, intrusion prevention (IPS), web filtering, antispam, and traffic shaping to your network, which reduce your risk of unauthorized access, data loss, or damage to critical systems.

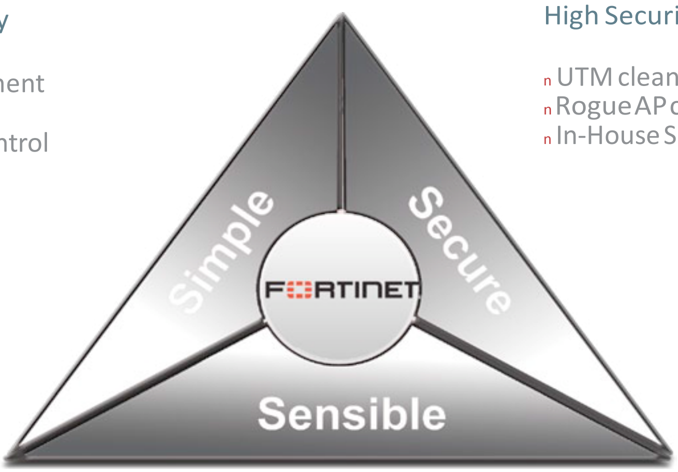
FortiGate and FortiWiFi platforms provide the 'single pane of glass' management you need for increased control and visibility of all network traffic. Our robust reporting and analysis tools also help you demonstrate policy compliance and satisfy audit requests. Fortinet delivers complete, end-to-end security, from the mobile endpoint to the network core. Our solutions scale for any size environment, from the SOHO to Headquarters to a global telecommunications provider.

Sophisticated Simplicity

- Unified global management
- All-in-one appliance
- Business application control

High Security

- UTM cleansing of wireless traffic
- Rogue AP control for PCI
- In-House Security Experts



- Use your existing FortiGate, no additional licenses
- Less devices to manage
- Lower TCO

Fortinet is a global provider of high-performance network security solutions that provide our customers with the power to protect and control their IT infrastructure. Our purpose-built, integrated security technologies, combined with our FortiGuard security intelligence services, provide the high performance and complete content protection our customers need to stay abreast of a constantly evolving threat landscape. More than 125,000 customers around the world - including the majority of the Global 1,000 enterprises, service providers and governments - are utilizing Fortinet's broad and deep portfolio to improve their security posture, simplify their infrastructure, and reduce their overall cost of ownership. From endpoints and mobile devices, to the perimeter and the core - including databases, messaging and Web applications - Fortinet helps protect the constantly evolving networks in every industry and region around the world.

AMERICAS HEADQUARTERS

1090 Kifer Road
Sunnyvale, CA 94086 United States
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA HEADQUARTERS

120 rue Albert Caquot Sophia
Antipolis France 06560
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC HEADQUARTERS

300 Beach Road 20-01 The Concourse
Singapore 199555
Tel +65.6513.3734
Fax +65.6295.0015

ICSA labs CERTIFIED SSL VPN

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED ANTI-VIRUS

ICSA labs CERTIFIED NETWORK IPS

ICSA labs CERTIFIED IPSEC - BASIC

FORTINET®

www.fortinet.com

Performance metrics contained herin were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.