Fortinet Secure Wireless LAN Controllers are powered by FortiOS, a purpose-built network security operating system, which forms the foundation of the FortiGate Network Security Platform. Delivering the industry’s most comprehensive suite of security, wireless and networking services, this enterprise class Wireless LAN Controller is purpose-built to leverage the hardware acceleration provided by custom FortiASIC™ processors. Fortinet Secure Wireless LAN Controllers deliver an easy to use and high performance enterprise wireless solution, in a single unified platform.

**End-to-End Wireless LAN Security**
Today's organizations are facing numerous challenges as the network environment evolves with the rapid adoption of BYOD, demanding mobile workforce and evolving security threats. The need for secure wireless networks with intra-SSID privacy, robust third-party certified security and advanced networking capabilities, is now more important than ever. Fortinet Secure Wireless LAN Controllers with FortiAP Access Points meet the demanding needs of enterprise Wireless LAN, with proven market leading security and management for both wired and wireless networks.

**Unbeatable flexibility to meet all deployment needs**
A wireless infrastructure must be flexible and scalable. By consolidating security and wireless network capabilities, Fortinet Secure Wireless LAN Controllers significantly reduce network complexity and ultimately TCO. Fortinet’s no-VLANs™ approach reduces complex Layer-2 requirements, eliminating the need to propagate VLAN information across the network to simplify and accelerating large, scalable deployments.

**FortiOS 5 Wireless LAN Controller Highlights**
- True Enterprise WLAN System
- Support for 802.11ac Gigabit WiFi
- Flexible Deployment Models for Distributed Enterprise, Education, Healthcare and Hospitality
- Integrated UTM Security and Management
- Automatic Radio Resource Provisioning
- PCI Compliance Capabilities for Retail Stores
- Integrated Guest Access Management with Captive Portal
- BYOD Device Finger Printing and Control
- Deep Layer-7 Application Control
- Easy to use Centralized Management through Web GUI
- Multi-Hop Mesh
- Point-to-Point Bridging
- Remote AP with Cloud Controller
- Integrated WIDS and Rogue AP Management
- Scale from 1 to 10,000+ of APs

**Key Features and Benefits**

<table>
<thead>
<tr>
<th>Scalable and Resilient</th>
<th>Highly scalable and centrally managed enterprise WLAN, with integrated radio resource management to reduce co-channel interference and provide consistent WLAN performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated UTM Features</td>
<td>Extends wired security features to WLAN, unifying both wired and wireless management into a single console, providing a “Single Pane of Glass” management interface to the network.</td>
</tr>
<tr>
<td>Layer-7 Application Visibility</td>
<td>Leverage the market leading UTM features with the power of ASIC-based deep packet inspection technology to deliver granular application level visibility and control.</td>
</tr>
</tbody>
</table>
**HIGHLIGHTS**

**Single pane of glass management**
Integrating wired and wireless security into a single pane of glass lowers operating costs and reduces IT staff workloads by eliminating the complexities of troubleshooting a multivendor network and the need for costly training and certification across multiple vendor products. In addition to reducing operating costs, a single pane of glass for management also ensures that a consistent security and control policy is applied across both the wired and wireless networks.

**Sophisticated Application Control**
Wireless bandwidth is a precious shared medium and it is critical that business applications receive priority on the wireless LAN. FortiOS Application Control is built-in to the Wireless LAN controller and uses deep Layer-7 inspection with over 2,700 application signatures to provide bandwidth guarantees and prioritization of critical applications. This industry leading Application Control capability provides the fine-grained application control required to ensure the Wireless LAN is performing at its best and is being utilized for the intended applications.

**Industry Leading Security**
FortiOS has its pedigree in Unified Threat Management and Fortinet holds more industry certifications than any other vendor, providing the best-in-class unified protection with an integrated set of security services. From antivirus, web content filtering, application control, network IPS, email filtering and DLP, the same security that is applied to the wired network can now be applied to the wireless LAN.

Built-in Wireless Intrusion Detection System capabilities intelligently further protects the wireless LAN by detecting a vast array of RF intrusion techniques including:
- Unauthorized Device Detection
- Rogue/Interfering AP Detection
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection
- Misconfigured AP Detection
- Weak WEP Detection
- Multi Tenancy Protection
- MAC OUI Checking
Automated Rogue AP Detection and Suppression
Rogue access points pose a serious network security threat by creating a leakage point where sensitive data such as credit card information can be siphoned off the network. For this reason, the PCI DSS and other data security standards often mandate proactive monitoring and suppression of rogue APs. The FortiGate Rogue AP on-wire detection engine uses various correlation techniques to determine if a Rogue AP is connected to the network. This automated process continuously monitors for unknown APs and automatically suppress any found to be unauthorized.

High Density
FortiOS monitors wireless client connections on each AP and ensures the connection load is spread uniformly across the network. This ensures better airtime utilization and provides increased capacity, resulting in a better performing WLAN. Devices can also be distributed across radios (frequencies) on a single AP, by intelligently steering dual band devices to the less crowded and higher performance 5 GHz band.

Automatic Radio Resource Provisioning
FortiOS DARRP (Distributed Automatic Radio Resource Provisioning) technology ensures the wireless infrastructure is always optimized to deliver maximum performance. Fortinet APs enabled with this advanced feature continuously monitor the RF environment for interference, noise and signals from neighboring APs, enabling the FortiGate WLAN Controller to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, DARRP also ensures that it chooses the optimal channel, without administrator intervention.

Strong, Flexible Authentication
FortiOS supports standard WPA2 authentication using pre-shared keys as well as enterprise grade authentication using 802.11i or 802.1x with RADIUS. When 802.1x is enabled, users are authenticated against a backend RADIUS server, either provided by FortiAuthenticator or directly against a Microsoft Active Directory server. FortiOS also supports embedded public certificates for WPA-Enterprise authentication, MAC address authentication and MAC address white/black lists for complete and flexible authentication options based on the network constraints.

Guest Captive Portal
Browser-based authentication for guest users is also supported in using via the SSL enabled captive portal. This built-in captive portal allows for HTML login page customization as well as guest account provisioning and management via an integrated guest management portal. FortiOS also supports universal access method (UAM) for integrating with third-party external captive portal servers as well as two-factor authentication with the FortiToken One Time Password (OTP) solution.

Wireless LAN Planning and Analysis
FortiPlanner is a graphical Wireless LAN Planning and Post-Deployment Site Survey utility, designed to simplify WLAN planning and deployment of Fortinet FortiAP based wireless networks. Sophisticated signal propagation ray tracing algorithms are used to ensure precise pre-deployment planning accuracy, as well as accurate post-deployment visualization via real-time heat-maps.

Secure Wireless LAN
Complete Secure Wireless LAN architecture:
- Captive Portal, 802.1x, Temporary Guest Access
- User & Device Identification, Authorization
- User & Device based policies, Application Control
- Rogue AP Mitigation, Wireless Intrusion Detection
- User & Application Based Wireless QOS
- Detailed Network & Threat Visibility, Compliance Reporting
**FEATURE SUMMARY**

### WIRELESS CONTROLLER

**Networking**
- **DHCP** Integrated DHCP server
- **VLANs** Import and export
- **SSID to VLAN mapping** Dynamic VLAN Support

**Routing**
- Static, dynamic and policy routing

**Multicast** PM mode

**Data Forwarding**
- Centralized – Bridged locally
- Distributed – Unicast conversion
- Split Policy based – Selective forwarding based on resources, policy

### Provisioning and Management

**Management Access**
- HTTPS via web browser
- SSH, Telnet and console
- SNMP (V1 and V2)

**Monitoring**
- Access Point (radio, channel) — Status, usage, utilization
- Wireless health monitoring, client trends, overloaded APs, excessive RF errors

**Centralized Management**
- Single pane of glass management for wired and wireless security and configuration
- Centralized management of thousands of locations via FortiManager and FortiAnalyzer
- Centralized reporting, network analytics and trends of thousands of locations

**Troubleshooting**
- Remote wireless packet capture

**Remote AP**
- Supported on all FAP models
  - Enables APs to be deployed remotely over WAN link to the FortiGate
  - Wireless LAN Controller
  - Option to encrypt data traffic via DTLS
  - Split routing – Selective forwarding based on policy (FortiOS 5.2)

**WAN Survivability**
- Wireless client connectivity is maintained when the wireless controller is unreachable for open and PSK type SSIDs

**Mesh and Bridging**
- Local FAP diagnostic web portal

**Topology**
- Multi-hop mesh
- Support for multiple mesh instances

**Mesh Hops**
- Configurable maximum hop count

**Bridging**
- Point-to-Point bridging
- Point-to-Multipoint bridging for wireless ISP applications

### Wireless Access and Authentication

**Access – Authentication Methods**
- IEEE 802.1x (EAP, Cisco-LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-AKA)
- RADIUS
- 802.1X RADIUS, authentication
- 802.1X RADIUS, support for EAP
- 802.11a: RADIUS, authentication
- WPA (Wi-Fi Protected Access) Personal and Enterprise – 802.11i standard
- WPA-Enterprise – 802.11i standard
- WPA2
- WPA2-Enterprise
- WPA3
- WPA3-Enterprise
- WPA3-Enterprise

**Authentication Servers**
- Internal Database, RADIUS, LDAP, RADIUS+, RADIUS, External Authentication Servers – Microsoft Active Directory, Microsoft IAS

**Encryption Protocols**
- WEP
- TKIP
- TKIP+AES
- AES
- AES+AH
- AES+ESP
- IPSec
- L2TP/IPSec
- L2TP/IPSec (RFC 3193)
- SSL
- AES TKIP+AES
- TKIP+AES

**VPN**
- SSL
- IPSec

**Captive Portal**
- Authentication against internal or external authentication server
- Fully customizable look and feel including branding, graphics and language

**Guest User Management**
- Inegrated receptionist guest user management portal
- Configurable expiration time
- Configurable start times
- Bulk account creation
- Integration with FortiAuthenticator for self-service captive portal with e-mail login

### RF and Performance Management

**DAARP (Distributed Automatic Radio Resource Provisioning)**
- Automated selection of RF channel to achieve consistent optimal performance

**DAARP Scheduling**
- Configurable (enable/disable)
- Enable with the option to exclude time slots

**802.11n HT20 and HT40 support**
- Supported

**802.11ac 80 MHz option**
- Supported on 802.11ac models

**Band Steering**
- Load-balances stations across 2.4 GHz and 5 GHz RF bands for optimal performance and reducing interference

**AP Load Balancing**
- Load-balances stations across 2.4 GHz and 5 GHz RF bands for optimal performance and reducing interference

**Self Healing**
- Automatically adjusts TX power levels to extend coverage to compensate for failed APs

**RF Planning**
- Enabled by FortiPlanner software
- Predictive RF planning
- Real-time Dynamic Heatmaps
- Site Survey

**Rogue AP Management**
- Background Scanning
  - Background and full-time scanning for rogue APs

- On-Wire Correlation
  - On-Wire correlation to identify malicious APs that are connected to the local network

- Over-the-air suppression of offending APs and counter measures to prevent clients attempting to connect to an identified rogue AP

- Wireless IDS
  - Detects andlogs multiple RF intrusion methods
  - Multi-layer detection of RF events

- Event Logging
  - Pre-built reported for PCI-DSS compliance generated via FortiAnalyzer

- Auditing
  - Policy based retagging of applications

- BYOD and Mobility
  - Distinguish between corporate assets and employee owned devices

- Device Identity
  - Identify and classify device types, vendor information, OS types and OS version

- Application Visibility
  - Layer 7 application detection with support for over 3,000 signatures

- Quality of Service
  - End-to-end QoS

- Policy based retagging of applications

- Quality of Service
  - Prioritize transmission of business critical applications over wireless

  **Authentication Servers**
  - Internal Database, RADIUS, LDAP, RADIUS+, RADIUS, External Authentication Servers – Microsoft Active Directory, Microsoft IAS

  **Encryption Protocols**
  - WEP
  - TKIP
  - TKIP+AES
  - AES
  - AES+AH
  - AES+ESP
  - IPSec
  - L2TP/IPSec
  - L2TP/IPSec (RFC 3193)
  - SSL
  - AES TKIP+AES
  - TKIP+AES
  - TKIP
  - AES TKIP+AES
  - TKIP+AES

  **VPN**
  - SSL
  - IPSec

  **Captive Portal**
  - Authentication against internal or external authentication server
  - Fully customizable look and feel including branding, graphics and language

  **Guest User Management**
  - Inverted receptionist guest user management portal
  - Configurable expiration time
  - Configurable start times
  - Bulk account creation
  - Integration with FortiAuthenticator for self-service captive portal with e-mail login

  **RF and Performance Management**
  - Automated selection of RF channel to achieve consistent optimal performance

  **DAARP (Distributed Automatic Radio Resource Provisioning)**
  - Configurable (enable/disable)
  - Enable with the option to exclude time slots

  **802.11n HT20 and HT40 support**
  - Supported

  **802.11ac 80 MHz option**
  - Supported on 802.11ac models

  **Band Steering**
  - Load-balances stations across 2.4 GHz and 5 GHz RF bands for optimal performance and reducing interference

  **AP Load Balancing**
  - Load-balances stations across 2.4 GHz and 5 GHz RF bands for optimal performance and reducing interference

  **Self Healing**
  - Automatically adjusts TX power levels to extend coverage to compensate for failed APs

  **RF Planning**
  - Enabled by FortiPlanner software
  - Predictive RF planning
  - Real-time Dynamic Heatmaps
  - Site Survey

  **Rogue AP Management**
  - Background Scanning
    - Background and full-time scanning for rogue APs

  - On-Wire Correlation
    - On-Wire correlation to identify malicious APs that are connected to the local network

  - Over-the-air suppression of offending APs and counter measures to prevent clients attempting to connect to an identified rogue AP

  - Wireless IDS
    - Detects and logs multiple RF intrusion methods
    - Multi-layer detection of RF events

  - Event Logging
    - Pre-built reported for PCI-DSS compliance generated via FortiAnalyzer

  - Auditing
    - Policy based retagging of applications

  - BYOD and Mobility
    - Distinguish between corporate assets and employee owned devices

    - Device Identity
      - Identify and classify device types, vendor information, OS types and OS version

    - Application Visibility
      - Layer 7 application detection with support for over 3,000 signatures

    - Quality of Service
      - End-to-end QoS

      - Policy based retagging of applications

      - Quality of Service
        - Prioritize transmission of business critical applications over wireless
### FEATURE SUMMARY

<table>
<thead>
<tr>
<th>Policy Management</th>
<th>Manage and enforce firewall and traffic shaping policies based on device and user identity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility Support</td>
<td>Fast Roaming — 2–3ms between APs on the same FortiGate</td>
</tr>
<tr>
<td></td>
<td>802.11i fast-roam back</td>
</tr>
<tr>
<td></td>
<td>802.11i fast-associate in advance</td>
</tr>
<tr>
<td></td>
<td>PMK caching</td>
</tr>
<tr>
<td>Presence Detection</td>
<td>Presence detection for presence analytics</td>
</tr>
<tr>
<td>IPv6 Support</td>
<td>Support for IPv6 clients</td>
</tr>
<tr>
<td>Traffic</td>
<td>Routing protocols, firewall and UTM support</td>
</tr>
<tr>
<td>Certifications</td>
<td><strong>Wi-Fi Alliance</strong></td>
</tr>
<tr>
<td></td>
<td>Wi-Fi Alliance certified (802.11a/b/g/n/ah, WPA™ Personal, WPA™ Enterprise, WPA2™ Personal, WPA2™ Enterprise, WMM™, WMM™ Power Savel)</td>
</tr>
<tr>
<td>Firewall</td>
<td>ICSA firewall enterprise certification</td>
</tr>
<tr>
<td></td>
<td>ICSA IPv6 certified firewall</td>
</tr>
<tr>
<td></td>
<td>USGv6 certified firewall</td>
</tr>
<tr>
<td>IEEE Standard Compliance</td>
<td>802.11a, 802.11n, 802.11g, 802.11n (2x2 MIMO), 802.11n (3x3 MIMO), 802.11n with Automatic Power Save Delivery (VAFS2), 802.11n with HT4Q support, 802.11ac, 802.11e and WMM/MIM Multimedia Extensions, Block ACK, NoAck, 4 priority queues, 802.11h, 802.11i, 802.11r, 802.11v, 802.11w, 802.11x</td>
</tr>
</tbody>
</table>

**NOTE:** Feature set based on FortiOS Version 5.2. Unique FortiOS 5.2 features are marked, some features or certification may not apply to all models.

### FORTIAP

**Operation Modes**
- Access Point
- Full-time Monitor
- Mesh Root
- Point to Point Bridge Mode
- Stand-alone site survey mode

**Controller Discovery**
- Static IP
- Automatic discovery via Multicast SNMP Broadcast
- Pre-provisioned AP using Serial No
- DHCP Option 138

### ADDITIONAL REFERENCES

<table>
<thead>
<tr>
<th>Resources</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>The FortiOS Handbook</td>
<td><a href="http://docs.fortinet.com/fgt.html">http://docs.fortinet.com/fgt.html</a></td>
</tr>
<tr>
<td>Product Datasheets and Matry</td>
<td><a href="http://www.fortinet.com/resource_center/datasheets.html">http://www.fortinet.com/resource_center/datasheets.html</a></td>
</tr>
</tbody>
</table>

**GLOBAL HEADQUARTERS**
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737

**EMEA SALES OFFICE**
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

**APAC SALES OFFICE**
300 Beach Road #20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

**LATIN AMERICA SALES OFFICE**
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2014 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results 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 certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. 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 covenants, representations, and guarantees pursuant hereto, whether express or implied. 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.

FST-PROD-DS-WLC
FOS-WLC-DAT-R1-201405