TCS WI-FI

Secure Wi-Fi Solutions Keeping You Connected

WHY YOUR ORGANIZATION NEEDS A TCS SECURE WI-FI SOLUTION

With 6.5 million Wi-Fi certified devices shipping every day, Wi-Fi has become the network of choice in every type of business large and small, public venues, and hundreds of millions of homes. Wi-Fi has become ubiquitous, from home and workplace to coffee shop and on aircraft, Wi-Fi can keep you connected.

The days of one-size-fits-all Wi-Fi are over. The wide range of different use cases, deployment models, security requirements, and budgets dictate that vendors deliver different Wi-Fi solutions for different markets and deployment topologies.

Large campuses, distributed enterprises, and small businesses all have diverse WLAN architecture needs but also a common requirement for security. That's why TCS has partnered with Fortinet, a global leader in Secure Wi-Fi. Collectively, we deliver a full suite of Secure WLAN products as part of a Secure Access solution designed to address the unique requirements of every organization, in every market segment without sacrificing comprehensive security.

Configuration and control of your wireless environment can be done directly with a FortiGate security appliance or via our Wireless LAN controllers.

FORTINET SECURE WI-FI INCLUDES:

- Single-pane-of-glass management for wireless, wired and security policies
- Zero-touch deployment - no requirement for onsite tech support
- Simplicity of the cloud with integrated UTM service in AP (Forti-AP S-Series)
- Industry-leading customer analytics and engagement tools for retailers

TCS Connected IT

FORTIGATE INTEGRATED WIRELESS LAN CONTROLLER

Customers demand more capability from fewer components to save on cost and complexity. Fortinet's security appliance, FortiGate, is supplied with a Wireless LAN and Switch controller built in for no extra cost. The Integrated solution is Security-Fabric-enabled, providing the broad visibility, automated protection, and integrated threat intelligence required to protect the valuable assets and data of organizations worldwide all within a single pane of glass.

HIGHLIGHTS

UNBEATABLE FLEXIBILITY TO MEET ALL DEPLOYMENT NEEDS

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 accelerate large, scalable deployments. With a wide range of FortiGate models to choose from, no matter the size of your network, there's a FortiGate solution right for you.

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, a single pane of glass provides complete visibility of clients, access points, switches and security services, ensuring consistent security and control policies are applied across the enterprise.

SOPHISTICATED APPLICATION CONTROL

FortiOS Application Control is built-in to the Wireless LAN controller and uses deep Layer-7 inspection with over 4,000 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:

- Association/Authentication/EAPOL Flooding
- Broadcast deauthentication
- Spoofed MAC
- Ad-hoc Network Detection and Containment
- Wireless Bridge Detection § Misconfigured AP Detection
- 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. 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.

BAND STEERING

Band steering makes more efficient use of your available wireless network by sending clients to the bands where they are most efficiently served. Without band steering, a dual band client could associate on either the 2.4 GHz or the 5 GHz channels, leading to overcrowding on one band or the other. With band steering, you can direct some of this traffic to your band of choice. Band steering can also separate devices by their importance (or the importance of the types of traffic they will be passing on your network). You can leave all clients with low priority profiles on the 2.4 GHz channels (where bandwidth is not a concern) and move clients to the 5 GHz band to achieve higher data rates.

Best-in-class, Unified Protection

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.

CAPTIVE PORTAL

Browser-based authentication for guest users is also supported 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.

DEVICE FINGERPRINTING

Device fingerprinting allows collection of various attributes about a device connecting to the network managed by the FortiWLC. The collected attributes can fully or partially identify individual devices, including the client's OS, device type, and browser being used. Device Fingerprinting allows system administrators to be more aware of the types of devices in use and take actions if necessary.

FORTIAP SERIES MANAGED ACCESS POINTS

FortiAP access points are managed centrally by the integrated WLAN controller of any FortiGate® security appliance or can be managed through the free FortiCloud provisioning and management portal. With the integration of the wireless controller functionality into the market-leading FortiGate appliance, Fortinet delivers a true Unified Access Layer. This enables you to easily manage wired and wireless security from a Single-pane-of-glass management console and protects your network from the latest security threats.

UNIFIED MANAGEMENT

Unified management console simplifies operations, ensuring consistent and effective policy enforcement and compliance.

ADVANCED SECURITY PROTECTION

Wireless LAN security done right, from the leader in network security. Integrated Firewall, IPS, Application Control, and Web Filtering protect the wireless LAN from the latest security threats.

BUILT-IN WIFI SECURITY

Protects the network from advanced wireless threats and satisfies PCI DSS compliance.

DEDICATED WIRELESS LAN CONTROLLER

Some wireless deployments require high mobility with high performance and the Fortinet Wireless Controller can provide enterprise-class Wi-Fi to deliver this in large and high-density environments. The Controller and Management platforms are available as appliances or as virtual machines, and when combined with enterprise-class 802.11ac Wave 2 access points, the controllers deliver seamless mobility, quick deployment, and easy capacity expansion with radio frequency virtualization.

FORTIWLC WIRELESS CONTROLLERS

The FortiWLC Controller series optimizes traffic across our controller-based wireless access points and client devices to support high density, high performance and predictability while addressing mission-critical enterprise demands for wireless connectivity.

HIGHLIGHTS

VIRTUAL CELL

Virtual Cell minimizes the complex, time-consuming process of channel planning, which can take months for a large campus, through its unique single channel deployment model which avoids the challenges of planning around co-channel interference. In a Virtual Cell, all radios operate on the same channel providing a layer of coverage across your campus and appear to clients as a single radio wherever they go. In addition, the network, not the client, controls how and when clients roam.

GUEST CAPTIVE PORTAL

Browser-based authentication for guest users is supported in FortiWLC via captive portal. The built-in captive portal allows for HTML login page customization by an administrator. FortiWLC also supports universal access method (UAM) for integrating with third-party external captive portal servers as well as OAuth based upon login credentials from social networks.

AUTOMATIC RADIO RESOURCE PROVISIONING

FortiWLC can be configured for ARRP (Automatic Radio Resource Provisioning), a technology that ensures the wireless infrastructure is always optimized to deliver maximum performance. When enabled, this advanced feature continuously monitors the RF environment for interference, noise and signals from neighboring APs, enabling the FortiWLC to determine the optimal RF power levels for each AP on the network. When a new AP is provisioned, ARRP also ensures that it chooses the optimal channel, without administrator intervention.

SPECTRUM SCANNING

FortiWLC provides the ability to configure deployed APs in spectrum scanning mode, acting as a software-based spectrum monitoring device. It provides a wealth of spectrum data detected in the 2.4 GHz and 5 GHz spectrum, including graphical representations of Channel Availability, Channel Utilization, Spectrogram, Equalizer, and Persistence data.

TIME-BASED ESS

When configuring an ESS within the FortiWLC, you can schedule the availability of that ESS based on pre-defined time intervals. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days. A network set up for a specific event can be configured to shut off as soon as the event completes, or for additional security, networks that are not needed during certain times of the day can be shut down to be unavailable.

HITLESS FAILOVER/REDUNDANCY

Enterprise WiFi is now a permanent fixture within all organizations, often carrying mission critical data, if the network stops, operations grind to a halt as well. Fortinet's FortiWLC provides for hitless failover with N+1 redundancy. The optional N+1 redundancy software feature, when implemented, allows a standby N+1 controller in the same subnet to monitor and seamlessly failover more than one master controller, and are considered to be an N+1 cluster. The standby monitors the availability of all the master controllers

Seamless Communication

in the cluster by receiving advertisement messages sent by the masters. If advertisements are not received, the standby changes state, assumes the IP address of the failed master, and takes over operations for the failed master. Because the standby already has a copy of the master's latest saved configuration, all configured services continue while the controller switches from standby to active state.

BAND STEERING

Band steering makes more efficient use of your available wireless network by sending clients to the bands where they are most efficiently served. Without band steering, a dual band client could associate on either the 2.4 GHz or the 5 GHz channels, leading to overcrowding on one band or the other. With band steering, you can direct some of this traffic to your band of choice. Band steering can also separate devices by their importance (or the importance of the types of traffic they will be passing on your network). You can leave all clients with low priority profiles on the 2.4 GHz channels (where bandwidth is not a concern) and move clients to the 5 GHz band to achieve higher data rates.

SERVICE CONTROL

Fortinet's Service Control feature is designed to allow clients in the enterprise network to access and communicate with devices that are advertising service via a protocol such as Bonjour. Many Bonjour-enabled devices were largely designed for small-scale use; however, they are growing increasingly prevalent in the enterprise-level environment. The nature of these services makes scaling for larger deployments challenging because the wireless traffic communications for these protocols cannot travel across various subnets. Service Control on Fortinet's FortiWLC addresses this problem by providing a framework by which Fortinet will direct traffic from clients on different subnets over to the Bonjour-capable devices (and vice versa), allowing seamless communication between the two.

DEVICE FINGERPRINTING

Device fingerprinting allows collection of various attributes about a device connecting to the network managed by the FortiWLC. The collected attributes can fully or partially identify individual devices, including the client's OS, device type, and browser being used. Device Fingerprinting allows system administrators to be more aware of the types of devices in use and take actions if necessary.

APPLICATION VISIBILITY

The FortiWLC allows for application visibility with Deep Packet Inspection. Administrators can set policies to monitor and/or block one or more types of application traffic. Application control can be flexibly implemented based on a number of conditions: All ESS profiles, Per ESS profile, All APs, Per AP, Per AP Group, or ESS and AP Combination. Additionally, users can define custom applications that are not part of the pre-loaded system defined applications.

HIGHLY SCALABLE

No matter the size of your network, there's a FortiWLC solution right for you, and should you need more than one controller, Fortinet's Wireless Manager platform (FortiWLM) allows you to stack and manage multiple controllers with ease.

ROGUE AP DETECTION

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. 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.

FORTIWLM WIRELESS MANAGER

Fortinet's Wireless Manager series provides both hardware platforms and a virtual machine to support Fortinet's controller-based wireless solution. The Wireless Manager offers full management of the controllers and access point configuration along with an extensive set of trouble-shooting and reporting tools.

HIGHLIGHTS

NETWORK MANAGER

KEY FUNCTIONS

- Comprehensive real-time and historical WLAN performance trends dashboards including RF metrics for a centralized view.
- Real-time and historical RF visualization enables remote management and saves on-site truck-roll expenses.
- Current and historical wireless station metrics enable rapid resolution of issues by rewinding and recreating past state.
- Customized dashboards for mobile devices allow anytime, anywhere management of WLAN network.
- Integrated Rogue AP detection enhances enterprise security.
- Extensive wireless reports support network audits and enterprise reporting requirements.
- Alarms and events with customizable notifications facilitate proactive wireless network monitoring and troubleshooting.
- Enterprise scalability allows management of up to 15,000 APs.

PROVISIONING AND DEPLOYMENT

The Network Manager enables users to easily provision and manage multiple Fortinet controllers from a single web interface. One of the primary functionalities of the Network Manager is the ability to create a global controller configuration and push it to one or more managed controllers. If a global controller configuration is changed in the Network Manager, all controllers using it are automatically updated with those changes. To enhance security, the global controller configurations are owned by the Network Manager and cannot be altered by the controllers using them.

Inventory view in the Network Management platform provides users with a streamlined view to look at all the provisioned controllers. Administrators can also directly add controllers from the Inventory, to be managed by the Network Management Platform.

SPECTRUM MANAGER

Spectrum Manager is a software application that detects and classifies sources of wireless interference to ensure optimal spectrum usage and high service levels. By keeping you informed about Wi-Fi interference, Spectrum Manager allows you to proactively take action to alleviate problems by removing, adjusting for, or working around the sources of interference.

Spectrum Manager gathers interference data from a network of dedicated sensors. It can also gather data from the APs which can dedicate one of its three radios to act as a sensor. The information captured includes the type of interferer, signal strength, impacted channels, start/end time, and duration.

SERVICE ASSURANCE MANAGER

Fortinet's Service Assurance Manager is the industry's only predictive diagnostic software for remotely diagnosing the health of wireless networks without requiring overlay sensors. With Service Assurance Manager, the network automatically performs predictive health checks and reports any issues before end users are impacted.

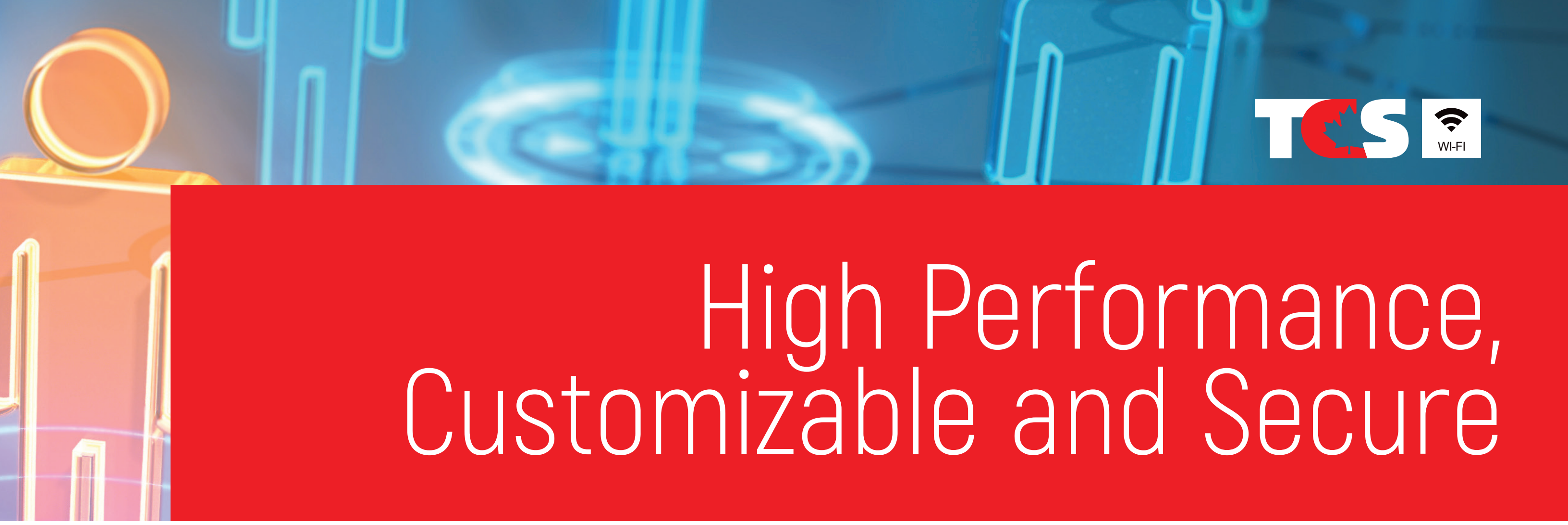
Service Assurance Manager creates network baselines and runs application-level tests continuously or on demand. It provides you with an executive summary of network operations through a simple dashboard.

Virtual Clients test for application performance from the client to the application server, without impacting users on the network. This approach enables Service Assurance Manager to proactively detect service failures that ordinary management software cannot – for example, if an antenna has fallen off an access point.

Many network issues require more detailed visibility. That used to require setting up an onsite test network, running diagnostic and performance tests, and analysing results on a variety of wireless security profiles. Service Assurance Manager uses the Virtual Client to automate these tasks remotely, providing visibility into network operations without the need to send IT staff and equipment onsite.

BENEFITS

- Dashboard with executive summary of network health lets you proactively detect network issues
- Remote diagnostic tests reduce onsite visits



High Performance, Customizable and Secure

- Fully integrated – no need for additional equipment
- Inject real, application-level traffic into the live network without disrupting service
- Identify root causes with automatic analysis of connection failure stage

WIPS

Fortinet Wireless Manager includes a signature-based Wireless Intrusion Prevention System able to detect and counter wireless security issues. Network administrators can customize the response to threats based on an organization's individual needs, as well as define new signatures and generate reports of all activity that affects security.

FORTINET AP SERIES

CONTROLLER-MANAGED ACCESS POINTS

Fortinet AP series Access Points (APs) provide a high-performance, premise-managed WiFi network with a broad range of 802.11ac Wave 1 and Wave 2 APs that ease deployment and scaling and offer a number of compelling quality-of-experience advantages. They also provide a complete portfolio of security services that offer additional means of protection to combat the ever-evolving threat landscape. Fortinet also offers an RF technology that uniquely manages the spectrum utilization, allowing it to dramatically simplify deployment vs competing solutions.

APPLICATION CONTROL

Provides administrators with Application Visibility to prioritize applications to improve the user experience by guaranteeing more capacity to select groups, such as mission-critical applications or mobile point-of-sale (mPoS) devices.

AIR TRAFFIC CONTROL

Provides sophisticated air traffic control mechanisms to govern station airtime so every client gets a fair turn on-air, which prevents the slowest, or the fastest, devices from hogging resources.

SINGLE CHANNEL TECHNOLOGY

Unique technology that manages spectrum utilization to overcome the interference-related deployment barriers commonly encountered in high density environments.

TCS WI-FI

TCS
Connected IT

TEL: 416-635-1234
TOLL FREE: 1-888-935-1234

7 KODIAK CRESCENT, TORONTO,
ONTARIO, CANADA M3J 3E5

SALES@TCSCANADA.COM
WWW.TCSCANADA.COM

Call today to learn how a TCS Wi-Fi solution can provide a secure Wi-Fi experience and superior threat protection.