



Fortinet Device and Technology Overview

Version 1.0

Prepared by Andy Memmott

December 2018

FortiGate: Next Generation Firewall (NGFW)

FortiGate Next Generation Firewall utilises purpose-built security processors and threat intelligence security services from FortiGuard labs to deliver top-rated protection and high performance including encrypted traffic. FortiGate reduces complexity with automated visibility into applications, users and network and provides security ratings to adopt security best practices.

In addition to content inspection, ALL FortiGate models offer a common feature set that includes; SSL & IPsec VPN, dynamic routing, traffic shaping, WAN load balancing, SD-WAN, FortiClient policy enforcement, Wi-Fi controller, switch controller, device identification & control and when multiple units are deployed high availability.

As of 10th August 2018, Fortinet were again named a leader in the 2018 Gartner Magic Quadrant for Enterprise Network Firewalls.



FORTIGUARD UNIFIED PROTECTION (UTM) BUNDLE

The FortiGuard Unified Protection (UTM) bundle is Fortinet’s traditional Unified Threat Management security bundle. The unified protection bundle extends threat protection across the entire digital attack surface, providing industry-leading defence against sophisticated attacks such as web and email-based attacks.

The UTM bundle includes: Antivirus, Antispam, Botnet, Content Disarm & Reconstruction, FortiSandbox Cloud, IP/Domain Reputation, IPS, Mobile Security, NGFW Application Control, Virus Outbreak Protection, Web Filtering, and FortiCare.

FORTIGUARD ENTERPRISE PROTECTION (ENT) BUNDLE

The FortiGuard Enterprise (ENT) Protection bundle is designed to address today's advanced threat landscape. The ENT bundle consolidates the comprehensive protection needed to protect and defend against all cyberattack channels from the endpoint to the cloud. It includes the technologies needed to address today's challenging Operational Technology, risk, compliance, and management concerns. The ENT bundle offers the most comprehensive protection overall.

The ENT bundle includes: all the UTM bundle features plus CASB, Industrial Security Service and Security Rating

FORTICARE

Available as 8x5 or 24x7 options, FortiCare covers the Fortinet hardware for extended warranty, firmware updates and technical support. RMA is offered as in country advanced replacement with the FortiCare 24x7 option.

FortiSwitch: Secure Access Switches

FortiSwitch Secure Access Series switches deliver superior security, performance, and manageability in a broad portfolio of secure, simple, and scalable Ethernet access layer switches. Tightly integrated into the FortiGate® Network Security Platform, the FortiSwitch Secure Access switches can be managed directly from the familiar FortiGate interface. This single pane of glass management provides complete visibility and control of all users and devices on the network, regardless of how they connect.

The Power over Ethernet (PoE) capability in some models, enables simple installation of wireless Access Points and IP phones in the network.

FortiSwitch includes:



Ability to enable security features to protect your infrastructure with no slow down



FortiLink facilitated provisioning and management through our industry leading FortiGate

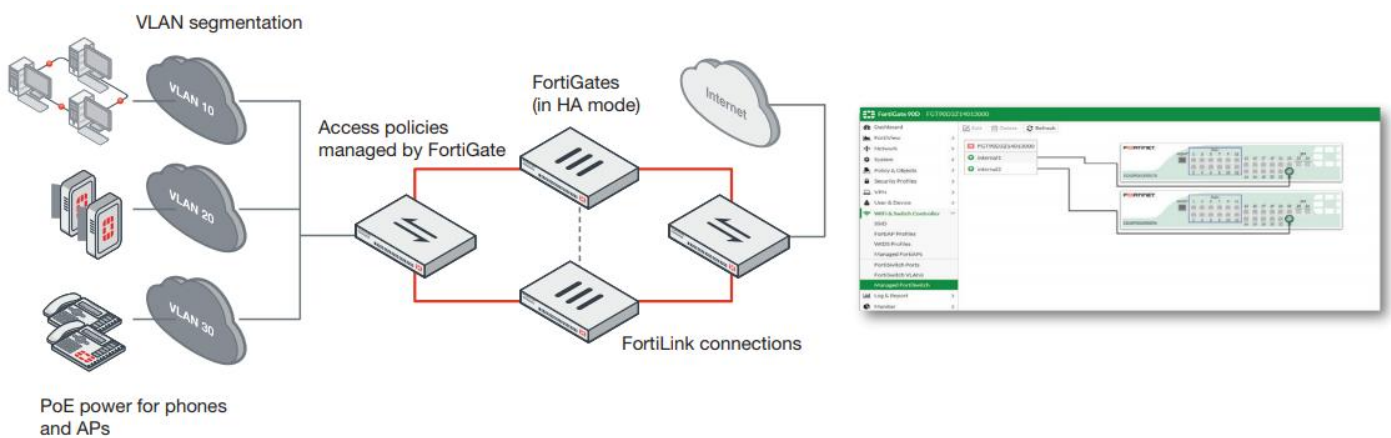


Network segmentation to help in data separation compliance



Capability to enable voice, data, and wireless traffic across a single network

The FortiSwitch Secure Access Switch series integrates directly into the FortiGate* Connected UTM, with switch administration and access port security managed from the familiar FortiGate interface. Regardless of how users and devices connect to the network, complete visibility and control over a network security and access through is presented through a single pane of glass, perfectly suited to security & threat sensitive network organisations of any size.



* Selected models only

FortiAP: Secure Wireless Access

The challenges associated with enterprise class Wi-Fi security continue to grow. With BYOD, a highly mobile workforce, and now IoT devices being brought into the business space, it's critical for IT organisations to manage their access while also dealing with evolving security threats. Fortinet offers a variety of wireless solutions, from management integrated into a FortiGate to dedicated WLAN controllers to ensure every user has the right solution for their network needs.

Fortinet's FortiAP series of access points support the latest technologies (802.11ac Wave2, 4x4), and the demand for plug and play deployment. FortiAPs are available in a variety of models to address specific use cases and management modes, including a Universal AP designed to operate with any on-premises or cloud solution.

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.

FortiAP 221E and 223E

Example multi-purpose AP



The FortiAP 221E and 223E are medium-density 802.11ac Wave 2 access points. These Enterprise-class access points are ideal for medium-density environments such as office or classroom with

Performance Throughput of up to 867 Mbps.



802.11ac Wave 2 | Dual Radio 2.4 and 5 GHz | 4 Internal/External Antennas

2x2 MU-MIMO | Up to 400 + 867 Mbps

FortiClient

The FortiClient software provides automated next-generation threat protection, visibility and control of your software and hardware inventory across the entire security fabric. FortiClient has a variety of features, including antivirus, web filtering, firewall, and parental controls, to individual computers and mobile devices. It can also be used to connect to a FortiGate using either an SSL or IPsec VPN.



FortiClient is available for Windows, Mac OSX, iOS, and Android, and can be set up quickly. After being installed, it automatically updates its virus definition files, does a full system scan once per week, and much more.

- ✓ Provides Endpoint Visibility & Compliance throughout security fabric
- ✓ Prevent Known Vulnerabilities from Being Exploited by Attackers
- ✓ Automated behaviour based protection against unknown threats
- ✓ Simplified Endpoint Management

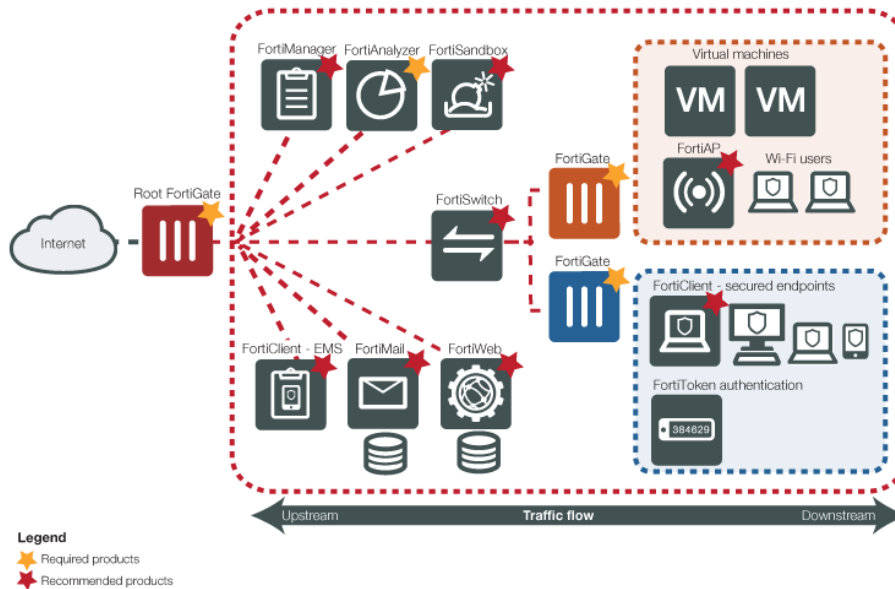
FortiClient is a top performer and "Recommended" by NSS labs in its 2018 Advanced Endpoint Protection (AEP) group test. NSS Labs expanded the scope of the AEP test and included malware, exploits, blended threats (combinations of threats), false positives, and evasions. FortiClient with integrated Sandbox blocked 100% exploits, 100% document and script-based attacks; 100% web and email attack, and offline threats with zero false positives.

As a key piece of the Fortinet Security Fabric, FortiClient integrates endpoints into the fabric for early detection and prevention of advanced threats. Security events including zero-day malware, botnet detections, and vulnerabilities are reported in real-time.

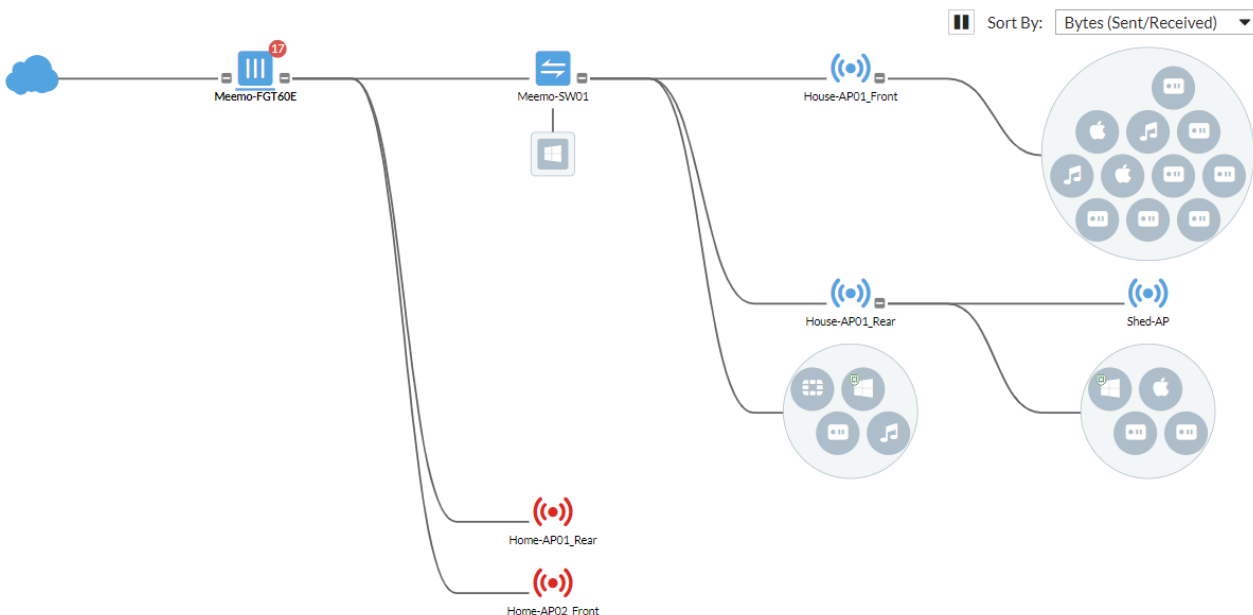
The deep real-time visibility into the network allows administrators to investigate and remotely quarantine compromised endpoints. Endpoint protection is more than just antimalware protection, the endpoint compliance and vulnerability detection features enable simplified enforcement of enterprise.

Fortinet Security Fabric

The tight integration between FortiGate appliances at the core of the network, FortiSwitch devices, and FortiAP Wireless Access Points enables a common security policy across the network, extending the protection of the firewall out to the edge.



With one operating system across the entire network, you get better visibility and awareness with simplified management.



The Fortinet Security Fabric delivers broad protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises. Automatically synchronise your security resources to enforce policies, coordinate automated responses to threats detected anywhere in your network, and easily manage all your different security solutions and products through a single console.

References

<https://www.fortinet.com/products/next-generation-firewall.html>

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf>

<https://www.fortinet.com/solutions/enterprise-midsize-business/security-fabric.html>

<https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-fortiguard-labs-services-bundles.pdf>

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11ac_Series.pdf

<https://www.fortinet.com/products/secure-switching/secure-access-switches.html>

<https://www.fortinet.com/content/dam/fortinet/assets/brochures/FortiCare-Services.pdf>

<https://www.fortinet.com/products/secure-wifi.html>

<https://www.fortinet.com/products/secure-wifi/access-points.html>

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSwitch_Secure_Access_Series.pdf

<https://www.fortinet.com/solutions/enterprise-midsize-business/secure-unified-access.html>

<https://forticlient.com/>

<https://cookbook.fortinet.com/forticlient/>

<https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiClient.pdf>