Fortinet UTM Solution Guide

THE LEADER IN UNIFIED THREAT MANAGEMENT

Introduction to UTM

The broad adoption of networking across small to mid-size enterprises, coupled with the explosion of mobile devices and applications, has accelerated the requirement to add network security to even the smallest network. Threats from hackers, sophisticated malware, botnets, and advanced persistent threats underscore the need to deploy and enforce security controls.

Fortinet pioneered the concept of Unified Threat Management (UTM) – consolidating multiple network security functions into a single device. UTM provides large and small organizations with a cost-effective and simplified way of dealing with today's sophisticated, evolving security threat landscape.

Essential UTM Elements

UTM is generally considered a 'superset' of Next-Generation Firewall capabilities. Though the definition of UTM has grown and evolved over time, the following are just some of the essential UTM network security functions.

Firewall: The inspection of inbound and outbound traffic on a network, allowing safe traffic to pass while blocking unsafe traffic.

VPN: A Virtual Private Network extends a private network across a public network. VPNs allow employees, for example, to securely access their company's network while outside the office.

IPS: Intrusion Prevention Systems monitor, log, identify and (optionally) stop malicious network activity.

Application Control: The ability to identify and control applications on networks and endpoints (PC, smartphones and tablets, etc.) regardless of the port, protocol, or IP address used.

Web/Content Filtering: Explicitly allowing or blocking web site traffic, based on a number of configurable parameters such as reputation and/or category of the web site visited.

AntiMalware/AntiVirus/AntiSpam: Typically provides real-time protection against malicious software being installed on a system.

Advanced Threat Protection: Advanced Persistent Threats (APTs) target specific people or functions within organizations, infiltrate from multiple vectors (fishing attacks, web drive-bys, etc.) and use extensive evasion techniques to remain stealthy for long time periods before exfiltrating data. Advanced Threat Protection is a set of sophisticated techniques designed to identify and stop APTs.

Integrated Wireless LAN Controller: Enables and manages the transmission of wireless data across a network.

Fortinet Protects while Lowering Costs

UTM is the most effective way for small-to-mid size organizations to manage the latest security threats while significantly lowering costs. In order to address the entire threat landscape, a vendor must provide comprehensive security protection – as previous outlined – as well as end-to-end wired and wireless security policies, centralized logging and management, and have advanced threat research capabilities to keep organizations protected ahead of the latest threats. Fortinet is the only vendor that provides all of these capabilities.

By combining and consolidating key network security functions into a single appliance or platform, users can achieve significant cost savings. Fortinet

takes this one step further. By having the fastest performing security platforms on the market, coupled with in-house threat research and development, Fortinet provides the lowest total cost of ownership in the UTM market space.

FortiGate, the Leading UTM Platform

FortiGate

The award-winning FortiGate Network Security Platform delivers unmatched performance and protection while simplifying your network with broadest range of network security and services on the market, including: firewall, VPN, traffic shaping, IPS, antimalware, application control, data loss prevention, vulnerability management, etc., all centered on a single platform. Fortinet offers models to satisfy any deployment scenario, from the desktop series for small offices and retail networks to the chassis-based FortiGate-5000 series for large enterprises, service providers, data centers and carriers. FortiGate platforms integrate the purpose-built FortiOS™ operating system with custom FortiASIC™ processors and the latest-generation CPUs to provide comprehensive, high-performance security.

FortiOS

FortiOS is a security-hardened, purpose-built operating system that is the foundation of all FortiGate® network security platforms. Building on Fortinet's history of innovation, FortiOS includes over 150 standard features, as well as new enhancements to help fight security threats, simplify deployments, and enhance security reporting and management.

FortiOS 5 includes a new, advanced anti-modern malware detection system for identifying and mitigating Advanced Persistent Threats. Together with superior, industry-validated AV signatures, FortiOS 5 delivers a multi-layered approach to mitigating today's most dangerous security threats, including:

FortiGuard Antivirus Engine, which identifies standard AntiVirus threats, and also uses advanced heuristics and "sandboxing" to determine malicious behavior.

FortiGuard Analytics, which identifies suspicious zero-day (unknown) malware for further analysis in the cloud.

FortiGuard Botnet Database, which contains up-to-date information about IP reputations and prevents remote command and control communications.

Fortinet Web Filtering, which uses URL matching and advanced DNS-based web filters to identify potentially harmful websites.

FortiASIC

Traditional Security Appliances use multi- purpose CPU based architectures, which can quickly become network bottlenecks. The only way for a network security platform to scale is via purpose built ASIC[1]s that accelerate specific parts of the packet processing and content scanning functions. FortiASICs are used to scale from 20Mbps to 500Gbps of Firewall throughput independent of packet size, and while maintaining a high number of sessions and low latency. For the best price performance, FortiGate UTM desktop models use specialized ASICs known as System on a Chip (SOC2) technology. Another benefit of the ASIC technology is the ability to run multiple security applications without degrading performance.

FortiGuard Labs

The FortiGuard Labs team consists of over 175 researchers and analysts dedicated to covering the entire threat spectrum. The researchers work with world class, in-house developed tools and technology to study, discover and protect against breaking threats. The FortiGuard Labs team develops the content for the FortiGuard Subscription Services, which is available to all FortiGate platforms. Through these Subscription Services, customers can rest assured their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security technology The FortiGuard security team continually

[1] Application-Specific Integrated Circuit

develops new attack filters to address the latest vulnerabilities and incorporates these filters into security signatures. Signatures are created not only to address specific exploits, but also potential attack permutations, protecting customers from zero-day threats. Signatures are delivered to customers on a regular basis – twice a day for IPS, four times a day for antivirus, and automatically for antispam and web threats, with no user interaction required. This constant updating against both the most prevalent and unexploited threats provides world-class protection to Fortinet customers.

Conclusion: Why Select Fortinet for your UTM?

Fortinet is the only vendor providing a full and comprehensive UTM solution. The FortiGate network security platform is the core of Fortinet solutions and provides the highest level of security, integrity and management.

Fortinet is recognized by IDC as the worldwide #1 leader in the UTM (Unified Threat Management) market and by Gartner as the leader in their UTM Magic Quadrant[2].

The FortiGate network security platform delivers the integrated, consolidated security every organization needs to fortify their wired and wireless networks. With FortiGate, users can quickly and easily add core security services such as firewall, VPN, application control, antivirus, intrusion prevention (IPS), and web filtering which reduce the risk of unauthorized access, data loss, or damage to critical systems. Fortinet delivers complete, end-to-end UTM security, from the mobile endpoint to the network core.

[2] Gartner “Magic Quadrant for Unified Threat Management” by Greg Young and Jeremy D’Hoinne, July 19, 2013