Fortinet's Solution for the Enterprise Campus
High Performance Next Generation Firewall

Introduction

Today's enterprises are increasingly looking to upgrade security at the edge of their networks. This upgrade is not just to match higher network speeds with higher security performance but also to introduce a deeper level of inspection, beyond traditional port and protocol firewalls, for greater visibility into and control over network traffic.

This guide discusses the major trends behind this desire to upgrade and demonstrates how Fortinet's next generation/edge firewall solution, with its multiple deployment personalities, can help you meet the corresponding security requirements that allow you to enable your employees yet secure your enterprise.

Market Trends Affecting the Enterprise Edge

- **Consumer grade technology in the workplace** – Smartphone and tablets, social media and other Internet-based applications, cloud-based storage and services. All are increasingly used for corporate purposes, and all create new opportunities and security challenges.
- **More sophisticated threats** – Today's highly targeted, highly tailored attacks are often specifically crafted (and even tested) to bypass traditional defenses.
- **Complexity** – New security technologies address new challenges, but carry deployment and management burdens.

What this Means for Security Requirements

1. In response to consumer-grade technologies in the workplace, enterprises need fine-grained visibility and control to manage the risk to tthe enterprise.
2. As threats increase in sophistication (with an emphasis on beating established security techniques), new inspection methods that focus on activity rather than attributes are needed.
3. As more business-enabling technologies are embraced at the same time that newer security technologies are being considered to address emerging threats, consolidation of functions becomes essential.

Benefits

- High performance "next generation" visibility and control enables yet secures the enterprise

- Extensibility to add secure web gateway or advanced threat protection capabilities simplifies increased security

- Rich reporting delivers actionable intelligence to establish/enforce appropriate policies and address advanced persistent threats

- Purpose built appliances with custom ASICs deliver best in class performance per security dollar

FÜRTINET

Solution for the Enterprise Campus

Fortinet consistently offers the highest performance appliances in a price band, with flexible software platforms that enables them to be deployed in many different "personalities" (combinations of functions).

Feature Select Allows Simple Configuration of FortiGate

Next Generation Firewall

The foundation of the enterprise campus offering is a high performance next generation firewall (NGFW) that adds intrusion prevention, application control and antimalware to the traditional firewall/VPN combination.
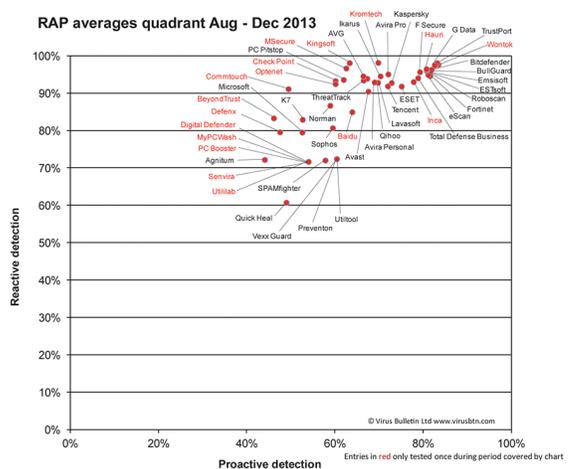
In particular, Fortinet NGFWs:

- Provide fine-grained, user – or device-based visibility and control over more than 3000 discrete applications to establish/enforce appropriate policies
- Include powerful intrusion prevention, looking beyond port and protocol to actual content of your network traffic to identify and stop threats
- Leverage top rated antimalware to proactively detect malicious code seeking entry to the network
- Deliver actionable application and risk dashboards/ reports for real-time views into network activity
- Run on purpose-built appliances with Custom ASICs for superior, multi-function performance, even over encrypted traffic
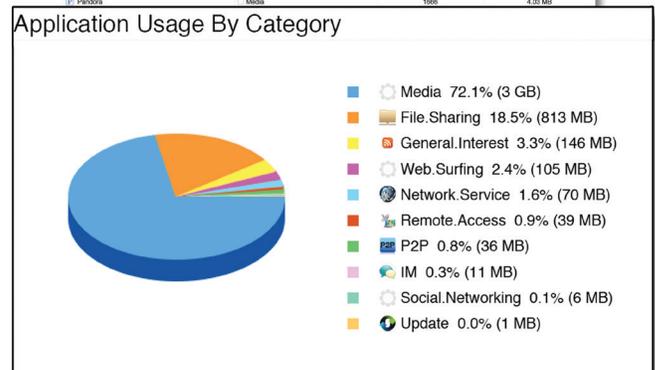
Granular Application Visibility and Control

Three common reasons we hear customers deploying FortiGate as an NGFW:

We gave iPads to the executives and they have started using all kinds of applications which we have to allow unless they constitute a clear risk to our organization.

We have seen the security breaches in the industry and we need to upgrade our traditional firewalls to improve our threat protection.

We bought IPS but it was too complicated to deploy and manage effectively so we want to move to a consolidated NGFW before our expensive IPS renewal.

Top-rated Antimalware

Actionable Reports

NGFW+Advanced Threat Protection

While upgrading to a next generation firewall will certainly improve enterprise security, there is a growing recognition that there is an evolving class of highly targeted, highly tailored attacks that are specifically designed (and often tested) to bypass established defenses.

Extending FortiGate with Advanced Threat Protection
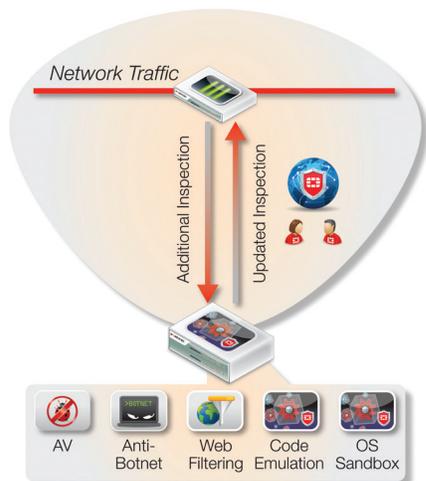
Leveraging security signatures, patterns, heuristics and reputation is necessary to deal with the wide range of threats today, however they all require a degree of prior knowledge about the attack or attack class. As a result, organizations are looking to complement these defenses with additional analysis that can assess the actual activity of suspicious or high risk objects in a contained environment and get updated protections in place (based on the new threat information exposed) to mitigate the impact of previously unknown attacks.

In addition to the core Fortinet NGFW features described above, the following Advanced Threat Protection capabilities can be added to a FortiGate deployment:

- Unique dual-level sandboxing to examine code activity in simulated and virtual environments detect previously unknown threats
- Rich reporting on system, process, file and network behavior, including a risk rating
- Web filtering, botnet and call back detection to prevent communication with malicious sites and IPs
- Option of sharing threat information with FortiGuard labs to receive updated in-line protections
- Option of integrating with FortiGate and FortiMail products for simpler deployment

FortiSandbox is a natural extension to your Fortinet next generation firewall.

Next Generation Firewall + Authentication

With many organizations relinquishing control over the end user device, either supporting smartphones and tablets or moving to full BYOD, authentication of the user, becomes essential. Further, in given the sophistication of threats noted earlier, there is growing need for two-factor or "strong" authentication. And in light of the complexity and desire for consolidation, many organizations are looking to extend their network security visibility with the control over user access.

In addition to the core NGFW capabilities noted the following strong authentication functions can be enabled:

- Hardware, software, email and SMS tokens
- Integration with LDAP, AD and radius
- End user self-service
- Certificate Authority
- Single sign on throughout the network
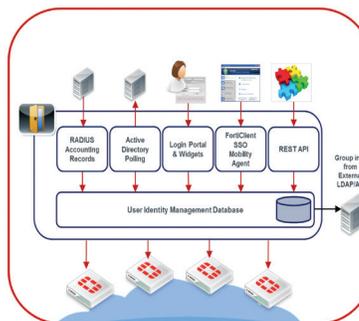
Next Generation Firewall + Secure Web Gateway

Given the transformation of IT – supporting more devices, applications and services- as well as evolution of the threat landscape requiring the addition of new security technologies, organizations with relatively constrained staff and budgets are looking to consolidate mature functions in order to free up resources for newer ones. The most common consolidation for enterprises is adding Web Filtering along with the IPS, Application Control and Antimalware of the NGFW in order to replace existing Secure Web Gateways, remove unnecessary appliances and avoid expensive renewals.

In addition to the core Fortinet NGFW features mentioned earlier, organizations looking to consolidate Secure Web Gateway functions can take advantage of:

- Dynamic web filtering covering over 56 million rated sites across 79 categories
- Flexible policy engine including support for Usage Quotas, User Override and more
- Central management and reporting to simplify administration

FÜRTINET.

The Fortinet Difference – Custom ASICs, Unmatched Performance

At the heart of the FortiGate next generation firewalls are purpose-built FortiASIC processors (describe in detail below) that enable high performance required for the deeper level of "next generation" inspection as well as the consolidation of multiple security functions onto a single appliance.

Further, our integrated architecture provides extremely high throughput and exceptionally low latency, minimizing packet processing while accurately scanning the data for threats.

Dedicated ASICs versus CPU Architectures
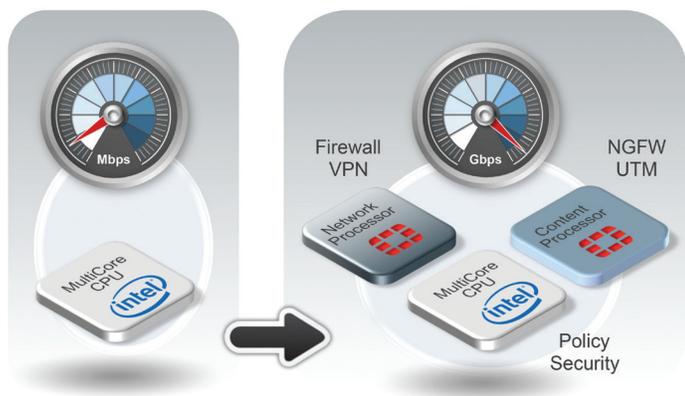
Traditional Security Appliances that use multi- purpose CPU based architectures becomes an infrastructure bottleneck. Even when using multiple multi-core general purpose processors, network security devices cannot deliver the high performance and low latency required.

The only way for a Network Security Platform to scale is via purpose-built ASICs to accelerate specific parts of the packet processing and content scanning functions. FortiGate technology utilizes optimum path processing (OPP) to optimize the different resources available in packet flow. The FortiASIC utilized by the latest FortiGate Next Generation Firewall models are:

- Content Processor (FortiASIC CP8) – Accelerated content security such as Antimalware, VPN encryption/ decryption and Authentication processing

- Network Processor (FortiASIC NP6) – Accelerated network security tasks such as Firewall, VPN and IPv6 translation

As a result, organizations can deliver low latency end while still improving security and consolidating functions. A win for everyone

Summary

Today's enterprise is undergoing a significant transformation, with increasingly tech-savvy employees taking advantage of the latest "consumer-grade" technologiesto become more agile and efficient.

However, these technologies represent a business risk as well as opportunity, especially given an evolving threat landscape and the rise of highly targeted and tailored attacks. In response, enterprises are upgrading from traditional to next generation firewalls for the visibility and control required to allow the use of these new technologies in a secure manner. Furthermore, many organizations are looking to add Advanced Threat Protection technologies as an extension of their NGFW and/or consolidate other network security appliances like Secure Web Gateways for more manageable and cost- effective IT security.

Fortinet built the FortiGate line of Network Security Platforms, and the accompanying management and reporting tools, to meet the demanding security and IT needs of enterprises with unmatched performance per dollar spent.

For more information on the FortiGate Network Security Platforms, please go to
http://www.fortinet.com/solutions/enterprise.html.

FÜRTINET.