Fortinet's Data Center Solution

High Performance Network Security

Introduction

The data center is the focal point of several trends in computing and networking that are driving rapid change to the overall IT infrastructure strategy for many organizations as well as the requirements for data center security.

This guide discusses these trends and demonstrates how Fortinet's data center security solutions can help you meet the corresponding security requirements to take advantage of the opportunities presented by these trends.

Market Trends Affecting the Data Center

- **Mobility and BYOD –** Smartphone and tablets are increasingly being used by employees, customers and end-users to consume data and services. This explosion of anytime, anywere data consumption has driven the need for greater network speeds in the data center, but also increased risk exposure of sensitive data to unauthorized access outside of corporate boundaries.
- **Server Virtualization and Data Center Consolidation –** As multiple physical systems were efficiently combined with server virtualization such as VMware, core network traffic density increased from first server consolidation and later even consolidation of multiple data centers. As IT efficiency reduced new server provisioning from months to mere days, it enabled further business productivity driving further increases in network traffic and utilization.
- **Cloud Computing and Software Defined Networking –** As organizations of all sizes utilize public and private cloud services, data centers have to evolve to support multi-tenancy, infrastructure orchestration, seamless integration with third party application services and greater access by external parties. This dynamic environment becomes even more fluid as control of the networking function is separated from its physical hardware for greater flexibility, speed, and agility. This enables increased business agility, but also with operational risk that sensitive data and assets will be more exposed to unintended access in shared, external computing environments.

Highlights

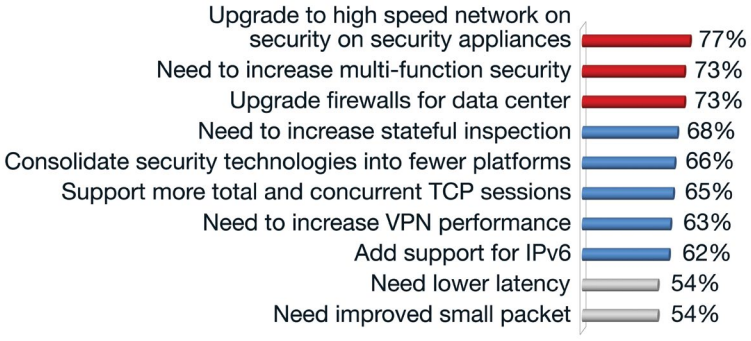
- High performance, high capacity, and ultra-low latency
- Cloud-ready multi-tenant support and virtual domain support for network segmentation
- Flexibility to enable the firewall personality you need to match your environment with edge or core deployment, network segmentation, or integrated security technologies
- Single-pane-of-glass management for unmatched visibility and control
- Single security platform delivers all needed data center services
- Lower TCO, improved projection, increased performance
- Unmatched flexibility of deployment with appliance, chassis, and virtual machine options

These trends are driving, if not accelerating an ongoing Moore's Law effect of core network speeds doubling every 18 months. This is not just in the refresh of the data center network switching and routing fabric, but also in the firewalls and network security appliances needed, more than ever, to secure data and IT assets in these dynamic, multi-tenant environments spanning on-premise and external cloud resources.

In fact, Infonetics Research found in a recent survey of decision-makers of large organizations of over 1,000 employees that most are looking for:

- Faster firewalls with 100+ Gbps aggregate throughput
- High-speed ports to interface to their core network fabric (40G and 100G) to
- Better performance of their multi-function security technologies
- The ability to deploy additional security services without affecting performance

Survey: 73% of respondents want to upgrade their data center firewalls.



Source: Infonetics High End Firewall Survey 2013

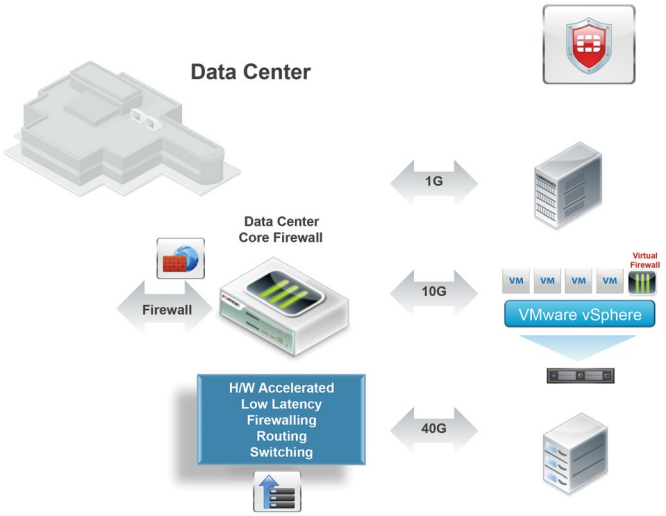
What this Means for Security Requirements

1. **Performance –** As networks continue to accelerate, the data center is at the forefront of the requirement to support higher performance and need high-speed, high-capacity, and low latency firewalls.
2. **Segmentation –** As data centers have become more dynamic, organizations are embracing increased network segmentation as a best practice to isolate data based on applications, user groups, regulatory requirements, business functions, trust levels, and locations. As a result, firewalls need to provide high port density and logical abstraction to support both physical and virtual segmentation across private and public clouds.
3. **Simplification –** As these datacenters extend to external parties of varying trust levels, organizations need to consider a "Zero-Trust" model for data access that drives multiple security functions from traditionally just the data center edge more deeply into fine-grained segmentation throughout the core of the network. This requires a consolidated security platform that can support high speeds even as many functions are turned out at each micro-perimeter.

Fortinet's Data Center Solution

Fortinet has been a leader in securing data centers for over 10 years. Our high-performance, low-latency chassis and appliance-based solutions have protected many of the largest data centers in the world. Fortinet customers are focused on very high throughput and ultra low latency to meet increasing data center core network speeds.

Data Center Core Firewall



To meet these performance demands, FortiGate platforms deliver some of the highest throughputs and lowest latencies on the market, several with over 100 Gbps aggregated performance and sub-5 µs latency.

This high performance enables organizations to implement the network segmentation discussed earlier to support regulatory compliance, function, location or trust level.

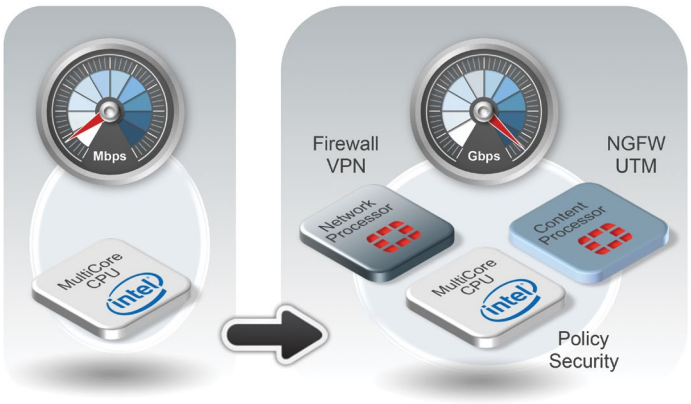
The Fortinet Difference — Purpose built appliances, custom ASICs

At the heart of the FortiGate Date Center firewalls are purpose-built FortiASIC processors (describe in detail below) that enable this extremely high level of performance. These custom content and network processors provide near-wire speed switching, routing, and stateful firewalling.

The network processors eliminate the need for legacy L2 switches and routers within the datacenter. Instead, FortiGate takes over and performs network segmentation, switching, routing, and network security, all while reducing network complexity.

Furthermore, our integrated architecture provides extremely high throughput and exceptionally low latency, minimizing packet processing while accurately scanning the data for threats. Custom FortiASIC™ processors deliver content inspection at multi-Gigabit speeds.

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 in data center deployments.

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 function. FortiGate technology utilizes optimum path processing (OPP) to optimize the different resources available in packet flow.

The FortiASIC can scale to 500 Gbps of Firewall throughput independent of packet size while maintaining a high number of sessions and extremely low latency. The FortiASIC utilized by the FortiGate Firewall models are:

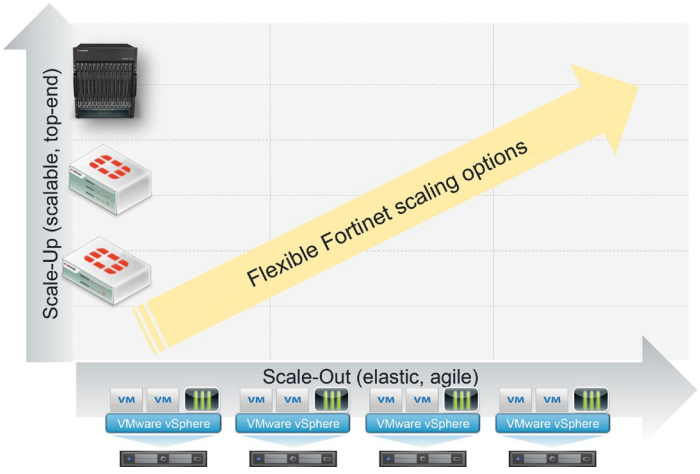
- Content Processor (FortiASIC CP8) - Accelerated content security such as antimalware, VPN encryption/ decryption and authentication processing
- Network Processor (FortiASIC NP6) – Accelerated network security tasks such as Firewall, VPN and IPv6 translation

Scale-Up and Scale-Out for Virtual and Cloud Environments

FortiGate hardware solutions provide scale-up performance for data centers of all sizes with a range of appliance and chassis form factors ranging from 20 Gbps up to an industry-leading 560 Gbps blade-in-chassis. These provide attractive performance, TCO and flexibility in a single unit for organizations ranging from mid-sized to larger enterprises, and to telco/carrier segments.

In addition to providing efficient scale-up performance in compact appliance and chassis options, FortiGate also provides equally critical scale-out performance through FortiGate-VM virtual appliances that provide agile capacity that can deploy elastically with virtualization hosts or cloud infrastructure to provide unlimited scalability through a distributed approach with dozens if not hundreds of virtual security appliances across both private and public clouds.

FortiGate Performance – Physical and Virtual



FortiGate-VM virtual appliances, along with nearly a dozen other Fortinet solutions available as virtual machines, support major enterprise hypervisors from VMware vSphere to Hyper-V, Xen, and KVM, as well as leading cloud service providers ranging from Amazon Web Services to major telecom public cloud offerings.

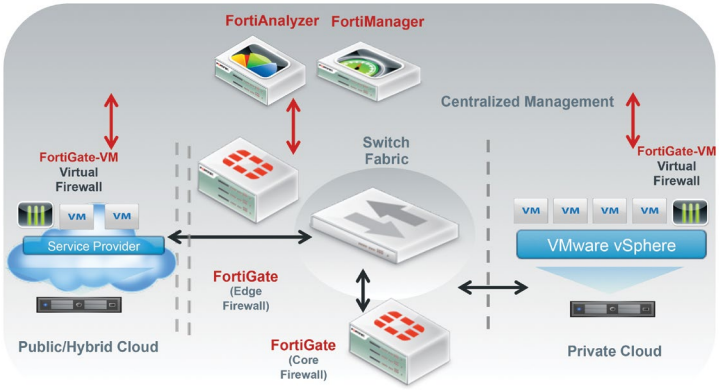
Unique virtual domain (VDOM) technology along with virtual LAN (VLAN) support provide ability for both FortiGate appliances to manageably scale in multi-tenant private or public cloud environments. Long used in large-scale managed service environments, VDOM's can divide a single larger physical (or even virtual) FortiGate appliance into dozens, if not hundreds of logical independent instances, to flexibly provide either isolated or coordinated firewall policies and security configurations to individual tenants.

Single Pane-of-Glass Management Across Hybrid Clouds

Fortinet's complementary management solutions ensure coordinated security policy across hundreds of physical and virtual FortiGate appliances, whether solely within an internal data center, extending the private cloud to an external public cloud, or across multiple public clouds. With a single, centralized platform for defining firewall rules and security policies and to aggregate and analyze logs and events, FortiManager and FortiAnalyzer ensure a consistent security posture across the hybrid cloud regardless of where workloads instantiate, migrate, or fail over.

FortiManager and FortiAnalyzer themselves can even run as virtual appliances in a private or public cloud, leveraging the benefits of cloud-based security management, such as for scale-out log aggregation and analytics capacity or ubiquitous administrative access.

Single Pane of Glass Management Across Hybrid Cloud



Summary

The data center is one of the most dynamic aspects of network security today. As significant trends in computing and networking continue to drive changes in many critical business practices, organizations look for innovative network security solutions to help them embrace those changes. Fortinet's FortiGate Network Security Platform can provide the backbone of your Data Center strategy. Fortinet's industry-leading, high capacity Firewall technologies deliver exceptional throughput and ultra-low latency, enabling the security, flexibility, scalability and manageability you demand across physical, virtual and cloud environments.

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

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

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