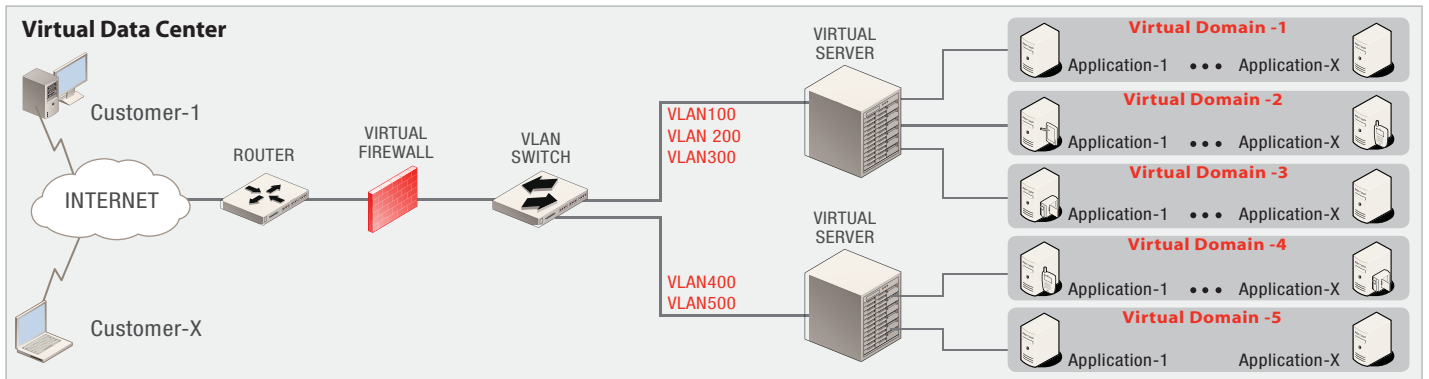


Securing Virtual Networks

**Scalable
Virtualized
Security Solutions**

The Benefits of Virtual Networking

Virtual networking provides a method to consolidate multiple devices, such as those typically found in a data center, in order to simplify and reduce physical hardware requirements. Implementing virtual networking technologies allows a single network device to transparently host multiple networks or customers on a common infrastructure. Implementing Virtual Local Area Networks (VLANs) allow network links to be shared by virtualized servers to help improve network performance, reduce management complexity and enable more granular usage policies.



Overview of Virtual Domains (VDOMs)

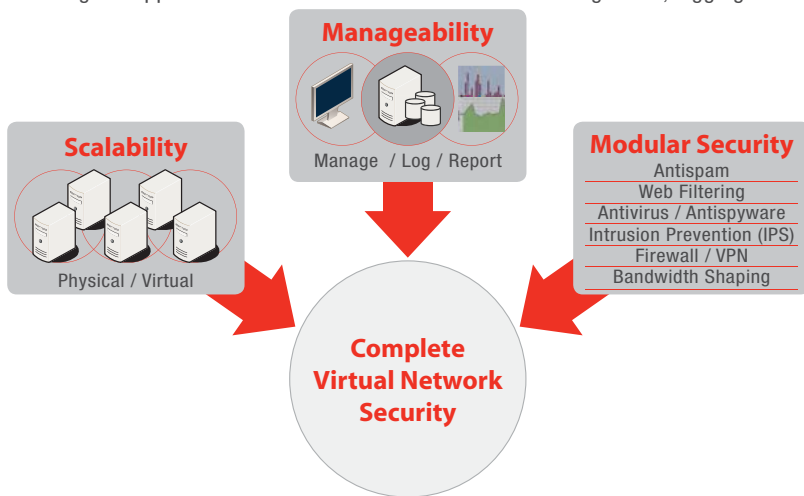
VDOMs enable the capability to use a common infrastructure to provide routing and network protection for several organizations or customers. This is useful for enterprises and service providers, where each organization requires its own network interfaces (physical or virtual), routing requirements and network protection rules.

Overview of Virtual LANs (VLANs)

VLANs allow a single physical trunk to support up to 4096 virtual networks. Using virtual networks allow a single trunk to support multiple customers and applications while providing a method to manage traffic and network performance. Routing between VLANs and between VDOMs adds more flexibility and scalability.

Challenges in Virtual Network Security

The primary reasons for implementing VDOMs and VLANs are to improve network manageability, scalability and security. Security solutions for virtual networks must allow management on a per-customer or per-application basis. Also required is a high-performance security platform that is capable of scaling to support thousands of virtual networks with management, logging and reporting customized for each customer or application.



Virtual Network Security Requirements

Manageability

Manage multiple domains and multiple networks from a single device with domain specific administrative profiles for log data, reports, alerts, options and menus

Scalability

Provides the performance to support thousands of VDOMs and VLANs without impacting overall network throughput, specific users or applications

Modular Security

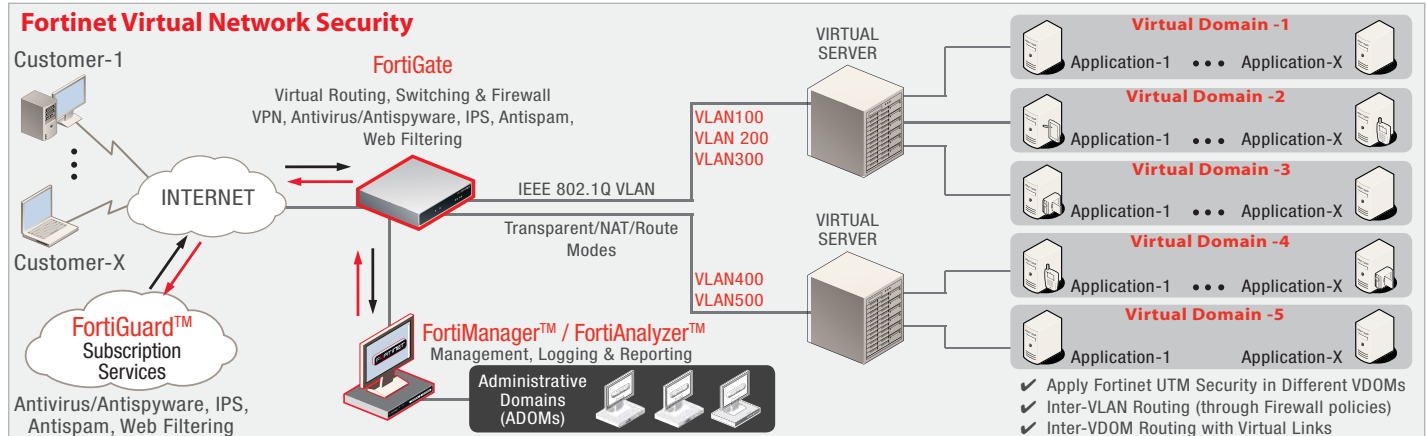
Requires a complete security suite where specific solutions can be applied on a per customer or per application basis while providing a low cost of ownership

The Fortinet solution is surpassing our high expectations and demands. Though we were seeking a performance and throughput improvement, we now also have less appliances to manage, 24/7 availability even if a data center goes down and a way to report on network usage without taking the entire network down.

*- Brian Bernard, Senior Network Administrator
Lee County Clerk of Courts*

Fortinet Unified Threat Management (UTM) Solutions for Virtual Networks

Virtual Domains provide a way to divide your FortiGate™ unit and operate it as multiple unique security domains. You can configure and manage interfaces, VLAN sub-interfaces, zones, firewall policies, routing and VPN configurations as if they were being applied to a dedicated security appliance. This virtual domain separation simplifies configuration because it reduces the number of separate routers or firewalls that must be managed. Support is provided for IEEE 802.1Q Virtual LAN tagging operating in both NAT/Route and Transparent modes, which allows administrators to increase the number of network interfaces beyond the physical interfaces. This allows a single FortiGate device to provide security services and control virtual networks across multiple security domains.



Fortinet Administrative Domains (ADOMs)

- ✓ Each ADOM is independent of other domains
- ✓ Manage all domains/devices from a single user interface
- ✓ Administrative access profiles (logs, reports, menus, etc.)

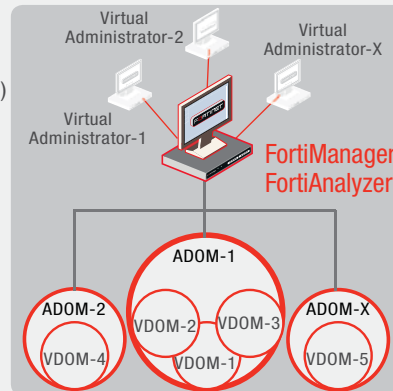
Fortinet VDOM Security

- ✓ Common or unique administrators for each VDOM
- ✓ Firewall policies between VDOMs & VLAN subinterfaces
- ✓ Unique security configurations across different VDOMs

Fortinet VDOM / VLAN Networking

- ✓ IEEE 802.1Q VLAN Layer-2 switching & Layer-3 Routing
- ✓ Supports Transparent/NAT/Route modes per VDOM
- ✓ Inter-VLAN Routing (all traffic through firewall policies)
- ✓ Inter-VDOM routing with virtual links

Complete Managability



Cost-Effective Scalability

All FortiGate Models Include 10 VDOMs

FortiGate-3000 Series Support up to 250 VDOMs*

FortiGate-5000 Series Support up to 3500 VDOMs*

** Purchased in 25 VDOM increments*

Fortinet Platforms

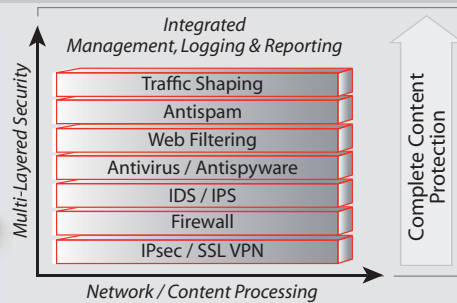
Protection, Management & Reporting



- Turn-Key Security Platforms
- Perimeter / Edge / ROBO Deployments
- Device Based Licensing (Not Per User)

FortiOS™

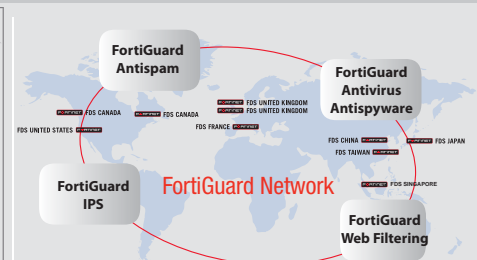
Modular Multi-Threat Security



- Modular Multi-Threat Security Suite
- Hardware Accelerated Performance
- Multiple Management & Reporting Options

FortiGuard Services

Security Update Development / Distribution



- Global Network of Distribution Servers
- 24x7 Dedicated Threat Research Teams
- Industry Leading Coverage and Accuracy

FORTINET

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700
Fax +1-408-235-7737
www.fortinet.com/sales

EMEA SALES OFFICE-FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33-4-8987-0510
Fax +33-4-8987-0501

APAC SALES OFFICE-HONG KONG

Fortinet Incorporated
Room 2429-2431, 24/F Sun Hung Kai Centre
No.30 Harbour Road, WanChai, Hong Kong
Tel +852-3171-3000
Fax +852-3171-3008