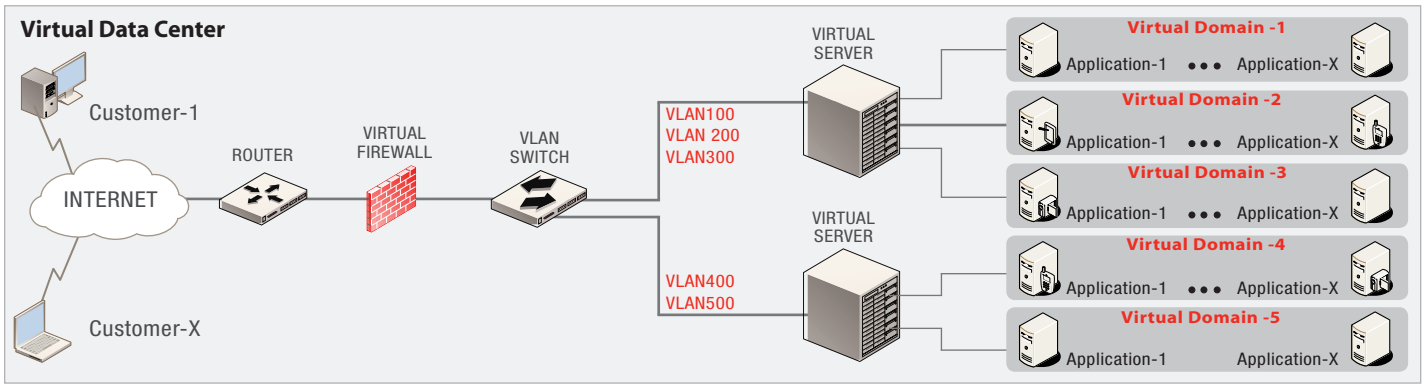
Secure Virtualization Solutions

Partner Solutions

VMware and Fortinet Partnership

VMware and Fortinet have partnered to provide market-leading solutions for protecting virtual infrastructures within data centers. VMware is the global leader in virtualization solutions enabling organizations to aggregate and virtually share network resources, resulting in reduced complexity and costs through consolidating IT infrastructure. Fortinet is the leading provider of ASIC-accelerated unified threat management (UTM) solutions that provide a comprehensive suite of security services at the highest levels of network protection and performance. Together, VMware and Fortinet deliver the highest performing, most advanced and flexible solutions while achieving significant cost savings through IT consolidation and simplified provisioning and management.



Overview of Virtual Domains (VDOMs)

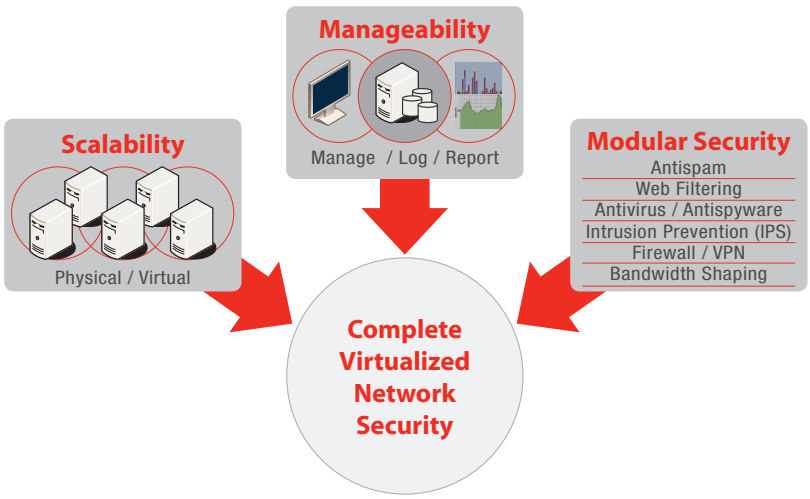
VDOMs enable the capability to use a common infrastructure to provide routing and network protection for several organizations or customers. This is useful for enterprises and service providers, where each organization requires its own network interfaces (physical or virtual), routing requirements and 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. By routing between VLANs and between VDOMs, increased flexibility and scalability can be achieved.

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 from a single device with domain-specific administrative profiles for system configuration, security policies, logging and reporting, etc.

Scalability

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

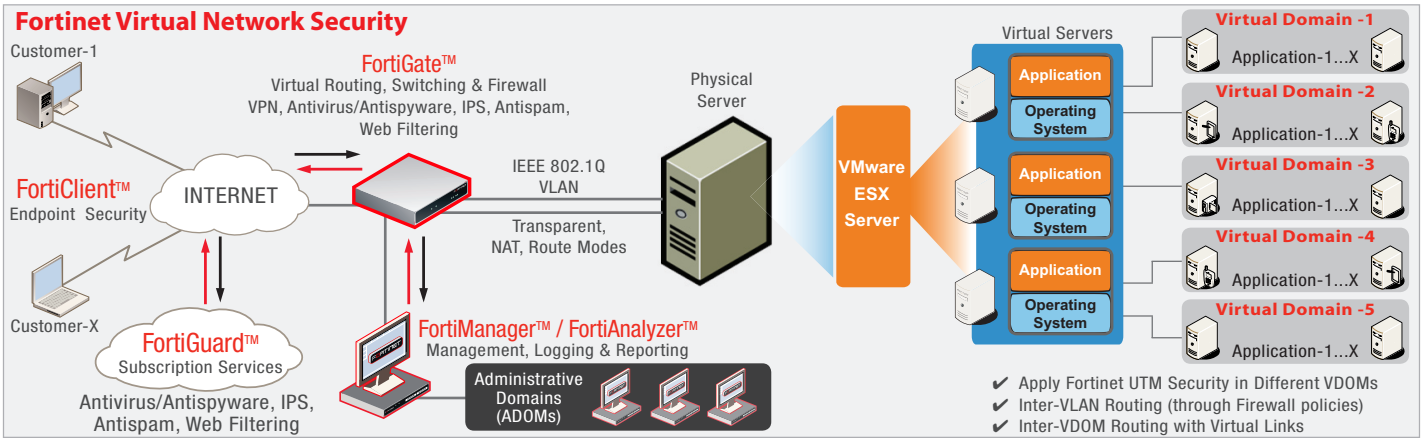
Modular Security

Offer a comprehensive security suite where desired features can be applied on a per-customer or per-application basis, all at a low total cost of ownership.

Solutions for Security and Network Virtualization

The FortiGate platform delivers virtualization technology through the virtual domain feature, which enables the device to operate as multiple independent security domains, each capable of configuring and managing its own set of interfaces, VLAN sub-interfaces, zones, firewall policies, routing, and VPN settings. This virtual domain separation simplifies configuration by reducing the number of discrete routers or firewalls that must be managed. Support is also provided for IEEE 802.1Q Virtual LAN tagging operating in both NAT/Route and Transparent modes, allowing administrators to increase the number of network interfaces beyond the physical limit. By leveraging Fortinet's unique virtualization technology, a single FortiGate appliance can effectively provide UTM services and control virtual networks across multiple security domains for multiple VMware virtual servers in a data center environment.

Similar to the benefits of virtualization solutions from VMware, FortiGate Virtual Domains maximize the use of security hardware systems while reducing network hardware and switch ports. FortiGate units can be deployed in front of VMware ESX Servers to provide custom levels of security for each virtual server rather than use a generic overarching policy, resulting in increased network security within virtualized environments. In addition, the management interface can be segregated into isolated domains, each with its group of users and administrative privileges, delivering a truly virtualized security solution.



Fortinet Administrative Domains (ADOMs)

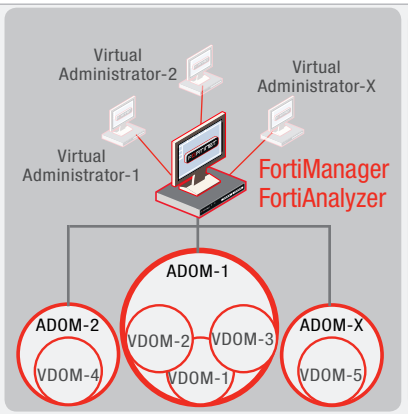
- ✔ Each ADOM is independent of other domains
- ✔ Manage all domains/devices from a single user interface
- ✔ Administrative access profiles (logs, reports, menus, etc.)

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



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*

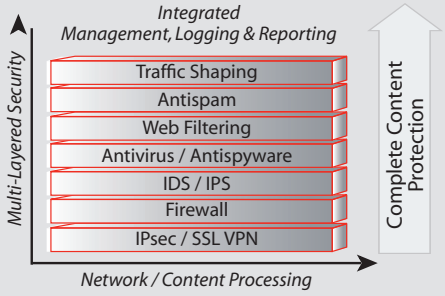
Fortinet Platforms

Protection, Management & Reporting

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

FortiOS™

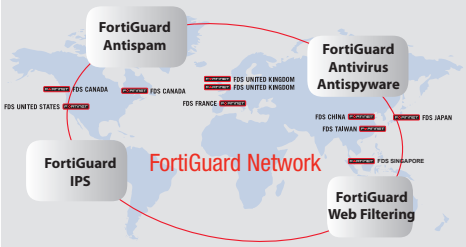
Modular Multi-Threat Security



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

FortiGuard Services

Security Update Development / Distribution



Fortinet Global Threat Research Teams

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

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-SINGAPORE
Fortinet Incorporated
3 Temasek Avenue, Level 21 Centennial Tower
Singapore 039190
Tel +65-6549-7050
Fax +65-6549-7259

SOL127-0408-R1