Virtual Firewalls

White Paper

White Paper

Virtual Firewalls

Introduction

A firewall is a network security device placed between networks to logically separate and protect the privacy and integrity of business communications across these networks, and to safeguard against malicious use. Firewalls are positioned between a corporate private network (trusted network) and other public networks, and monitor and enforce Corporate policies on all the communication flowing in and out of the corporate network.

Conventional firewalls performed the basic function of controlling access to communication occurring between an enterprise network and the outside world. However, next generation firewalls have significantly increased security capabilities. One very essential function is of preventing Denial-of-service (DoS) and Distributed DoS attacks. Denial-of-service is when a hacker or malicious user programmatically probes the Intranet to gain access to a private network, and then proceeds to use this information to further repeatedly scan and install disruptive tools. This leads to the network being compromised and steals considerable processing capabilities of the network, resulting in disrupting service and rendering the network unavailable to customers for large lengths of time.

A simple firewall configuration consists of a box with 3 ports – one port connecting to the network that requires the firewall, another to the Internet, and the third port to DMZ networks providing useful public utilities such as HTTP and FTP.

Firewalls can be standalone or installed as an integrated gateway solution. Standalone firewalls require significant administration effort and are a less-preferred solution, keeping in mind the increasing network complexity and rising security needs. Enterprises and small businesses increasingly prefer routers and gateways with built-in Firewalls with widely acceptable technologies like Stateful Packet Inspection (SPI). Stateful Packet Inspection provides the highest level of security by extracting the state-related information required for security decisions from all application layers and maintaining this information in dynamic state tables. This information is then used for evaluating further action on packets of the same session.

Security Enforcement using Policies

A corporate firewall is configured to enforce secure access to and from the network based on its Policy. A security policy is a living document that states in writing how a company plans to protect the company's physical and information technology assets. A security enforcement strategy is developed to safeguard

these assets against predicted threats. This strategy dictates the technologies, resources, tactics, and training required for security enforcement.

Enterprises use various tools and technologies to electronically secure their networks – firewalls, Virtual Private Networks (VPN), and Intrusion Detection systems are some methods for doing so. For all these security solutions, a security enforcement policy forms the foundation for implementing a security strategy, and the solution has the responsibility of enforcing security electronically, based on the security policy.

Policies can be inbound or outbound. Inbound policies are policies that are enforced on communications originating from outside and destined to enter a network. Outbound policies govern the communications originating from a network with a destination outside the network.

Firewall Implementation Options

Enterprises and small businesses have the following choices for setting up a firewall for their network(s):

- configuring and administering a firewall of their own or using third party services
- purchasing add-on firewall modules to install into their existing router, server, or switch
- using routers and switches with embedded firewalls – hardware or software
- engaging a service provider to host a firewall

Standard features of firewalls in the market are:

- Protection against various DoS and DDoS attacks
- Policy-based access control
- Inbound and Outbound policies for the corporate network
- Separate set of policies for DMZ network(s)
- Access control
- Application content filtering
- Generation of log and alert messages
- Generation of access statistics
- Intuitive user interface

The Market & Its Challenges

Multi Tenant Units (MTUs) or commercial office buildings, campuses, hotels and multi-family apartment buildings, present a large market opportunity for service providers to gain new customers through the provision of secure connections. The MTU/MDU customer base is currently underserved by existing local exchange carriers. Cahners-In-Stat group projects that the worldwide MTU

market will grow from $1.2 billion in 2001 to $9.8 billion in 2005. Revenue forecast for MDU services and hardware is projected to grow from $393 million in 2001 to $3 billion in 2005.

Small businesses and home offices need cost-effective and reliable networking solutions. Moreover, the solutions need to be easy to install and use, and scalable to accommodate changes as the business grows. Effective firewalls with advanced security are essential to protect confidential information and to maintain quality of service.

Challenges

The rising reliance on the Internet for executing core business tasks has propelled businesses to rapidly execute steps to ensure always-on, reliable, and increasingly secure network for their employees and customers. The major factors differentiate firewalls in the business community are performance, scalability, application support, and ability to protect against increasing number of malicious attacks.

Large enterprises and Service Providers mandate as critical, the need for high performance firewalls. This is achieved through high-performance CPUs and firewall software optimized for maximum performance on a given hardware platform.

Scalability is dependent on whether the firewall software architecture can secure an existing network as well as future expansions to the network (or addition of subscriber networks, in the case of service providers.)

Next Generation firewalls will need to actively support extension of security and collbaboration for selective user communities within an enterprise.

Next generation firewalls will need to actively support extension of security support and collaboration for selective user communities within an enterprise. An enterprise consists of a collection of individuals with separate functions and responsibilities, requiring disparate access control. Different divisions of an enterprise may need to maintain separate networks, requiring some collaboration but limiting the access privileges across the entire enterprise.

The increasing need for enterprises and businesses to scale - to add users and user communities and separate network entities with their own governing security policies - will require the management of firewall security by duplicating indefinite numbers of firewall boxes, one for each additional network. Technology solutions that can provide an aggregation of firewalls in one box would be more practical and easy to maintain.

The Virtual Firewall System

A Virtual Firewall System (VFS) provides multiple logical firewalls for multiple networks, on one system. That is, a service provider with numerous subscribers can provide firewalls separating and securing all the subscribers and yet, is able to manage it from one system. This is accomplished by establishing "security domains" controlled by Virtual Firewalls, with each firewall having its own defined

security policy. Security domains are exclusive in that they are external to any other security domain in a given system.

Virtual Firewalls are functionally similar to a simple firewall, and are configured with their own outbound and inbound policies, and network objects. However, Virtual Firewalls enable easy management of a collection of firewalls through policies at a defined security domain. In addition, VFS allows additions and removal of security domains, providing scalability with the growth of subscriber networks.

Virtual Firewall Selection

In a Virtual Firewall system, physical ports connecting to Security domains on the system are identified by VLAN IDs. Each security domain is associated with physical ports/VLAN ID and IP addresses. When the packets come into the VFS, the security domain is identified by this association.

For connections originating from the Security domain, the Virtual Firewall is selected based on the physical port or physical port & VLAN ID combination, and outbound policies of the firewall are enforced.

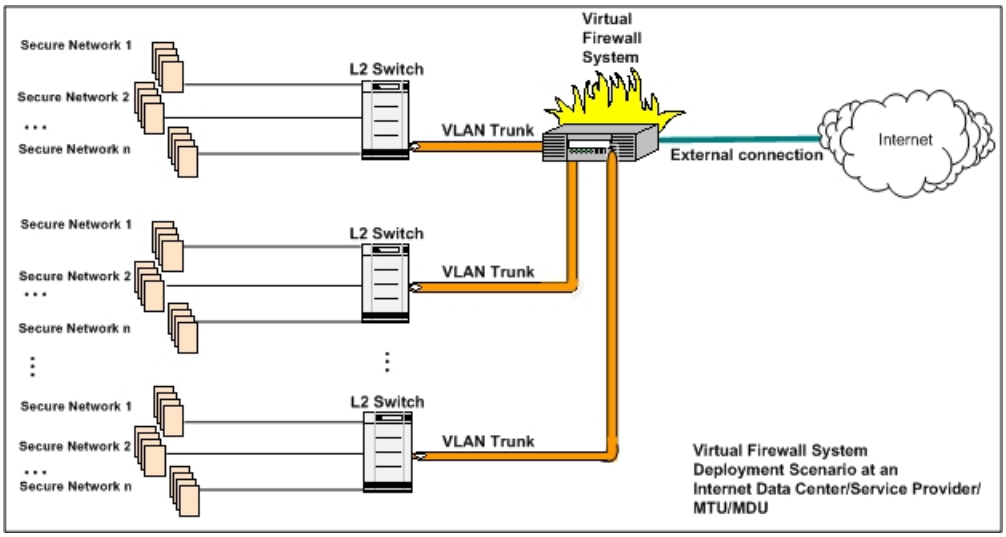
For connections originating from outside the Security Domain, the Virtual Firewall is selected based on the destination IP address, and inbound policies of the firewall are enforced.

Deployment Scenarios

Two deployment scenarios are illustrated for Virtual Firewall.

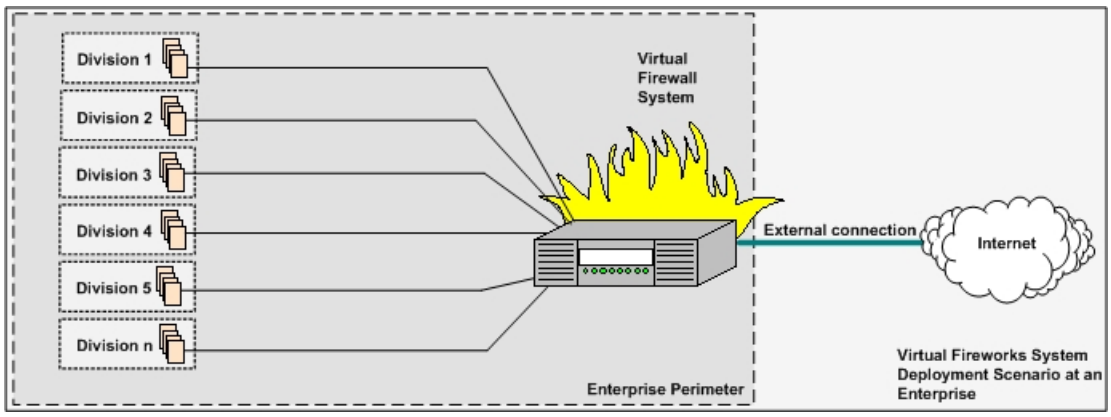
Internet Data Center/Service Provider/MTU/MDU Deployment Scenario

The figure displays several secure networks (representing subscriber networks for a service provider, or tenants/dwellings/offices in an MTU (Multi Tenant Unit) or MDU (Multi Dwelling Unit) connecting to the Internet through a gateway box embedded with the Virtual Firewall System. Each network has its own security domain and connects to VFS through an L2 Switch.



Enterprise Deployment Scenario

The figure displays one VFS box with multiple ports corresponding to each division network on one end, and the external network at the other end. The secure networks for the division in an Enterprise connect to the Virtual Firewall System through a single VLAN Trunk connection. Each division has its own security domain.



Benefits of Virtual Firewall Systems

Ease of Deployment

Traditional firewall solutions will require Service Providers/MTUs/MDUs to incur huge infrastructural and maintenance costs to purchase several firewall boxes, one for each office/tenant in a unit.

Virtual Firewall reduces the requirement to procuring one box that will connect to the external Internet one end, and to multiple networks providing for several subscriber networks on the other, each with the security of a separate firewall. The cost saving factor is chiefly realized in **lower deployment costs and effort** – enterprises can avoids the need to duplicate firewall units across

networks, and take advantage of security solutions readily offered through Service Providers, totally avoiding the need to interfere with the network operation of the enterprise.

Ease of Management

A service provider with multiple subscribers will need to host one instance of a virtual firewall for all subscribers of a network, governed by one set of policies. For a second subscriber network, there will be another instance of a Virtual Firewall with its set of policies, and so on. Here, the Service provider has multiple logical firewalls for multiple networks, but needs to manage only one system.

Deployment is easy since Service Providers provide the capability and enterprises do not need to tamper with their network operations to provide this solution. Management is also more efficient through web-based user interfaces.

A Virtual Firewall System provides multiple logical firewalls for multiple networks, on one system.

Lower Costs

The capital equipment cost of one system providing multiple firewalls for multiple networks is far less than the compounded costs of purchasing and maintaining a separate simple firewall system for each subscriber network.

- Cost of one VFS box: many subscribers < Cost of 1 firewall box * no. of users in a unit

The MTU and service provider market segments can reduce equipment costs, setup costs and maintenance effort by using Virtual Firewall Systems. Large enterprises requiring multiple security domains will also find VFS an attractive proposition. For example, different divisions of an enterprise can be setup to have separate security domains with firewalls having independent access privileges and policies, all from one VFS system.

The direct cost benefits are:

- Savings on hardware purchases
- Savings on administration and maintenance costs

Easy Management

VFS provides an interactive web-based user interface for managing numerous firewalls from one system, while maintaining the look-and-feel of a standard firewall. This makes it favorable for users transitioning from a traditional firewall solution to VFS. VFS also provides the capability of adding and deleting security domains. For example, an enterprise can define a security domain on the evolution or change of its divisions, or a service provider can define a security domain with the addition of a new subscriber network.

The Intoto Approach

Intoto Inc.'s iGateway-npFirewall software provides comprehensive Virtual Firewall capabilities that can be integrated into communication gateway

equipment. Our software solution provides a complete security solution, including virtual firewall capability supporting multiple security domains.

iGateway-Firewall uses Stateful Packet Inspection (SPI), bringing with it all the features of a standard SPI-based firewall product. iGateway-Firewall additionally provides integrated NAT, and User Group configuration features.

iGateway-Firewall comes with integrated Network Address Translation (NAT) to conceal IP addresses and provides assigning of easy-to-remember names for IP addresses using network objects.

Flexible user configuration is provided in iGateway-Firewall through the use of User Groups allows creation of user groups and access policies specific to these groups. This is of immense use to manage security of mobile users accessing private networks remotely.

The iGateway-npFirewall Advantage

Intoto's FastPath Adaptation Layer optimizes performance of network processors by separating the Data Plane executing fast processes, from the Control Plane carrying out normal policy checks and access control activities of the firewall.

Intoto's innovative architecture provides a competitive advantage in iGateway™ for service providers to deploy current and future high-margin managed security systems. iGateway-npFirewall is equipped with the capabilities of Virtual Firewall Technology.

iGateway-npFirewall's FastPath Adaptation Layer (FPAL) provides well-defined APIs that work with fast path engines of various network processors and specialized ASICs. Independent Data and Control planes contribute to performance optimization through the use of Fast Path and normal path processing. Standard security checks such as policy lookup and session creation, and processing requiring application intelligence happen in normal path processing. Fast Path includes all forwarding functions on data packets, and separating this Data Plane from the Control Plane (performing normal path processing) greatly accelerates perimeter security performance.

Use of Stateful Packet Inspection requires creation of many associations for communication of data packet across secured networks. iGateway-Firewall manages association classification through the support of hash tables defined for each security domain, accelerating the data processing pace by effectively reducing search time for associations belonging to a security domain.

iGateway is highly scalable through addition of security domains with virtual firewalls. In addition iGateway-Firewall software is architected into a Core module with zero-dependence on interfaces and network elements, and a Porting module customizable for different market segments. This makes iGateway-Firewall suitable for a range of users – from service providers using low-end CPE devices to cater to residential/SOHO market segments, to MTU segments using high-end devices, and large enterprise Service provider markets.

Partners in Progress

Embedded systems on the Internet are the fastest growing class of devices using Internet technologies. Uncompromised security over the Internet is an undeniable need for businesses communicating over networks.

Positioned as the enabler of gateway infrastructure, Intoto Inc. provides complete embedded security software providing for security, connectivity, convergence, management and network processor solutions. Used extensively in a majority of gateway equipment in conjunction with embedded microprocessors, system-on-chip communications processors, and next-generation network processors, Intoto's iGateway™ software platform integrates security, wired and wireless connectivity, advanced networking protocols, web-based management and WAN/LAN interfaces to provide a complete infrastructure for next generation gateway products.

Intoto has successfully established strategic licensing relationships with processor vendors to pre-integrate iGateway on multiple processors such as x86, MIPS or ARM-based SoCs, PowerPC and specialized network processors. Its licensing-based business model allows equipment manufacturers to create and rapidly deploy fully validated, reliable gateway equipment. Equipment manufacturers have successfully reduced development costs, and re-used the modular software across multiple products to maximize returns.

In the area of network security, iGateway™ Security Solutions are licensed to a large number of customers including over 15 blue-chip equipment manufacturers and processor vendors. Intoto licensed its embedded iGateway™ solutions to over 100 customers.

For high performance gateways, Intoto's innovative architecture in npFastPath Application Layer APIs, seamlessly integrate with iGateway to provide optimized performance and rapid deployment through separation of data plane software for individual network processors from the control plane.

The iGateway™ Security Solutions have been extensively validated by leading equipment manufacturers and processor vendors. Intoto solutions are certified by ICSA, a leading security assurance organization.

Conclusion

The increasing dependence and dominance of the Internet in the business world goes hand-in-hand with the need to ensure secured communication channels. This opens up a large market opportunity for scalable security solutions for small businesses, home offices, and MTU/MDU market segment, as well as large companies and service providers.

A firewall is a network security device placed between networks to logically separate and protect the privacy and integrity of business communications across these networks, and to safeguard against malicious use. Most importantly,

firewalls protects corporate networks from Denial-of-service (DoS) and Distributed DoS attacks.

Firewalls can be standalone or installed as an integrated Gateway solution. A firewall is configured for security based on a corporate's Security Policy. A security policy documents the security strategy for a company's physical and information technology assets. Traditional firewalls are less scalable, requiring hardware and infrastructural investments with increased need for firewall protection.

A Virtual Firewall System (VFS) provides multiple logical firewalls for networks that are geographically distributed, on one system. Functionally similar to firewalls, Virtual Firewalls provide easy management of a large number of firewalls through security policies at defined security domains.

The major benefits of Virtual Firewalls are realized in ease of deployment and management, and reduced costs. Virtual Firewalls offer scalability by providing multiple firewalls from one system, and the ability to define "security domains' or boundaries for firewalls within a network. This reduces the equipment service providers and businesses need to buy, and provides one integrated system, greatly reducing cost and resources needed to manage the system.

Intoto's Virtual Firewall System – iGateway-Firewall[1] provides all the standard features of a Virtual Firewall system. In addition to using SPI and NAT, it also provides interactive web-based management interfaces, and options to define user groups.

Intoto Inc.

3160 de La Cruz Blvd., Suite #100
Santa Clara, CA 95054-0480, USA
Voice: 408.844.0480
Fax: 408.844.0488
www: http://intotoinc.com

[1] All trademarks and copyrights referred to are the property of their respective owners.