# Protecting the New Perimeter With Symantec Firewall Products

Vladimir S. Amarante

April 2, 2002

SANS GSEC Practical Assignment v. 1.3

## Abstract:

Every day more computers are being connected to the Internet, worldwide, and many of them use broadband connections. Computers host valuable information, and they should be protected from non-authorized access or attacks.

The concept of the perimeter is changing because of the growing need of connectivity, information availability and user mobility. Also, companies are looking for VPN solutions to provide a secure connection for mobile users and partners.

It is very difficult (or impossible) to proactively detect and block intrusions without software products or tools (free or commercial). Many companies choose to use commercial products because of legal concerns and responsibility issues.

It is important to find a vendor that offers good quality products and capacity of maintenance and investments. This affects the speed that the vendor provides new features, patches and updates to their products, investments in new technology (product roadmap) and background infrastructure.

Symantec is a security company with such profile. They have award-winner products, a very good background infrastructure such as their *Security Response* lab (a.k.a. SARC - http://www.sarc.com/), and unique technologies like *LiveUpdate*™. Symantec offers many options on the Firewall product line, from softwares to appliances.

Firewalls are used to provide some level of security on the perimeter (border), and they are offered as softwares or appliances. Each implementation has its own advantages and disadvantages, which are related to the ease of installation and total cost of ownership.

There is the concern of the firewall being a single point of failure. With the option to use High Availability solutions, which sometimes also includes Load Balancing features, it is possible to stay online and protected in case of a failure.

Today we are facing a new type of threat, called "Blended Threats", and they can only be effectively detected and blocked by using a secure firewall such as a Proxy Based firewall and also good IDS (Intrusion Detection Systems) and Antivirus software. Recently Symantec has launched a product that has all of this technology in a single box.

Firewalls are an important component of the network security, and the company should choose the best option considering the security, performance and cost. There are options for different needs and budgets, offered by reliable vendors such as Symantec.

## The Perimeter:

The perimeter of the company used to be the doors, windows and walls of a building or room. But today there is another perimeter, a virtual border that separates the company's trusted network from other untrusted public network - such as the Internet. We will call this virtual border as "the perimeter".

Traffic coming from and to the Internet passes thru the perimeter.

## The broadband connections and the Perimeter Security:

New companies and users are getting connected to the Internet, at the same time that other companies are moving from expensive leased lines to cable modems or DSL lines. It means that more computer networks are being connected to the Internet using high-speed links [1].

The risk of an attack is now higher because computers are staying connected to the Internet for more time than ever, and many of them for 24 hours a day. Considering that many broadband providers do not apply a filtering protection for the customer connections, the security infrastructure must be implemented on the PC or the company's network.

The company and users to provide some level of protection at the network border, and sometimes between network segments should use firewalls.

## The Need for Perimeter Protection and Basic Concept of Firewalls:

Companies need a device to control what type of traffic comes in and out of the network, the same way they need doors and guards in a building or office to control what type of individual goes in and out.

Internet traffic passes thru the perimeter, so in most networks it is a logical location to install firewalls, since they can filter that traffic reducing the possibility of a successful attack. In other words, mitigating the risk at the perimeter.

Firewalls analyses networks packets and consider what to allow or deny based on rules. Rules reflect the company's security policy, which states what are the permitted and denied types of traffic (packets). Rules consist of a combination of parameters such as protocols, network entities (e.g.: subnet, host), daytime, user, user group, network interface, etc [2]. It can differ from each firewall product. Some firewalls use only protocols and IPs, others can use more objects such as user and daytime, when defining rules.

Some firewalls by default block all the traffic. This is the most secure implementation. Other firewalls came with all open, and the administrator should choose what to block, instead of what to allow [2].

Firewalls are very important for the border security as a filter for packets. But there are many other security needs such as authentication and encryption for the network traffic, and some firewalls offer user authentication and integrated VPN servers (to provide encryption for the communications).

## The different types of Firewalls:

Basically there are three technologies when talking about firewalls products:

***Packet Filter Firewalls:*** Usually implemented on routers, it is the least secure type of firewall, but they are fast because they apply filters only by:

- Source and destination IP addresses;
- Source and destination port numbers;

It is less secure because it does not consider the data payload on the packet [3], so any data or command can be sent inside a packet that passes the IP and port filters. E.g. some hacker can send malformed commands to port 80 trying to exploit vulnerabilities on a web server, or even send a wrong sequence of packets (used to map the network based on responses that the computers generate).

***Stateful Inspection Firewalls:*** This technology extract information from all protocol layers to make the decision. It maintains the information in dynamic state tables for subsequent packets. It knows the state of the communication, and the type of protocol, like HTTP for instance.

It monitors the connection negotiation and creates a temporary state table. If an incoming package arrives, it is checked against a connection state table for a matching outgoing request packet. [3]

It is more secure than packet filters, and faster but less secure than proxy based firewalls.

***Application Layer / Proxy Based Firewalls:*** This is the most secure technology, but with more delay than the other technologies. This firewall is based on proxies, so every authorized package creates a new package from the firewall to the destination. The firewall will only accept valid commands for the specific protocol, because there are different proxies, one for each protocol, so the firewall can understand what is a valid HTTP command, FTP, Telnet, SMTP, etc [3].

It is very secure, but some firewalls do not offer proxies for all types of protocols. To handle this situation, Symantec Enterprise Firewall offers a GSP (Generic Proxy) that works for all others without specific protocol checks. It is still more secure than other implementations, because it will at least hide the client IP and check for valid TCP headers.

**Additionally there is another type of Firewall:**

***Hybrid Firewalls:*** Firewalls that mix the three types of technologies above. Symantec Enterprise Firewall, Symantec VelociRaptor and Symantec Gateway Security are examples of Hybrid Firewalls.

You can create rules that uses proxies, rules for stateful inspection and rules with packet filtering, all active at the same time in the same firewall. This allows the balance between speed and security.

**The importance of Rules:**

Firewalls filters are based on Rules. A rule describes what packets are allowed or denied, for traffic coming from x to y.

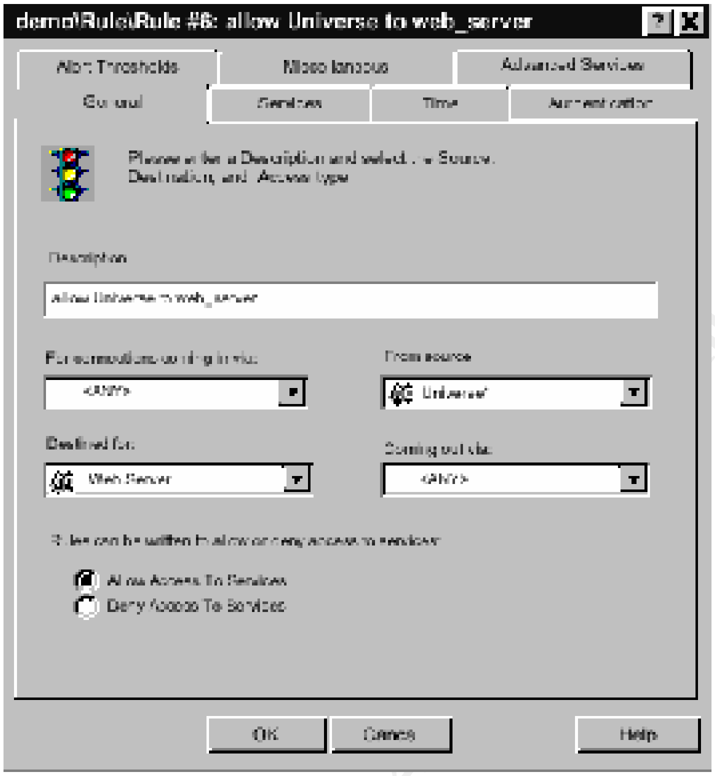
In Symantec Enterprise Firewall, Symantec VelociRaptor and Symantec Gateway Security rules are created using:

- Entities (Hosts, Networks, Subnets, VPN Tunnels)
- Network Interfaces
- Services (Protocols and Proxies)
- Users / User Groups
- Time

Rules are the most important part of the security configuration of the firewall. The rules should be created based on the company's security policy. If the rules are misconfigured all the firewall technology become useless.

If the firewall is configured with a lot of rules, you will have more chances to make a mistake. If you have a problem it will be easier to troubleshoot and review the rules to find what is wrong. The ideal number of rules varies from each environment, but usually it should be no more than 30 rules, for administration reasons. [4]

The Symantec products allow the administrator to specify what Network Interface the traffic should come from and go to (figure 1), this helps avoid spoofed packets. For example, a packet originated from the Internal Network with a spoofed source IP from the Service Network (DMZ) will not be accepted because the firewall knows that packets from the Internal Network should come from the Internal Network Interface, not from DMZ's.



demo\Rule\Rule #6: allow Universe to web_server

Please enter a Description and select the Source, Destination, and Access type

Description: allow Universe to web_server

For connections coming in via: <ANY>

From source: Universe

Destined for: Web Server

Coming out via: <ANY>

Rules can be written to allow or deny access to services:

● Allow Access To Services
○ Deny Access To Services

The Rule Creation Window
Souce:  Symantec Enterprise Firewall 7.0 – Configuration Guide
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_config.pdf

There are basically two types of Rule analysis:

- Order dependent rules
- Order independent rules

Symantec Enterprise Firewall utilizes Order Independent Rules, it means that the firewall will analyze all the rules and go for the most specific and restrictive [5]. Remember that if there is no rule matching for the traffic, SEF will block it.

Some firewalls such as the Checkpoint Firewall 1 implement order dependent rules. The disadvantage of this method is that the administrator can put a rule up or down another rule, in such wrong order that:

- Create a security hole: Going up down, if one rule **allows** the traffic the other rules below will not be checked.
- Create a Denial of Service situation: Going up down, if one rule **denies** the traffic the other rules below will not be checked.

## VPN – Virtual Private Networks:

VPN is a technology that allows the creation of encrypted data tunnels between hosts or gateways. The VPN was developed based on the AAA concept (Authentication, Authorization and Accountability) [6].

The VPN can be established between a mobile user device and the company's VPN Server or between two VPN Servers:

- Client-to-Site Tunnels: One client PC connecting to a VPN server
- Site-to-Site Tunnels: Connecting two VPN Servers to serve as gateways for the connected networks.

One benefit of the VPN is the reduction of expenses with Leased Lines or Frame Relay Links. Now, the remote computer can connect to the near Internet provider (via Modem, Cable Modem) and then open the VPN client software to establish the VPN tunnel. Once established, the user will virtually feel that he is inside the company's network, the big difference will be the performance because of the encryption overhead and link speed.

### VPN and Firewalls together

It is possible to have one box for VPN and other for the Firewall, or have it all together and integrated in one single box.

Separate solutions can be harder to administer and depending on where you position this components you can open a security hole. For example, if you position the VPN server outside the network, with a second NIC for the inside or service network, if an attacker gain access to the VPN server he can try to reach the internal machines, or even do a DoS attack on the unprotected VPN server causing many users to lost connections or being unable to connect to your company.

There are many solutions on the market that integrate the firewall and VPN components. Some of them allow you to create the VPN tunnel with Firewall rules active for that connection. It can be done in a single console or interface, making the administrative task easier. So the benefits are one single console, firewall rules for VPN traffic, consolidated logging, simplified routing, etc [7].

### The New Perimeter

In the past the main objective of security was "let the people out", but today it is "let the right people in". This people are the users, such as customers, partners, employees, contractors or any authorized user that needs connectivity to the company's network.

Some of them are mobile users such as home-office workers or traveling employees. They carry notebooks or PDAs with company information, and often they need to access the company's network when outside the office. The company now has to extend the perimeter and protect these assets with personal firewalls and VPNs [8].

Other example is the e-Commerce applications. Now the user is an Internet User that wants to buy our products via the Web. The Web Server is hosted on the company's network, so there is traffic coming from outside to inside the perimeter. Our perimeter protection device – the firewall – must be configured to allow the required protocols to pass when the source is the Internet and the Destination is the Web Server.

So, there is a new extended perimeter, created by the need to connect Partners, Customers and Mobile users to our network (let the right people in).

## Expanding the perimeter protection - Confidentiality

To ensure confidentiality and integrity of the data being transmitted over the Internet to the trusted network, companies are looking for VPN solutions, because it authenticate and encrypt the data for the connection (tunnel).

It is also important to install personal Firewalls on notebooks and internal computers, to protect from attacks coming from the trusted network and also from strange or public networks, such as when a mobile user is in a hotel or in a customer site.

## The Authentication

It is important to use authentication mechanisms to identity users and restrict access to services and information.

Authentication usually relies on usernames and passwords. Technologies such as tokens and biometrics equipments can be used to apply a more secure authentication mechanism. The authentication mechanism should be protected with some level of encryption to avoid password stealing.

To increase the security of the perimeter protection, authentication can be required to access specific services or computers for traffic that passes thru the firewall.

VPN tunnels are used to connect external computers or networks to the company's network. This tunnels use authentication to in the process of establishing the tunnel.

It is also important to have a firewall that integrates with the existing user and password repository of the company, such as NT Domain, LDAP providers, RADIUS Servers, … Making the administrative task easier and not requiring different passwords for the same user.

## Software solutions x Appliance Solutions

Appliances are hardware-based solutions. They run some proprietary OS, or a market OS, and host different types of software for many uses.

Appliances are usually easier to set-up than software based solutions, considering that the administrator doesn't need to install the OS, Service Packs and other required software prior to the firewall installation. It's almost "plug-and-play", requiring little configuration to activate the box.

Usually it is more expensive to buy new hardware for the Server, OS licenses (like Windows NT/2000 licenses), apply service packs for the OS, install hardware drivers, and install the firewall. It's easier and faster to deploy the appliances and provide some level of protection in short time.

In other hand, software-based solutions can be more flexible when talking about customization. Most times you can't add more processors, memory or network interfaces to appliances.

### One scenario where appliances are useful

Recently CompanyX implemented DSL lines from the headquarters to branch offices and stores all over the country. They want to provide Internet connection and also establish VPN tunnels from the remote locations to HeadQuarter.

One solution is to implement Appliances on each location and a software based firewall and integrated VPN server at the Headquarters. The appliances can be managed remotely, without the need of a firewall administrator on site.

All the Internet and VPN traffic will be checked by firewall rules, filtering and reducing the amount of traffic that will pass over the DSL line. The administrator can easily define who can access the VPN or the Internet, and what service to allow (HTTP, FTP, SMTP, SQL, …).

The company is now connected with a lower cost than leased lines, and with distributed Internet connection (reducing bottlenecks).

### Symantec Firewall Products

Today Symantec is positioned as the Leader in the Internet Security (Gartner Group) and they offer many products, from the antivirus to the intrusion detection.

In the year 2000 Symantec acquired Axent Technologies, which brought mature security products, such as the Raptor Firewall.

Today Symantec provide products and services that help us implement the "defense in depth".

For perimeter protection with Firewalls, they have the following products:

- Symantec Desktop Firewall – *This is the personal firewall;*
- Symantec Enterprise Firewall – *The new Raptor Firewall;*
- Symantec Firewall Appliance – *The small appliance for Small Business;*
- Symantec VelociRaptor – *Firewall and VPN appliance for up to 1000 users;*
- Symantec Gateway Security – *Appliance for Firewall , VPN, IDS, AV and Content Filtering, all together.*

### Target Market for the Symantec Firewall products

The Desktop Firewall is targeted for any company that wants to protect notebooks or PCs with a personal firewall. It is most times used on notebooks because often they are directly connected to strange networks.

The Symantec Enterprise Firewall 7.0 is targeted for companies with 5000+ employees.

The Symantec Firewall/VPN Appliances are targeted for small offices with up to 40 users. (Models 100, 200 and 200R)

The Symantec VelociRaptor Appliances are targeted for companies with up to 1000 users. (Models 500, 700 and 1000)

The Symantec Gateway Security Appliances are targeted for companies with up to 1000 users per node, with the option to scale with load balancing. (Models 5110, 5200 and 5300)

**Main Product features that help us provide a good perimeter protection:**

Let's take a look at the most important security features of the Symantec Firewall products:

*Symantec Desktop Firewall [9]:*

- Monitoring of Inbound and Outbound Communications: SDF checks both traffic that comes from the Internet and traffic that originate from the PC. Many personal firewalls, including the one that came in the Windows XP, check only for incoming connections.
- Rules per application: This feature enables or disables traffic only for one specific application.
- VPN Support: It contains rules that allow VPN traffic. That's important since personal firewalls are installed on mobile user's notebooks.
- Blocking Known Trojans and Attacks: It comes with pre-configured rules to block known Trojan Horses - like Back Orifice – and network attacks.
- Automatic download of updates via Internet: This is an important feature, which deals with the updating of the rules for known Trojans and attacks. The user just need to click the *LiveUpdate* button to have the program go to the Internet, download and apply the new rules.
- Configuration Packages: Using a package creation tool, the administrator can create different profiles of users, and then create an EXE file to distribute and reconfigure the clients.
- Helps maintain Confidentiality: Checks and blocks HTTP forms and packets that contain specific strings, such as credit card numbers, e-mail addresses and other confidential information.

*Symantec Enterprise Firewall (SEF) [5]:*

- Application Inspection Technology: This is a very important feature. SEF has a lot of specific proxies, for most common protocols such as HTTP/HTTPS, FTP, SMTP, NNTP, H323, RealAudio, … It is important to have proxies specifically for a protocol, because it allows the firewall to prevent attacks that use malformed commands, helping prevent vulnerability exploits like buffer overflows. When the firewall is using the proxies, it will receive the original packet and if it passes thru the filters the firewall proxy generate another package for the destination, but only if the command is understood by the specific proxy.

- Integrated VPN Support: Symantec Enterprise VPN can be integrated to SEF. This allows the administrator to create firewall rules for VPN tunnels, using the same objects of the object-oriented interface of the product, in one single console.
- System Hardening: During the installation, and constantly while the firewall is running, SEF does a System Hardening of the server where it its installed. The System Hardening is done by a process called "Vulture", and protects the firewall itself from intrusions. The hardening consists of the following actions:
    - Stopping unauthorized services or processes
    - Disabling any non-administrator/root login
    - Disabling IP routing and forwarding at all times
    - Detecting and logging port scans against the firewall
- User Authentication: SEF provides compatibility with a lot of authentication mechanisms bringing compatibility with existing authentication services, eliminating the need of creating user accounts in the firewall, and also eliminating the duplicate user management.
- Blocks All By Default: SEF comes by default with the most secure approach for firewalls, which is block all traffic by default. This reduces the risk of creating security holes, since the administrator should only specify what to allow.
- Centralized and Remote Management: This enables the administrator to manage remotely all of their Symantec firewalls and appliances, reducing the administrative cost.
- High Availability and Load Balancing: Enable the administrator to join firewall machines in a firewall cluster for configuration replication, load balancing and high availability.
- Integration with Antivirus software: SEF can use Symantec CarrierScan antivirus software, to check for viruses on HTTP, FTP and SMTP packets. This is enabled per rule.
- Network Address Translation: Prevents internal IP addresses from being visible on the Internet. The Internet users will only see the firewall's IP a ddress. The firewall does the NAT automatically because it is proxy based by default. Once the proxy generates a new request for each original client request, the outgoing package originates from the firewall itself.
- Address Transform: This option can be used to change the IP Address of the package. It is possible to define when to maintain the Original Client Address, Use the Gateway Address or Use a NAT Pool. This option is useful because Nat is always active, but the administrator may want to see the original source IP.
- Service Redirects: This feature allows the administrator to redirect a request coming for an specific IP and port to another. This is especially useful when there are servers with public services, such as a Web Server or Mail Server. The administrator can configure a redirect rule that looks for the HTTP connections at port 80 coming from the outside interface and forward them to the Web Server on the internal service network.
- Generate alerts: The administrator can enable alerting for specific log file events. This alerts can be set to use SMTP, SNMP, run a program, …
- Tamper proof configuration files: SEF can detect if the configuration files were tampered or edited by hand, and automatically restore a backup copy.

- Backup: The administrator can make backups of the system configuration. Backups are always important specially when it is needed to recover from a system failure.
- Log file exporting: The administrator can export the logs to a CSV formatted file. This is useful to generate graphics or summarize the information for executive reports.
- MMC Console: Many administrators are familiar with the MMC interface. MMC is a console that uses Snap-Ins for each product. Administrators can create a customized console with different products in the same screen.

*Symantec Firewall Appliance [10]:*

- HTML Console: Simple interface allows users to easily define what type of services they want to allow.
- Blocks All By Default: This device blocks all by default. The user should specify what services to allow. Many small devices have all open by default, it is easier for inexperienced users but it is not a secure approach. Symantec goes for the most secure approach, always.
- IPSEC VPN: This little box has VPN capability. The model 200R is the only one with client to site VPN, in the SFA family.
- Backup Dial-Up: If the WAN ports fail, the appliance dials for a backup route such as a ISP via modem.
- Load Balancing between the WAN ports: The administrator can set a threshold to balance the traffic load between the two WAN ports. If it is set for 40%, when this threshold is reached, the new traffic begins to flow via the other WAN port.

*Symantec VelociRaptor Appliance [11]:*

- Powered by Symantec Enterprise Firewall: Symantec VelociRaptor provides the same features, level of protection and configuration flexibility of Symantec Enterprise Firewall. The SEF administrator will feel comfortable to administer VelociRaptor appliances. There is only one console used for both SEF and VelociRaptor, allowing a centralized and remote management of different firewalls.
- Lockable Front panel: This option allows the administrator to block the access to the buttons that can be used to configure interface IPs, reboot and shutdown the appliance.

*Symantec Gateway Security Appliance (SGS) [12]:*

- Powered by SEF: Just like VelociRaptor, SGS has the same features and benefits of SEF.
- Integrated VPN, IDS, AV, and Content Filtering: It is a multi-functional box that provides many of the security technologies that are needed by most corporations, all in one single box.
- High-Availability and Load Balancing: This box can be part of a firewall cluster, allowing fault-tolerance and load balancing.

- Antivirus Built-in: This box includes Symantec CarrierScan. CarrierScan is an antivirus for high volume of data, and it is being useful to stop virus before they enter the network.

The Symantec Firewall products have the optional VPN component, which is the Symantec Enterprise VPN. It is an important component of a security solution. Let's take a quick look at its main security features:

*Symantec Enterprise VPN [13]:*

- IPSec compliant: This product uses IPSec protocol for the VPN tunnels. It is a standard and it's used in many VPN products. It is technically possible to connect VPN products from different vendors using the IPSec Protocol, like connecting the Symantec Enterprise VPN and the Checkpoint VPN-1, for instance.
- AES, DES, 3DES: There are 3 options for encryption. The administrator can choose between AES, DES or Triple-DES to balance security and performance.
- MD5 and SHA1: The Symantec Enterprise VPN utilizes MD5 or SHA1 to implement cryptographic checksums and detect data modification.
- IKE Key Management: The product utilizes IKE as the method for authentication and key exchange.

## Can the Firewall be a Single Point of Failure?

In most environments, the firewall is used as the gateway for the network. If it fails it can cause Denial of Service (DoS), such as:

- The internal users lost their connection to the Internet;
- The Internet users can no longer reach the company's Web Server and Mail Server;
- Customers and partners lost their connections to e-Commerce applications;

The Firewall can create Denial of Services when there is a hardware failure, a software failure, or wrong configuration of the system, like wrong Rules.

The solution to reduce the risk of a total failure on the firewall is High Availability components.

It is virtually impossible to have redundancy in all of the computer systems and network components, but the company must define what is the most important computer assets and try to understand what are the cost of a DoS versus the cost of implementing a secure solution. Also, the company must define if they will assume some risk, and take actions to reduce or mitigate the risk.

Basically High Availability is an implementation of redundancy. If one device or service fails, there must be other to take its place, automatically.

You can have two or more systems participating in a High Availability cluster. If node one fails, node two wakes up and take over its place temporarily until the node one comes up again, or until the administrator chooses to change it back to node one.

If node 2 does not know what was happening in node 1 (established connections), every connection in node 1 will be lost, since node 2 won't recognize what is that traffic for. This means that node 2 does not know the "state" of node 1.

Some High Availability solutions implement the state sharing capability, so node 2 will now know what is happening in node 1 and it can continue node's 1 work when required.

Having backup nodes paused waiting for a failure it's good but not so smart. It's better to activate those nodes bringing improvement to the performance. This is called Load Balancing.

The Symantec Enterprise Firewall 7.0 and the Symantec Gateway Security Appliance products have the Rainfinity Rainwall High Availability and Load Balancing software built-in.

The Rainfinity Rainwall for Symantec Enterprise Firewall 7 utilizes a technology named RAIN – Redundant Array of Independent Nodes. The performance improvement is linear. The Rainwall technology is implemented using VIPs – Virtual Ips – and relays on the ARP Resolution. The network communication is based on MAC Addresses. ARP is a protocol to convert IP numbers to MAC addresses. RAIN plays with the ARP resolution. Every time that there is an ARP resolution request, it will reply with the MAC address of the node that are available and that has lower utilization (figure 2). The nodes exchange information about their status, and dynamically distribute the load between them. [14]

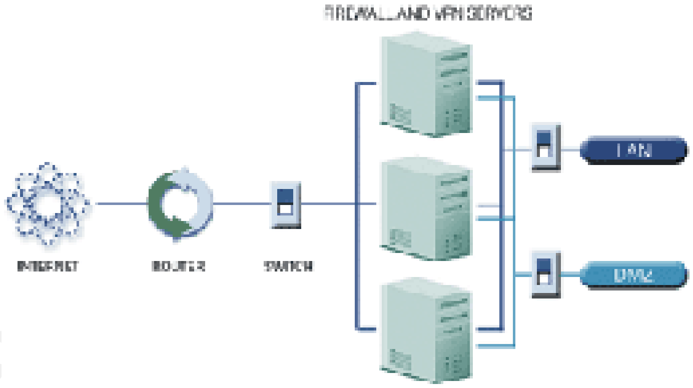


Figure 2: Nodes appears to be one single IP (VIP)

**The Tendency of Perimeter Protection:**

There is a new type of threat called "Blended Threat". It means that there is no single cure for one threat. It consists of attacks that are a mix of techniques and methods of invasion. Two recent examples are the virii Nimda and CodeRed [15].

With the risk of Blended Threats, Companies are looking to install devices such as:

- Firewalls/VPN Servers
- Intrusion Detection Systems

- Antivirus at the Gateway
- Content Filtering

Those technologies help prevent intrusions and filter the allowed content for malicious code and improper content.

At the beginning of the year 2002, Symantec released the Symantec Gateway Security appliance, which has all of the above technologies in one single box.

There is no single box alone that protects all network from all threats, but products like Symantec Gateway Security can provide a good level of protection when merging different technologies in one single box or a cluster, ensuring various levels of checks, helping us achieve the defense in depth.

**Conclusion:**

We live in a world where people use connected devices to exchange information. More and more information are staying online, public or confidential.

The risk of an attack and losses is real, and we should look for tools and products that help us mitigate risk. Firewall is an important component of the security infrastructure, and it is used to filter traffic that passes thru the network perimeter.

With the new blended threats, different technologies such as Firewall, IDS, Antivirus and Content Filtering are being integrated into one single product, to provide different checks and levels of protection at the gateway.

There are good products made by reliable companies that have background infrastructure and commitment on the continuous development of technologies and release of product updates. There are new Attacks every day, and security products should be in constant process of evolution, and the perimeter is one important place to install such defense technology.

**References:**

[1] "Study: Broadband growth will continue"
URL: http://news.com.com/2110-1033-268316.html (apr 30, 2002)

[2] "Guidelines for configuring your firewall rule-set"
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2707159,00.html (apr 30, 2002)

[3] "Three basic types of firewalls"
URL: http://supportnet.merit.edu/m-intsec/t-firewa/text/3kinds.html (apr 30, 2002)

[4] "Building Your Firewall Rulebase"
URL: http://www.enteract.com/~lspitz/rules.html (apr 30, 2002)

[5] “Symantec Enterprise Firewall 7.0 – Configuration Guide”
URL:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/manuals/7.0/sef_sevpn_70_config.pdf (apr 30, 2002)

[6] “Cisco – Access VPNs for the Enterprise”
URL: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/justify/avpnn_bc.htm (apr 30, 2002)

[7] “Why choose integrated VPN/Firewall solutions over Stand-alone VPNs”
URL: http://www.checkpoint.com/products/security/whitepapers/firewall-1_integrated.pdf (apr 30, 2002)

[8] “Special Report: Securing The New Perimeter”
URL: http://www.networkmagazine.com/article/NMG20010518S0006 (apr 30, 2002)

[9] “Symantec Desktop Firewall 2.0 User’s Guide”
URL:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_desktop_firewall/manuals/sdf.pdf (apr 30, 2002)

[10] “Symantec Firewall/VPN Appliance Installation and Configuration Guide”
URL:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_firewall_vpn_appliance/manuals/fwvpn_100_200_200r_install_config.pdf (apr 30, 2002)

[11] “Symantec VelociRaptor 1.1 Installation and Configuration Guide”
URL:
ftp://ftp.symantec.com/public/english_us_canada/products/symantec_velociraptor/1.1/manuals/vr11_install_config_guide.pdf (apr 30, 2002)

[12] “Symantec Gateway Security”
URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133 (apr 30, 2002)

[13] “Symantec Enterprise VPN 7.0”
URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=54 (apr 30, 2002)

[14] “RainWall High Availability Software for Symantec Enterprise Firewall and Symantec Enteprise VPN”
URL: http://www.rainfinity.com/products/ds_rainwall_symantec.html (apr 30, 2002)

[15] “Responding to the Nimda worm: Recommendations for addressing blended threats”
URL: http://www.symantec.com/avcenter/reference/nimda.final.pdf (apr 30, 2002)