

# NETWORK SECURITY AND THREATS IN MODERN ERA-REVIEW

Ku. Ragini. S .Dubey

ME, CSE, PRMIT, Maharashtra, India

---

**Abstract:** One of the most difficult challenges in computer network is the computer network security .This paper presents the various network security and different threats, which causes to computer system. Almost all organizations and sectors are currently faced with the problem of insider threats to vital computer assets. Internal incidents can cause more than just financial losses. The three primary goals of network security which are confidentiality, integrity and availability are achieved by setting the security goal. The complexity of these functions can cause significant delays in the processing of packets, resulting in degraded performance, traffic, bottlenecks, and ultimately violating Quality of Service constraints.

**Keywords:** Network security, Service constraints.

---

## INTRODUCTION

### *Part 1 - Evolution of Network Security and Prevention Techniques:*

The past few years have seen a radical evolution in the nature and requirements of network security. There are many factors contributing to these changes, the most important of which is the shift in focus from so-called 'network-level' threats, such as connection-oriented intrusions and Denial of Service (DOS) attacks, to dynamic. Finally, threats are just as likely to come from inside the local network as they are from the Internet. One trend alone overshadows all others in this regard; users are taking their laptops home at night and over the weekend, where they are at increased risk of becoming infected or compromised. When the laptops are brought back into the office, the entire network is at risk since the user entered the network "behind the firewall". This is one of many reasons that an emerging "best practices" in secure network design is to segment the network into separate "security zones" (by physical or logical segmentation) such that attacks can be contained in the event of an outbreak, content-based threats such as Viruses, Worms, Trojans, Spyware and Phishing that can spread quickly and indiscriminately, and require sophisticated levels of intelligence to detect.

There are several major drivers that are shaping the new security landscape:

#### **1 - Increasing complexity in networks**

Where a network 10 years ago might have consisted of a LAN connected to the Internet through a WAN connection, and maybe a few remote accesses or site-to- site VPN tunnels, the reality today is much more complex. A common environment today will have multiple access mechanisms into the network, including 802.11 wireless LAN (with myriad Client devices including portable computers, PDAs and Smart Phones), web portals for partners and customers, email servers, end-users using new communication platforms (such as Instant Messaging) and peer-to-peer applications for file-sharing. An example of such a network, and the threats that are present, is illustrated in Figure 1.

In addition, the workforce is becoming more mobile. From telecommuters who work from a home office to mobile workers who are never in a particular location for more than a day, this growing "distributed" model adds a significant

amount of risk to the network. To help mitigate these risks, the IT manager must ensure that all remote locations and remote clients are protected with the same level of security as is present in the corporate network.

Finally, threats are just as likely to come from inside the local network as they are from the Internet. One trend alone overshadows all others in this regard; users are taking their laptops home at night and over the weekend, where they are at increased risk of becoming infected or compromised. When the laptops are brought back into the office, the entire network is at risk since the user entered the network "behind the firewall". This is one of many reasons that an emerging "best practices" in secure network design is to segment the network into separate "security zones" (by physical or logical segmentation) such that attacks can be contained in the event of an outbreak.

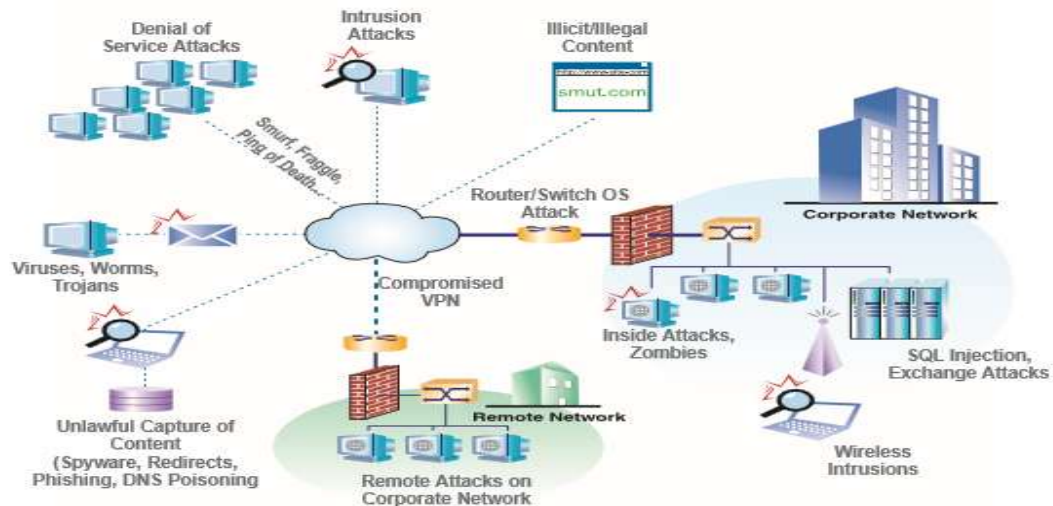


Figure 1 - Prevalent threat vectors in today's networking environment

## 2 - Increasing sophistication of applications and attacks

Applications are growing in complexity. Where Windows NT launched with 5 million lines of code in 1994, Windows Vista has over 50 million... more than 1,000% growth! With this increased complexity comes increased vulnerability, particularly in server systems, which must be patched on a regular system.

While applications are becoming more sophisticated, so are the attacks. A "serious" attack in the early 2000's might have consisted of a simple indiscriminate DOS attack aimed at restricting or temporarily disrupting network access. Today's serious attacks target applications themselves, and in many cases have goals of significant criminal intent, as is demonstrated by the Sasser worm described below.

### Intrusion Attacks, Worms and Trojans:

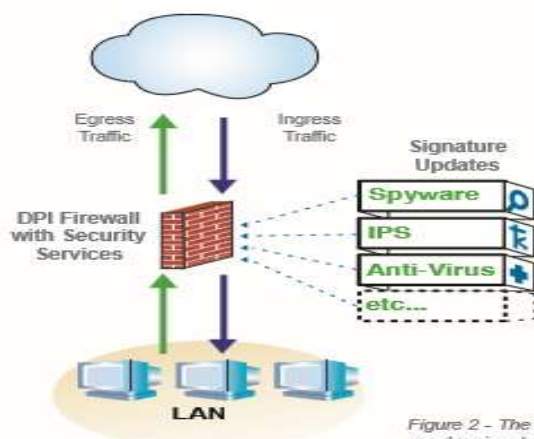
The grand-daddy of them all, the universe of Intrusion attacks is wide and deep. Intrusion attacks are modern threats that target applications and application layer protocols (e.g. using the SMTP protocol to exploit a buffer overflow on an Outlook Exchange server), rather than the networks they are transported on (e.g. DOS attacks that utilize ICMP echo and TCP SYN floods). Examples of common Intrusion attacks are Worms, Trojans, web site cross-scripting, SQL injection and tampering, Outlook Exchange server attacks, Apache/IIS buffer overflow attacks, file-path manipulation etc.

The security appliance is now a dynamic threat prevention system that requires constant, real-time updates to its attack signature libraries, URL lists, virus definition files, etc. to ensure the network.

### Viruses:

Viruses (and Worms) are a class of attack whereby an infected attachment or download causes damage to a host system or network. The damage can range from minor (client DOS attack) to catastrophic (full-blown corruption of critical stored

information or system registries). A critical trend that is resulting from the increased sophistication of Viruses is the rapidly decreasing "window of infection". In July of 2001, it took the Code Red virus just under 6 hours to infect 359,000 clients. Just eighteen months later, the Slammer worm infected 75,000 clients in under 30 minutes. The threats are real and spread fast. Security vendors have responded by trying to decrease their own "windows of inoculation" which is the time it takes to detect a threat, issue a patch release, and download it to its host Systems under management.



A major impact of IPS (and the other DPI-oriented technologies described below) is that the security appliance is no longer a static element that sits in the network.

The security appliance is now a dynamic threat prevention system that requires constant, real-time updates to its attack signature libraries, URL lists, virus definition files, etc. to ensure the network is protected against threats that are present this hour... as well as those of last week, last month and last year.

Figure 2 - The security appliance is now a dynamic system that requires regular signature updates

There is also a new class of virus-related attack called a 'blended threat'. A blended threat is a 'perfect attack' whereby a virus is accompanied by a number of other attack and intrusion techniques to maximize penetration and damage. A good illustration of this type of attack is the So Big virus detailed below.

So Big and Sasser are good examples of how complicated it has become to detect and prevent sophisticated application-layer attacks. To protect against these types of attack, it is mandatory to have IPS and Gateway Antivirus (GAV) installed and activated in the network, whether it is provided by a Deep Packet Inspection is protected against threats that are present this hour... as well as those of last week, last month and last year.

### 3 - Financial rewards for hackers with the advent of Spyware and Phishing:

The Internet has evolved from being a general information source to a critical enabler of international commerce. Because of the sensitive type of information that now flows freely over the Internet, a new breed of threat aims at obtaining this information... sometimes honestly and sometimes with malicious intent. Because the information obtained in these types of attacks has value, hackers are being financially compensated for their work, often by major public corporations; sometimes by organized crime. This is a particularly disturbing trend, since it is attracting the best and the brightest one-time programmers into the black-hat world of hacking and malware generation.

#### Spyware:

Spyware (and Adware) is one of the most misunderstood of the new generation of application-layer threats because there is no consensus on what defines a threat (or more appropriately, what the difference is between 'annoying' Adware and a true threat).

There are three general classes of Spyware:

- **Harmless-but-annoying:-**

Generally consists of actions such as changing the default home page of your browser, or unsolicited/untargeted pop-up ads.

- **Information-collecting:-**

Cookies are the most common type of information collecting mechanism, but simple keystroke and activity loggers are becoming more common. This class of Spyware is generally interested in collecting basic information about you, the

sites you visit, and other preferences so that a 3rd party can send you targeted ads or promotions. There is generally not malicious intent, but many would call this an invasion of privacy.

- **Malicious:-**

Collecting private information with the intent of sending the information to a collection server. The information is collected, and sold to 3rd parties who have varying interests. Even today, this type of Spyware can be downloaded instantly on a Client device simply by visiting a URL... no further clicking necessary. This type of Spyware is illegal and critical for an organization to detect and stop.

To further add to the complexity, there are three major Spyware delivery mechanisms:

- ✚ **Embedded Installs :-**

The most 'honest' of the three mechanisms, embedded installs are typically Spyware/Adware elements that are embedded into programs or services that are downloaded from the web.

- ✚ **Drive-by Installs:-**

In this method, a banner ad or popup attempts to install software on a PC, usually through the ActiveX controls distributed within Windows and by default enabled in Internet Explorer. Depending on the security settings on the PC browser, the Spyware downloads silently or was downloaded when the user clicked 'Yes' in the installer dialogue box. In many cases, Drive-by's also take advantage of browser exploits that can force an unsuspecting PC browser to automatically download and execute code that installs the Spyware.

- ✚ **Browser Exploit :-**

As described above, targets vulnerabilities in the web browser code to install Spyware. A classic example is the Internet Explorer iFrame vulnerability. Because IE is such a targeted browser, many IT departments are migrating to alternate browsers such as Mozilla's Firefox. This is only putting off the Spyware is difficult to stop because it requires so many technologies to detect and prevent the exploit. A robust Spyware prevention architecture will consist of both client/server and gateway-based elements.

Client and server based Anti-Spyware software will detect and try to prevent users from accessing known bad sites, and to a limited extent provide more advanced functionality to detect suspicious behaviour from actual downloads and ActiveX controls. The software will also inspect individual system memory, system registries, start-up files and other stored items to detect and remove Spyware. While necessary, client and server based Anti-Spyware software is not enough.

Since Spyware is carried by so many delivery mechanisms and is getting so sophisticated, an additional gateway-based Anti-Spyware element is required. The gateway element not only reinforces URL filtering to prevent access to known bad sites, but provides thorough IPS functionality that detects abnormal behaviour from ActiveX Controls and Java Applets and the like, and also provides Anti-virus functionality that inspects attachments for malicious code that installs Spyware. The gateway is also an effective tool for scanning both Instant Messaging (IM) and peer-to-peer protocols/programs, which are a growing target for Spyware and other attacks. Perhaps most importantly, a gateway-based Anti-Spyware solution mitigates the harmful outbound effects of pre-infected client and server devices (that might be attempting to contact a collection server on the Internet to deliver sensitive personal or company data, for instance). Phishing scams can get quite sophisticated; it is not unusual for a hacker to re- create an entire web-site in an effort to look legitimate. Worse yet, there are other Phishing-related threats that are much more serious. With Phishing, an informed user can fairly intelligently determine if what they are being asked to do is normal practice. With a new threat such as Pharming, also called DNS route poisoning, the DNS servers themselves are compromised, and the DNS entries are modified to point to criminal websites. With a good job of re-creating the target web site, Pharming can be very hard to detect. In a 'nightmare' scenario the user types in their target URL, where the compromised DNS server sends them to an innocuous looking, but malicious website. The user then types in their username and password in the bogus web server, which the criminals collect. Finally, before the user knows anything malicious has happened, they are re-directed to the official web server, where they are already logged in and can access their account as usual. All of this is completely transparent to the end user. While this sounds far-fetched, it is an increasingly regular occurrence.

Like Spyware, Phishing is a complicated threat to detect and prevent. The IT administrator's security schema must not only have Spyware software as a mandatory element on the client side, but also at the edge of the network itself on the security gateway. Not only will the gateway prevent Phishing from occurring in the first place, but like Anti-Spyware, it will help mitigate the outbound effects of users who inadvertently accessing something they should not be.

#### **4 - Governmental regulations compliance:**

Another important trend affecting network security is the growing number of governmental regulations in the US and abroad. One popular example of recent US regulation is the Health Insurance Portability and Accountability Act (HIPAA), which regulates how and when sensitive medical patient data can be transmitted. This regulation mandates that health organizations have Intrusion Prevention and secure connectivity (e.g. VPN) technologies in place to ensure conformance. Another recent US regulation is the Children's Internet Protection Act (CIPA), which aims at protecting minors from pornography, obscenity and other material harmful to minors. CIPA conformance mandates that all publicly accessible Internet connections are protected by URL and Web Content Filtering, which ensures only "proper" sites are accessible from the PC. These are examples of US regulations; almost every nation has, or will soon have, similar regulations in place.

Where the government has been lenient on conformance up to this point, they are starting to become much stricter on enforcing and penalizing violators.

#### **5 - Security as a tool to increase workforce productivity**

One of the most profound impacts of security is how it is utilized across all types of organizations to increase operational efficiencies through enhanced workforce productivity. There are two main technologies that are helping achieve this:

**Web Security and Policy Enforcement** It is no longer a secret that a good amount of an average employee's day can be spent online doing non-work-related activities. Web surfing, online shopping, online gambling, stock trading and even online dating are a few of the more common uses of company Internet resources.

In what many employees might consider a breach of privacy, the company employing URL filtering technology can monitor and report on individual Internet usage, and can also set scheduled restrictions on what types of sites employees are allowed to access throughout the day. If the company is using this type of technology, eSoft highly recommends that the HR department make public notice that this technology is being used, and also clearly state (in the employee handbook, for example) the rules and restrictions of employee Internet usage. The figure above shows a typical screen an eSoft user will see when they are trying to access a site that was banned by an IT department employing eSoft SiteFilter technology, described later in this document. URL filtering is also a necessary tool for reducing liability that stems from illegal and unethical use of the Internet in public places or organizations. A classic example of this is where an employee (or Internet café patron, for that matter) is accessing a porn site, and another person walks by, witnesses the activity, and sues the company for emotional distress or a hostile work environment. Libraries and schools, by their very nature, MUST have this type of technology deployed.

In addition to workforce productivity and liability protection, URL Filtering technology is also the first line of defence at preventing users from accessing Spyware sites. As noted in the previous section, however, Spyware is a much more complicated problem than URL filtering alone can handle.

#### **SPAM**

Spam has grown into a major problem for all companies and organizations. Spam is especially problematic for public email addresses (listed on a website, for instance), or for common email addresses (support@your\_company.com). Spam is also the primary delivery mechanism for Phishing attacks, so its importance has grown over the years. In 2006, over 86% of all e-mail was classified as spam. Over 63% of this spam originates from new or unknown sources.

Spam is best dealt with at the security gateway. The reason for this is simple... once Spam emails are inside the network; they are already consuming precious network resources (such as storage, bandwidth and mail server CPU cycles). If prevented before they ever get to a mail server, Spam can become a more manageable nuisance and threat. Another reason Spam is best dealt with at the security gateway is the sophistication of the tools and techniques that are possible to implement at the gateway. Technologies such as word filtering, Bayesian filtering, black and white lists, real-time black hole lists (RBLs), DNS MX record lookups, reverse DNS lookups, sender policy framework (SPF) compliance and other techniques are all mandatory for effective Spam mitigation. A good gateway Spam filter will reject Spam in such a way that the Spammer will eventually remove the target from their Spam list.

For many technologies such as Bayesian filtering, it is necessary to have many, many samples of known spam, and known ham (non-spam) to begin the heuristic process of self-learning. This is another advantage of Anti-Spam technology at the gateway, where there is visibility into every email coming into or exiting the network.

### **Part 2 - Issues with Current Security Solutions:**

Whether dealing with Intrusion attempts through application buffer overflows, Spyware through drive-by installs, Phishing through deceiving emails or any of the other threats described in this paper, there is one capability the security appliance requires above all else: Deep Packet Inspection (DPI) intelligence.

To understand why, it is useful to look at the makeup of a typical Ethernet frame and how a traditional firewall processes it.

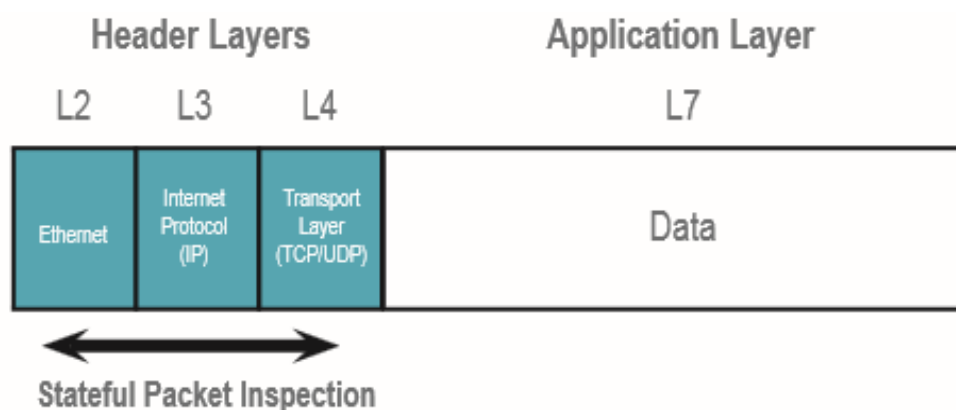


Figure 7 - Ethernet frame and how Stateful Packet Inspection (SPI) views it

As shown in the Ethernet frame above, Stateful Packet Inspection (SPI) essentially has access to Layers 3 and 4 of the OSI stack (sometimes Layer 2, as well). SPI firewalls perform the 'classic 5-tuple lookup' that is, they scan and make allow/deny decisions based on:

1. Source transport layer address (typically TCP or UDP)
2. Destination transport layer address (typically TCP or UDP)
3. Source IP address
4. Destination IP address
5. Service type (e.g. FTP, HTTP, SMTP, and POP3)

What does this really mean? Using a Post Office analogy, the SPI firewall essentially looks at the To and From addresses on a package, as well as the package type (tube, box, letter, etc), and makes a decision about whether to mail the package based on pre-defined rules. There is no knowledge of what is inside the package.

SPI firewalls are generally regarded as "network-layer" security devices, as they provide no protection for anything above Layer 4.

The figure below shows the same Ethernet frame, but this time with application-layer information.

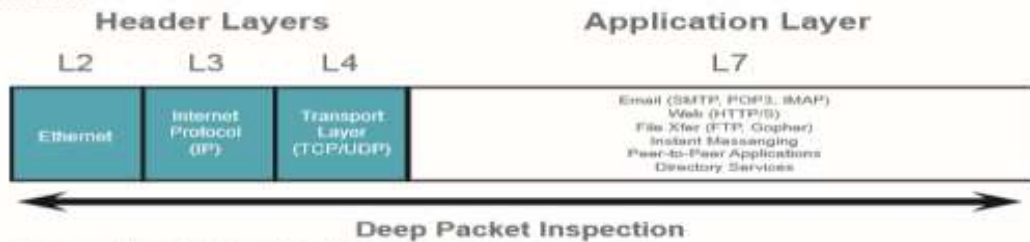


Figure 6 - Ethernet frame and how Deep Packet Inspection (DPI) views it

In addition to the classic 5-tuple lookup, DPI firewalls have "application awareness". Application awareness is a very broad term, but in general it means that the security appliance understands L7 protocols such as HTTP, SMTP, POP3, IMAP and FTP, and also understands the actual applications that rely on those protocols. For instance, Microsoft Outlook Exchange Server relies heavily on the SMTP protocol; Microsoft Explorer and Mozilla Firefox rely on the HTTP protocol, etc. In addition, there are custom protocols for applications such as Instant Messaging, Microsoft SQL Server, Oracle Server, Siebel, etc.

DPI-capable appliances must also have the associated security services that allow them to protect against Spyware, Viruses and other app-layer intrusions. Most vendors, eSoft included, offer these services as optional software modules... purchase the basic security appliance, and add services in an a la carte fashion depending on network need.

As stated previously, the basic nature of network security has evolved to a point where the MANDATORY services for any gateway security appliance are Intrusion Prevention and Gateway Antivirus. Without these, the network and its users are only partially protected.

### Part 3 - Current Network Security Alternatives:

To protect against modern network threats, there are essentially two deployment architectures that are available to the IT manager:

- Deploy a next-generation DPI firewall that performs traditional SPI firewall functionality, as well as DPI application security, or
- Deploy a DPI Content Security appliance that sits behind an existing SPI firewall

Both of these approaches are illustrated in the Figure 9 below. In the latter example, the Content Security appliance is typically configured in transparent mode, where the device sits 'invisibly' between the firewall and the switch such that subnets do not have to be re-mapped. The device examines all traffic in a 'promiscuous' mode, where it makes forward/drop/log/quarantine decisions based on what services are activated (e.g. Anti-Virus, Intrusion Prevention, Anti-Spam, Anti-Spyware, URL Filtering and Spam Filtering).

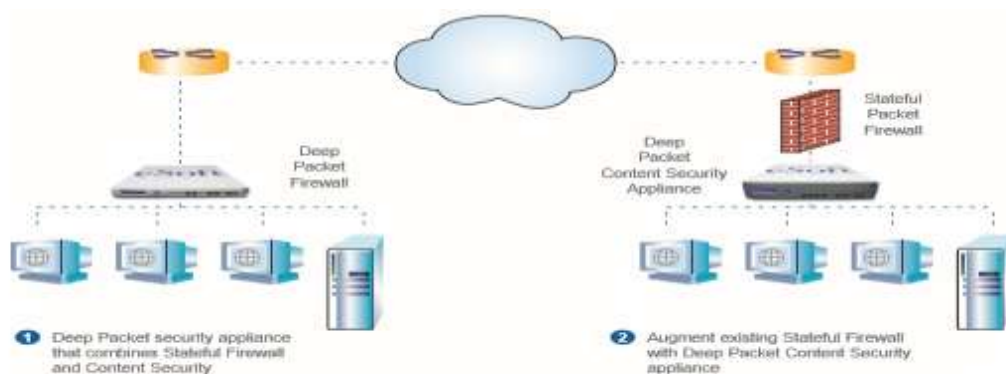


Figure 9 - Modern alternatives for Deep Packet security

**Part 4 - The eSoft Solution:**

eSoft offers a complete line of next-generation Deep Packet Inspection security appliances that fit into either deployment scenario described above.

**InstaGate Integrated Security Gateway**

The InstaGate line Integrated Security Gateways provides state-of-the art Firewall and IPSec VPN functionality, in addition to DPI services such as Anti-Virus, Intrusion Prevention, Anti-Spyware and Anti-Spam. In addition, for the IT manager who wants FULL integration, many of the InstaGate products can be configured with optional office server elements such as Internet server, Email server, Webmail server and File/FTP and Print servers. InstaGate gateways currently integrate Deeper Packet security services than any other vendor on the market

**ThreatWall Content Security Appliances**

The ThreatWall is an award-winning platform that performs ultra-high-performance Deep Packet Inspection services such as Anti-Virus, Anti-Spam, Web URL Filtering as well as Intrusion Prevention, Anti-Phishing and Anti-Spyware. ThreatWall is tailored for networks with an existing Firewall/VPN system, and can be deployed either in-line in Transparent mode, or in an off-line proxy mode, making it exceptionally versatile for diverse network environments. Additionally, the Threat Wall scans in both inbound and outbound traffic, obviating the necessity for different devices to be dedicated to inbound and outbound traffic (which many manufacturers require).



Figure 10 - InstaGate Integrated Security Gateways

SoftPaks and the SoftPak Director At the core of both the InstaGate and ThreatWall appliances is eSoft's patented (U.S. Patent No. 6,961,773 B2) and industry-renowned SoftPak and SoftPak Director (SPD) architecture for enforcing and managing Deep Packet Inspection services. As shown in Figure 12 below, SPD is the mechanism by which:

- Software services are added to the InstaGate and ThreatWall products
- Signature updates are automatically scheduled and downloaded to each device
- Subscription maintenance and billing is performed

**ThreatPaks:****Network ThreatPak**

Modern network threats such as Spyware, Worms and Trojans were built to bypass traditional firewalls. Worse yet, technologies such as Instant Messaging (IM) and Peer to Peer networking have opened up serious holes in the security fabric that are incredibly hard to detect and prevent. The Network ThreatPak combines many of eSoft's proven security technologies to provide the network and its user's protection from the dynamic threats that cause network outages, Virus infections, Spyware installs and loss of intellectual property.

Features:

- Real-time Spyware Protection
- Active Intrusion Prevention



- Gateway Anti-Virus for Web and FTP
- Instant Messaging and P2P Application Control
- MySpace and Social Networking Application Control
- eSoft Distributed Intelligence Architecture Integration
- Detailed Reporting and Statistics

### **Web ThreatPak**

Assure maximum workforce security and productivity by monitoring and enforcing the use of organizational Internet resources. Web ThreatPak also protects against legal liability brought on by inappropriate/illegal use of Internet resources. A database containing millions of global URLs is continually updated with web sites in 30 categories. Policy based control allows selection of which categories should be blocked at different times of day, and which users are affected.

Features:

- a) Millions of URLs
- b) Block Spyware Sites
- c) Automatic Updates
- d) Custom Categories
- e) Authentication
- f) User/Group Policies
- g) Day/Time Policies
- h) Logging and Reporting
- i) Custom White/Black Lists
- j) Custom URLs
- k) Integrated Web Caching
- l) Custom Block Message
- m) Simple Installation
- n) Web Based Administration

### **SoftPaks:**

#### **Desktop Anti-Virus / Anti-Spyware**

This easy-to-deploy SoftPak, which combines full Anti-Virus and Anti-Spyware protection into a single, easy-to-manage client, is a key tool in protecting the organization from costly network outages caused by Viruses, Worms, Trojans and Spyware. Automatic signature updates and 'invisible' deployment ensure that users are always protected at the maximum level. The user may not uninstall the software.

This client proactively protects users from internal threats such as Disk, CD or USB and prevents Spyware on laptops that leave the corporate network. Administrators can set policy controls to quarantine, trust or delete various levels of Spyware. Policy controls are also defined to keep IT managers informed of threats with custom reports and Spyware alerts which are all logged back to the server console.

#### **Gateway Anti-Spyware**

Gateway Anti-Spyware combines signature matching, intrusion prevention and web filtering techniques to detect and prevent Spyware from infecting the network, whether delivered by web, email or other delivery mechanisms. Infected computers on the internal network are also detected and blocked from sending private data to Internet collection sites. Proactive security at the gateway stops new Spyware infections, prevents confidential data from leaving the network and eliminates resource drains that result from reactive measures of constantly scanning and cleaning each computer on the network.

## SiteFilter

Filters Internet content according to your organization's security policies and user guidelines. It allows you to manage Internet access ranging from simple access restrictions to complete blocking of any site. SiteFilter includes a base access control list of more than four million URLs covering 12 languages, all categorized into 40 different content groups, ten of which you can define and customize. In combination with Threat Wise Technology, SiteFilter enables implementation of highly customized and detailed access restrictions-by category, user, day, and time-for improved business productivity and liability control.

### Features:

1. Automated Signature Updates
2. Real Time Black hole Lists
3. Customizable White and Black Lists
4. Phishing Protection
5. Attachment Stripping
6. Compressed/Archive Files
7. Address Verification
8. SPF (Sender Policy Framework)
9. Bayesian Filtering
10. Heuristic Analysis
11. Rule-based Spam Scoring
12. Historical Averaging
13. Keyword Filters
14. Reject, Redirect, and Tagging Email Policies
15. Admin and User Quarantine
16. Web-based Administration
17. Reports, Statistics, and Graphs
18. Simple Installation

## CONCLUSION

The evolution of network and application-layer security threats has significantly altered the requirements for modern network security architecture. Just a few years ago, a simple Stateful Packet Inspection (SPI) Firewall was sufficient to stop basic attacks such as port scans and DOS attacks. Now, application-layer buffer overflow attacks, Spam, Spyware, Polymorphic Trojans, Blended Threats, Phishing and Pharming are causing unprecedented amounts of financial damage and loss of productivity.

To detect and prevent these threats, a completely new kind of security system is required. This system still performs all of the classic functions of the firewall, but much more. This system is based on Deep Packet Inspection (DPI) technology, where the appliance has the brains - and the horsepower- to inspect every byte of every packet even across multiple thousands of streams of packets. The modern DPI security appliance resembles its SPI predecessor only by its looks inside is a completely new system, designed from the ground up to deal with the rigors of in-depth packet inspection. The DPI security appliance also differs from its SPI predecessor in that it requires real-time security services to ensure it is protecting against threats that are not only relevant this week, but also this hour. The great news for the IT manager is that these security services are typically broken down into optional a 'la carte services where they can be deployed on an as-needed basis.

## ACKNOWLEDGMENT

The work has been guided by Prof. Gupta sir, ME cse, PRMIT, Maharashtra India. The Authors would like to thank all the concerned people.

**REFERENCE**

- [1] C. Chen, P. Maniatis, A. Perrig, A. Vasudevan, and V. Sekar, "Towards verifiable resource accounting for outsourced computation," in Proc. of ACM VEE, 2013.
- [2] Z. Wang, C. Wu, M. Grace, and X. Jiang, "Isolating commodity hosted hypervisors with hyper lock," in Proc. of Eros's 2012.
- [3] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimall, and L. Flynn, "Common sense guide to mitigating insider threats, 4th edition," Software Engineering Institute, Carnegie Mellon University, Tech. Rep. CMU/SEI-2012-TR-012, 2012.
- [4] M. Salem, S. Herskop, and S. Stolfo, "A survey of insider attack detection research," Insider Attack and Cyber Security, pp. 69–90, 2008.
- [5] B. Lampson, "A note on the confinement problem," Communications of the ACM, vol. 16, no. 10, pp. 613–615, 1973.