Global Information Assurance Certification Paper

Protecting the Perimeter

Symantec Gateway Security Appliance

An Integrated Solution

Author: Alexander Austein
Date: 3-Jun-03
Assignment: v1.4b Option #2

Table of Contents

Abstract

As organization networks become more dependent on external data sharing and "e-enabled" applications these networks need to be more accessible and operational. But not only accessibility to the networks become easier, access to critical data they store becomes easier too.

Blended threats: threats which combine the characteristics of viruses, worms, Trojan horses, Hacker technologies and malicious code are compromising the security of entire networks.

Today's security solutions are typically comprised of multiple point products, resulting in a lack of interoperability, manageability and higher cost of ownership. The concept of integrated security is an effective approach to address blended threats as well as new challenges. The combination of multiple security technologies improves manageability, enhances performance, tighten security and reduce costs.

This paper provides an overview of the growing sophistication of network attacks and describes the key elements and benefits of an integrated security solution.

Executive summary

Every network has demarcation point that separate the trusted network from the untrusted network. The points provide control over the flow of network traffic and are a logical location to place security appliances. Appliances are devices that are self contained, centrally manageable and require little or no support by the end-users at the location where they are installed.

Types of network attacks

Common types of threats include:

Malicious Code Attacks

Usually viruses, worms and Trojan horses that hide within files or programming code only to self-replicate, self-propagate, or be spread by unknowing computer users. These attacks are capable of damaging or compromising the security of individual computers as well as entire networks.

Denial-of-Service Attacks (DoS)

Are explicit hacker attempts with the intention to disrupt normal business operations. Typical examples are "flood" attacks thereby blocking legitimate traffic and disrupting connections between two machines, thus preventing access to a service. These attacks are capable of disabling a single computer or entire networks.

Distributed Denial-of-Service Attacks (DDoS)

Basically the same as a DoS whereas the attack is done from hundreds or thousands of source machines. Due to the enormous data flow servers, corporate networks as well as internet backbones may breakdown.

Unauthorized Access - Hacking

Hackers are people who are able to gain access and control over computers, information and technology without proper authority. Today's hackers are exploiting security vulnerabilities using methods and technologies like "buffer overflows" to break a system. This modern hacker generation does not have any "hacker ethics". They are often young people – "script kiddies" - who do not have the technical knowledge to break into a system but ready-to-use exploits, attacks, etc. can easily be downloaded from the web and used to attack computers.

Blended Threats

These threats combine some or all of the characteristics described above. By utilizing multiple methods of attack and self-propagation they can spread rapidly and cause widespread damage. Blended threats such as Nimda and CodeRed are designed to exploit the vulnerabilities of security technologies working independently from one another.

Impact of network attacks

Network attacks range from easy-to-quantify consequences such as interrupted business operations, to losses that are difficult to calculate (e.g. damaged brand equity).

Interruption of business operations

Downtime due to an attack results in lost productivity and the costs associated with restoring a hacked network can increase the overall financial impact of an attack. Once attacked an organization typically deploys a "cleanup team" to resume business as soon as possible, but the cleanup team is pulled away from its daily duties, compounding productivity loss.

Damage to brand equity

Damage to a company's brand is degrading their position in the marketplace. For example, companies who have had customer data stolen and publicly displayed on other web sites have a hard time restoring customer confidence in their brand.

Reduced ability to compete

Information is considered a company's most valuable asset. The loss of that data can degrade their possibility to compete in the marketplace. For example, confidential development data stolen and publicly published by a hacker may result in being unable to be the first bringing out a new generation of software, hardware, etc.

Legal Liability

Organizations that have been hacked may find themselves in court as a defendant or witness. Especially organizations which are required to comply with privacy and security regulations (e.g. health care, financial institutions) may need to demonstrate their due diligence in minimizing their exposure to network attacks.

Current security solutions and situation

Typical security solutions consist of multiple point products. The main disadvantage of this solution is that they need to be handled separately. All of them need to be installed, managed und updated but there is less or no interoperability between each of the products.

With this approach, protection is usually not comprehensive because cross-vendor interoperability issues often allow threats compromising security. When an outbreak occurs, fixes and patches may need to be tested, verified and applied across various platforms and technologies. This can slow response to attacks and leave the organization vulnerable for a longer time.

Integrated security – the logical solution

This security method combines multiple security technologies with manageability into one solution. By using the principles of defense in depth at multiple levels it can more efficiently protect against a variety of threats to minimize the effects of network attacks.

Integrated security reduces the need to install, update and manage multiple security products from multiple vendors or address interoperability issues between various vendors products.

In addition to these security solutions for attackers, adding a secure tunnel for authorized end-users would provide a speed lane for those folks with business to do and content filtering assists with an organization's liability issues, such as regulatory concerns for financial services.

At last, integrated security it may enable reallocation of IT personnel to other strategic projects, improving security manageability overall.

Integrated solution – Symantec Gateway Security (SGS)

Overview

The Symantec Gateway Security appliance is a multifunction appliance that provides the following security technologies in one system:

- Firewall
- Antivirus
- Intrusion detection
- Content filtering
- VPN
- High Availability/Load Balancing

All functions are managed from one central console and log to a central logging mechanism. As an additional option up to 8 appliances can be combined to a High Availability or Load Balancing cluster. As it as an appliance the administrator does not have to install an operating system, software and network environment – those components are already loaded and can be configured through the admin console.

Different technologies complement each other

The components offer different areas of strength in security solutions. The firewall components create perimeter defense mechanism to try and prevent many types of unsanctioned network traffic into or out of a network. Antivirus scanning adds a greater layer of security to check traffic for viruses or known malicious executables. Intrusion detection helps identify what type of attacks have occurred. VPN allows a corporation to extend the network to remote or travelling employees and to connect to regional offices or partner companies. Content filtering helps corporations enforce acceptable use policy, so that misuse of network resources does not occur. The High Availability/Load Balancing feature ensures that companies do not have a single point of failure or throughput bottleneck for communication through the network.

Case study: The CodeRed II worm

Technical details

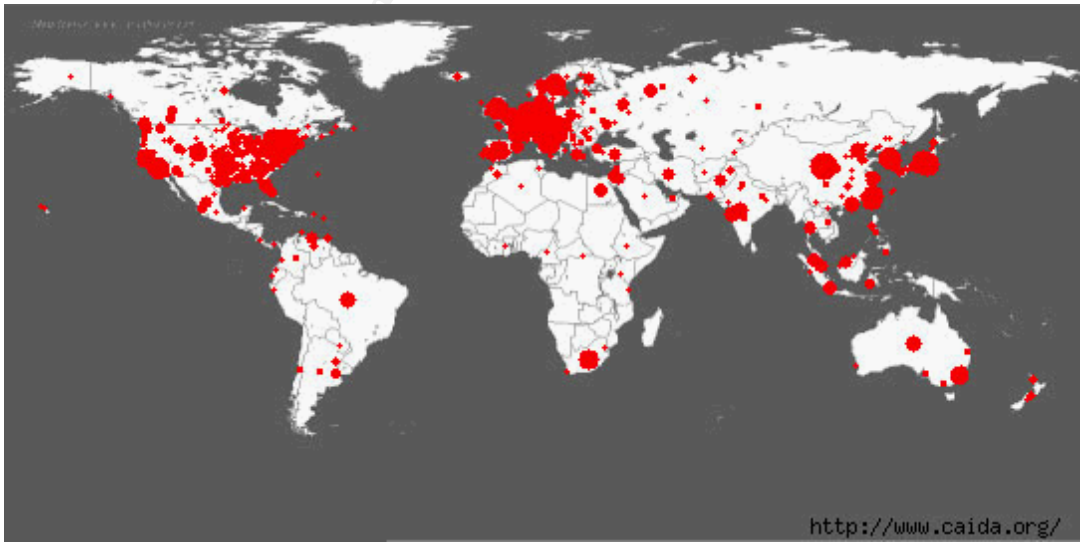
The worm propagates by installing itself into a random Web server using a known buffer overflow exploit. When a Web server is infected, the worm first calls its initialization routine, next it gets access to a set of API addresses:

The main thread checks for two different markers. The first marker controls the installation of the Trojan. The other marker is a semaphore named "CodeRedII." If the semaphore exists, the worm goes into an infinite sleep. Next, the main thread checks the default language and creates up to 600 new threads (depending on the language).

These threads generate random IP addresses which are used to search for new Web servers to infect. While these threads are working, the main thread copies the command shell (Cmd.exe) to the default execution - enabled directory of the IIS Web server, allowing a hacker to take full control of the Web server.

Note: The Nimda worm uses directory traversal techniques to access cmd.exe on IIS servers that had previously been compromised by CodeRed II.

The diagram below shows how effective CodeRed II spread over the internet.



Note: An animation of this diagram can be downloaded at http://www.caida.org/analysis/security/code-red/newframes-small-log.gif

How SGS defense against the CodeRed II worm

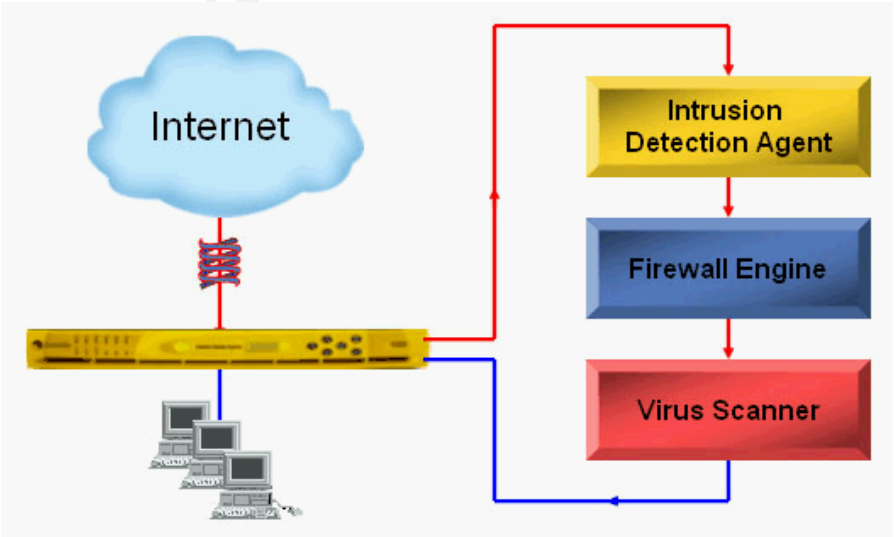
As we have seen the CodeRed II worm is a good example how blended threats can infiltrate corporate networks and the large impact they could have. SGS has the capability to detect and protect against the CodeRed II worm using 3 different mechanism:

1. Intrusion detection
   All traffic delivered to any interface is examined and compared by the built-in "path through" IDS to a known set of intrusion detection signatures (patterns). If there is a match, the system logs the information and reacts as configure d by the administrator. For example the system will block further packets from the source IP address.

2. Firewall
   All traffic delivered to any interface is inspected at the packet layer, circuit layer and application layer. To identify Layer 7 attacks a set of secure proxies is supplied w ith the appliance. If properly configured the secure proxy (in that case the HTTP proxy) w ill block the CodRed II w orm.

3. Antivirus
   The appliance incorporates several anti -virus technologies, including detection of unknown vir uses using heuristic algorithms, detection of complex polymorphic viruses or self -mutating viruses. Traffic is delivered to the anti -virus scanner by application proxies and the administrator defines what action to take should a virus be detected.

The dia gram below shows how traffic is handled by the appliance.



Note: The diagram is part of a Symantec presentation published on CD -ROM

Appliance security components - technical details

Hybrid firewall

The appliance contains a full inspection firewall, inspecting traffic at all layers (packet, circuit, application). The combination of stateful packet filter firewall and application proxy firewall results in high performance + high security.

1. Default application proxies supplied with the appliance:

   FTP, HTTP, HTTPS, Gopher, Telnet, CIFS, Exec, Login, NBDgram, DNS, NTP, Rating, NNTP, SMTP, Ping, RTSP, RealAudio, H323, Shell, ESMTP, WEBDAV

2. Generic proxies:

   TCP-GSP, UDP-GSP, IP-GSP

   The TCP and UDP GSPs (Generic Proxy Passer) are used to pass a protocol where no application proxy exists. This protocol can be defined with a single port or a range of ports. The IP GSP has similar functionality but it passes IP protocol traffic like PPTP, IPSec/IKE, etc.

3. Special Proxy: ALL*

   The All* proxy is a special mechanism which allows any given IP, TCP or UDP protocol to flow per the defined rule.

Network Address Translation (NAT)

The application proxies automatically enforce network address translation. Traffic that is passed to the application layer is automatically translated to hide all internal addresses. Outbound traffic is made to look like it came from the external IP address of the appliance. Inbound traffic is validated by the appliance through its state table and then redirected to its true internal address. This behaviour is configureable to allow for clients to be given special IP addresses from a NAT pool or to retain their original IP addresses. NAT can also be disabled for inbound traffic on an as needed basis.

Intrusion detection

The appliance has a special component in the kernel that examines all traffic delivered to any interface of the appliance. Traffic will be examined and compared to a known set of intrusion detection signatures that help to identify a break in attempt. If there is a match the system logs the information and reacts as configured by the administrator.

Most intrusion detection signatures are set "gated" by default. That means that the packet must be analyzed and accepted by the IDS engine before it can continue up the application layer to the proxies or other components. If the packet is found to match an IDS signature and it is gated, the packet is dropped. Non-gated signatures do not prevent the traffic from continuing on to the other components, however the traffic is still logged and can be configured to be blacklisted.

IDS signatures are automatically updated through Symantec's LiveUpdate technology. LiveUpdate can run on demand or scheduled to get daily, weekly or monthly updates.

Antivirus

The appliance uses a unique engine that can filter through layers of a file to search for viruses. It includes technologies which offer the ability to detect unknown viruses of various types using heuristic algorithms and detection of polymorphic and self-mutating viruses.

Traffic is delivered to the anti-virus scanner by application proxies. That means when the proxies and anti-virus components are configured, they work together to handle traffic. Traffic flows from the application layer proxies to the anti-virus scanner – it is scanned and returned to the proxies to pass the destination.

Three types of traffic can send to the anti-virus scanner – HTTP, FTP and SMTP. On all protocols the administrator defines what action to take should a virus be detected, what to do if the scanner is not available and what file type to look at.

Anti-virus definitions are automatically updated through Symantec's LiveUpdate technology. LiveUpdate can run on demand or scheduled to get daily, weekly or monthly updates.

VPN

The appliance supports site-to-site (also known as gateway-to-gateway) VPN connections where dedicated servers are used to negotiate the parameters of the VPN on behalf of the client system. Optionally the appliance can be upgraded (through a license key) to support client-to-gateway VPN too. The VPN engine is IPSec/IKE compliant and supports various authentication methods as well as two authentication protocols.

Authentication methods:

- Gateway password
- NT Domain (via RADIUS protocol)
- Defender
- CryptoCard
- Entrust PKI
- RSA SecurID
- Bellcore S/key
- Out of Band authentication

Authentication protocols:

- TACACS+
- Radius
- LDAP

Encrypted traffic entering the appliance can be sent up the protocol stack for extra checking using the supplied proxies. As the traffic that is entering the proxy is decrypted by the VPN daemon on its way in, rules can be applied to that specific protocol. VPN traffic can be NAT'ed before or after the packets are encrypted. Depending on the method choosen the receiving end must know what has taken place to decrypt the packets in the appropriate manner.

Content filtering

The appliance uses the WebNot URL database. This database is dynamically updated and contains a list of sites rated into various categories. Used with a rule this prevents access to websites within the selected categories. Attempted access is logged and the user will get a "Forbidden" message displayed in the browser.

Rating modification gives the option to re-rate sites as well as adding new sites manually – which retain across downloads of the database.

Once configured, a special service called "Fetcher" automatically downloads the database updates on a daily basis.

High Availability/Load Balancing

The appliance includes all of the components for software High Availability and Load Balancing, so the administrator does not have to load additional software. Two or more systems can be configured to work in a cluster, where all nodes are active, distribute the network load and pass traffic across the different systems. This differs from HA only solutions where one node is purely in standby mode. Up to eight nodes can be member of a cluster. If one system goes down, other systems automatically carry on and take the load of the non-functioning system.

Cluster environments have impact on how the network is setup. All inbound traffic needs to be routed to a special address called a Virtual IP (VIP) address. Additionally every packet passing the cluster will have its MAC address rewritten, so every packet looks like as it comes from one and the same device.

The cluster is managed trough a GUI called Symantec Raptor Management Console (SRMC). Configuration data is propagated by copying the configuration files across the different systems. This can be done from any cluster node, typically one specific node will be chosen which will function as the "main" node. Host specific information, such as unique interface references and keys are retained, all other common information will be overwritten.

Management

Initial setup of the appliance is done through the front panel. Optionally the front panel can be locked to prevent misuse and tasks like rebooting or doing a factory reset. In generally the appliance is managed trough a GUI called the Symantec Raptor Management console (SRMC) which handles the operating system and security configuration. Although the SRMC can handle all aspects of system configuration there is an additional utility called Secure Remote Login (SRL). SRL gives the option to connect to the appliance Unix OS shell as root and is provided for debugging and advance level use, such as manipulating the log files. SRL and SRMC sessions are always encrypted and authentication is used for this communication. The SRMC can be installed on any machine running Windows NT/2000/XP but for security reasons access to the appliance is only granted from IP addresses defined by the administrator.

Common tasks like reboot, shutdown, patch, backup, restore can all be done through the console. For example, configuration data of one appliance can easily be backup'ed and restored to the same or onto another appliance. Special tasks like manipulating the routing table can be done through the SRMC too. Additionally there is built-in editor which allows to manipulate configuration files directly without the need to use the SRL.

The appliance logs each connection attempt, all intrusions, tunnel connections, viruses detected, etc. The log files are stored on the built-in harddisk of the appliance and may become very large in high usage environments. So it is recommended to move them off the appliance to another machine on a regular basis.

Technical specifications

Maximum throughput:	Up to 90 Mbps
Sustained throughput:	40 Mbps (T3)
Easy to use and manage:	yes
Support information offered:	1 Year Gold Support induded
Recommended network size:	Up to 1000 (unlimited)
Remote-to-Site VPN:	Option
Site-to-Site VPN:	Standard
High Availability and Load Balancing:	Option
Firewall:	Full inspection
Antivirus:	Carrier class AV
Intrusion Detection:	Pass through
Content Filtering:	URL
Weight:	23.5 lbs (10.7 kg)
Dimensions:	44.5W x 57.7D x 4.5H
Ethernet Ports:	4 independent 10/100 Base-T
Serial Ports:	2 ports
UPS support:	yes
Front panel:	2 Line x 16 LCD
Input rating:	100/240 V, 50/60 Hz
Typical operation power consumption:	100 Watts
Maximum power consumption:	130 Watts
CPU:	Intel compatible processor
Harddisk:	40 GB

References

Books

Building Internet Firewalls
O'Reilly & Associates /WA
ISBN: 1-56592-871-7

Practical Unix & Internet Security
O'Reilly & Associates /WA
ISBN: 0-596-00323-4

Computer Security Basics
O'Reilly & Associates /WA
ISBN: 0-937175-71-4

URLs

Symantec Web Site
http://www.symantec.com
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=133

FireTower Internet Security
http://www.firetower.com/

Cooperative Association for Internet Data Analysis (CAIDA)
http://www.caida.org

The Spread of the Code-Red Worm (CRv2)
http://www.caida.org/analysis/security/code-red/coderedv2_analysis.xml

Internet Firewalls: Frequently Asked Questions
http://www.interhack.net/pubs/fwfaq/

Intrusion Inc.
http://www.intrusion.com/

PC Magazine
http://www.pcmag.com/article2/0,4149,274319,00.asp

Information Security
http://www.infosecuritymag.com/2002/aug/testcenter.shtml

Last Updated: May 30th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event