Global Information Assurance Certification Paper

An Approach for a Secure Enterprise Network

Robert Suarez
December 12,2001
Version 1.2F

I. Introduction

In today's environment there is more of a need than ever for increased security in enterprise level networks. Companies are finding themselves with offices around the world and needing a way to cost effectively provide high speed secure communications between them. This paper describes an example of how this can be done and talks about the special issues and solutions associated with securing these types of networks.

II. Security – Do I need it?

If you are feeling very lucky maybe you think you don't need to worry about network security. Most of us don't feel that lucky.

It can be very expensive for a company to not protect its intellectual property and network. It has been reported that the CodeRed attack alone cost around 2.0 billion to clean up.

It is up to each individual company to determine what is at risk and what the cost would be if its systems were compromised. A breach in security can cause a loss of data and critical IT services. If somebody were to gain unauthorized access to your systems critical company information could be lost. Examples of the information companies need to protect are:

- Strategic Plans – A company would have a significant advantage if they had access to a competitor's plans.
- Business Operations – Information such as client list and cost and pricing data could hurt if it got in the wrong hands.
- Design Data – If your competition had access to this information it could significantly help them.
- Personnel Data – Information about employees can be very useful when a competitor is trying to hire people with some critical skills

III. What are the threats?

Threats to the security of your systems can come from internal as well as external sources. Threats from internal sources should be taken very seriously because they can be more devastating than those from the outside. Internal sources

usually have more knowledge about your systems and networks so they know the best way to attack them.

The typical threats to be dealt with are denial of service, destroying of critical data and the transfer of valuable confidential data outside the company.

IV. Considerations when developing a solution

The work environment is much more complex now than it was even a few years ago. There are many more distributed systems scattered across the world, which increases the vulnerability of all systems. There are also a lot more sophisticated and well-organized threats. This makes it much more difficult to protect networks and systems.

Some factors to consider in developing a security solution:

- What you are trying to secure – Some areas of your company may require less security protection than other areas. Knowing what you really need to secure and to what level is very important.
- Cost is always an important factor and we all have to live within the budget. Use of things like leased lines can be very good from a security point of view but are very costly.
- Scalability is a major consideration. If the company grows how easy will it be to accommodate this growth and still maintain the same level of security?
- Ease of Managing the Security Systems is another factor. It must be feasible to effectively manage all the security products in the network from a single location.

V. Example solution

A. Overview

A company's security systems can never be 100% effective against all possible attacks. Most security systems use a layered approach. Any single security mechanism in one layer will have certain flaws or holes that can be blocked in another layer. This approach with multiple layers will provide the best security protection. Each additional layer exponentially increases the security of the system.

The example solution uses many layers to ensure the security of the system. The block diagram in Figure 1 shows an example of an enterprise level architecture that could be used to provide a very secure network.

A commercial WAN network, like WorldCom's, could be used to provide the connectivity to all the company's sites. The WAN boundary is used to connect each site into the commercial WAN. Virtual Private Network (VPN) devices are used to ensure secure communications over the commercial WAN network. Note that the design assumes that all the company's sites are trusted sites. If they were not, it would be necessary to use a firewall and IDS to secure traffic coming from sites that can't be trusted.

The Internet Boundary is used to connect a site into the Internet. Most of the company's sites would not have an Internet Boundary. The number and location of the sites with this capability would be determined by the bandwidth requirements of the network. It most cases the number of sites with this capability can be limited to 2 - 4 sites. Sites that don't have a direct connection would access the Internet through a site that does have an Internet Boundary.

Each site would have its own site LAN. All the desktops systems at a site would be connected to the site LAN. The larger sites would have their own server farm, connected to the LAN, to support the desktops with functions like email. The small sites with out a server farm would use the commercial WAN to access the server farm at another site.

Two sites would be used to host the Security Management Center. This center would have Console systems that would be used to monitor and control all the security devices in the network. It would also have the capability of correlating events it gets from the various security devices. This would help the operators identify and classify security attacks.

The main features of this solution are as follows:

- Use a less costly commercial network and not leased lines or a private network to connect remote site.
- Centralizes the management of the security systems and also provides redundancy for reliability purposes.
- Limits the Internet connection points into the companies Intranet to just a few locations which lowers the cost, makes it easier to manage and improves security.

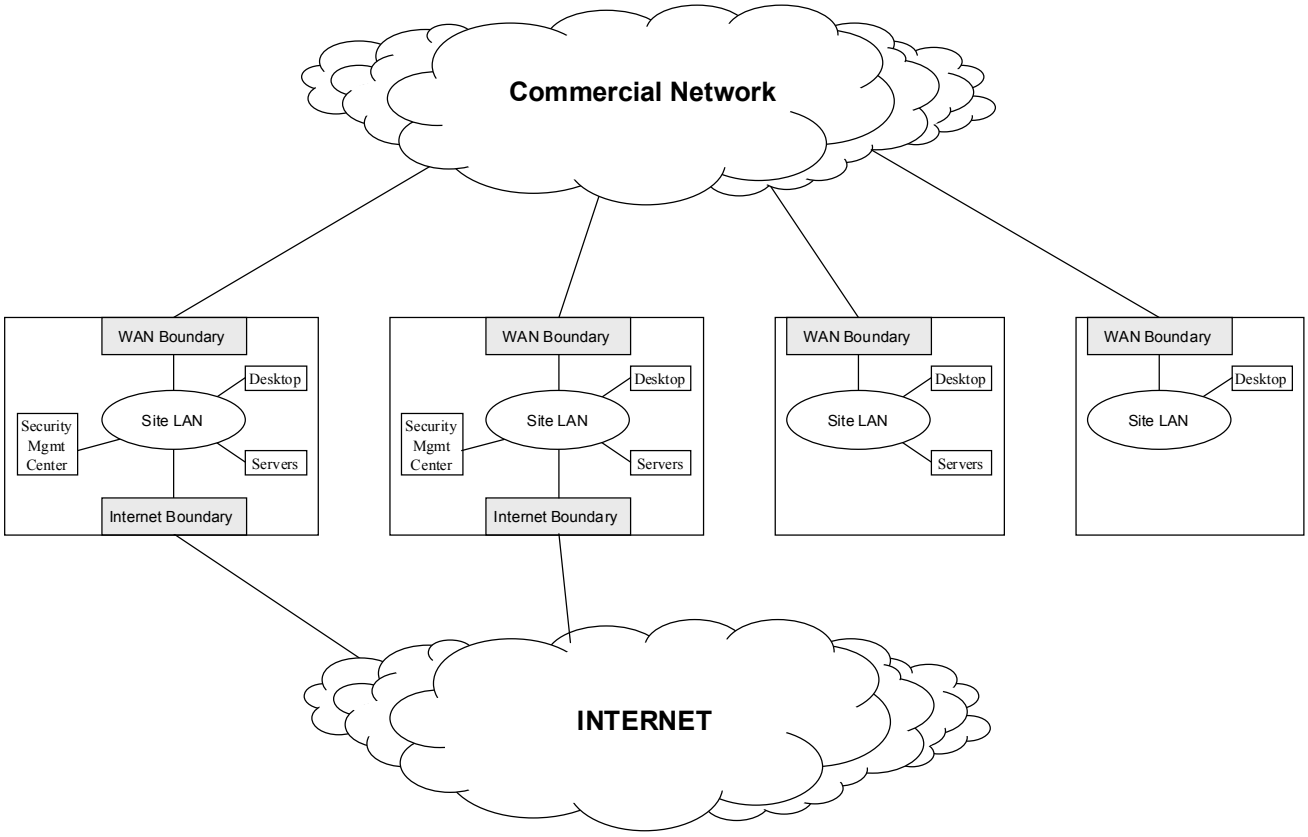

Figure 1

B. Major Components

Figure 2 shows a block diagram of a site. This site has desktops, a server farm, a WAN Boundary and a Security Management Center (SMC). The minimum configuration for a site would be desktops and a WAN Boundary.

Note that a multiple layered security approach is achieved by having more than one security device in the WAN Boundary, Internet Boundary, LAN Infrastructure, Servers and the Desktops.

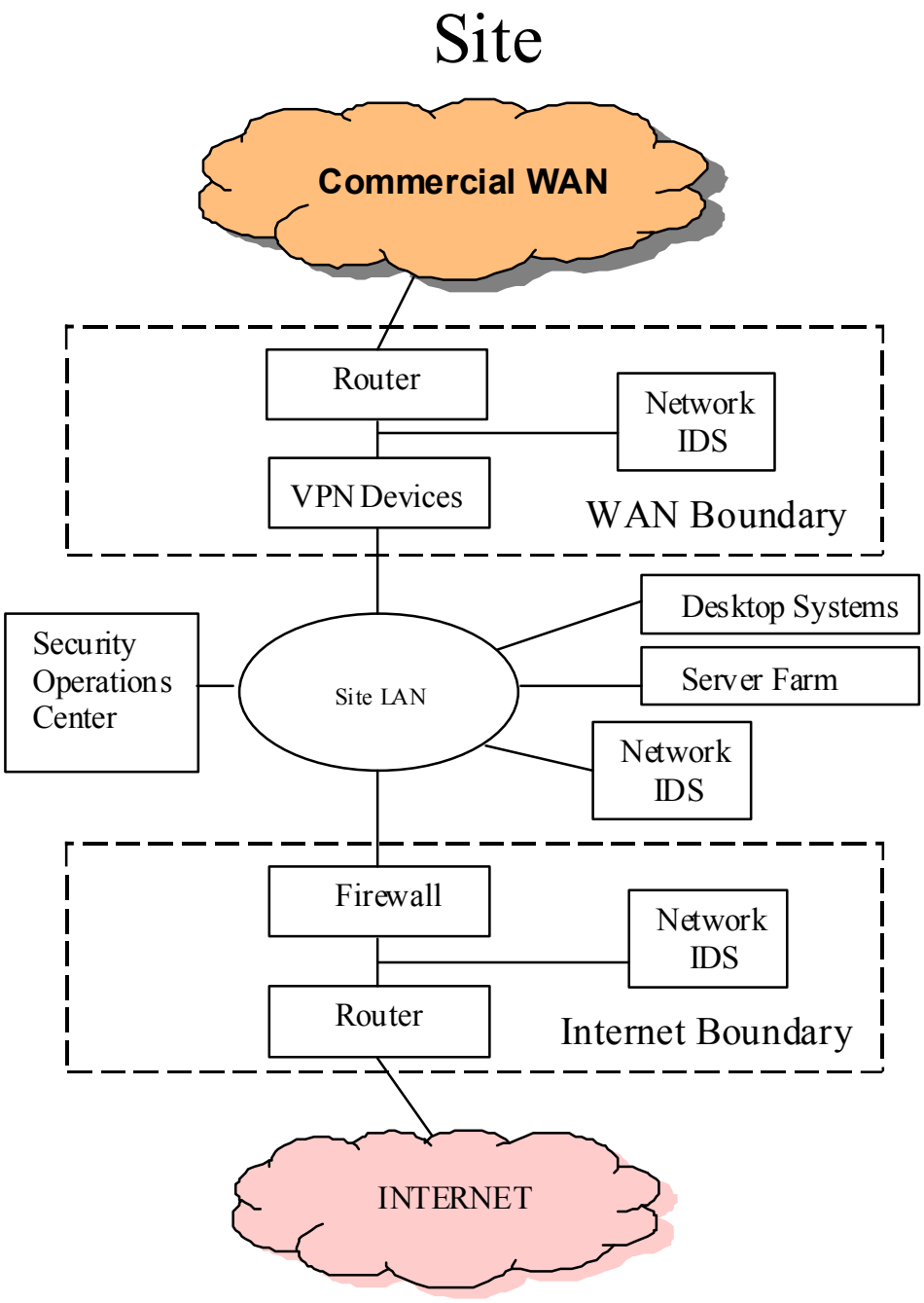

Figure 2

1. WAN Boundary

Router – This connects the site to the commercial WAN. The main security feature that is used in the router is its ability to filter data using an Access Control List (ACL). This can be used to filter on destination address, source port, destination port and specific protocols in use (UDP, ICMP, or TCP). Stateful filtering routers are available today that can use their knowledge of higher level protocols to help separate legitimate traffic from attacks on the network. When it does find an attack on the network it can block it. The filtering in the router can help prevent some attacks from getting through but it can't prevent all attacks. This is why a layered approach is necessary.

Intrusion Detection System (IDS) – The IDS sensor will provide real time traffic analysis of all the data passing between the router and the VPN devices. In real time it uses attack signatures to identify attacks. When it does identify an attack it sends an alert to the security management center and logs the possible intrusion or other malicious activity that it detected. The attacks can originate from other company sites or other users on the commercial WAN.

Virtual Private Network (VPN)- This device passes data between the router and the site LAN. The VPN device is used to set up a secure tunnel to another company site. It encrypts and decrypts the data to provide confidentiality and data integrity across the commercial WAN. If a very secure link is required units can be used that provide triple-DES encryption.

2. Internet Boundary

Router – This device provides the connection from the site to the Internet. Like the router in the WAN Boundary it uses an ACL and its knowledge of higher level protocols to provide filtering to and from the Internet. It is important to filter data sent to the Internet so as not to pass on viruses that might already be present in the companies Intranet.

Intrusion Detection System (IDS) – The IDS sensor will provide real time traffic analysis of all the data passing between the router, which is connected to the Internet, and the firewall. In real time it uses attack signatures to identify attacks. Like the other IDS devices, when it detects an attack it sends an alert and logs the possible intrusions or other malicious activity.

Firewall (application proxy) – All data from the router would pass through the Firewall. An application proxy firewall examines and authorizes all packets that try to pass through it. If the packets are not authorized they are dropped. This type of firewall translates all internal IP addresses to an IP address than can be seen externally. The firewall typically has one external IP address that is visible to the network it is connected to, which in this case is the Internet. In this way the Firewall hides all the internal IP addresses from the Internet so a user on the Internet can't find out valuable network topology information through the firewall. Another advantage of a proxy is that it conserves Internet address space, which is getting very scarce.

Most firewalls have the capability to scan and filter incoming and outgoing e-mail, FTP file downloads and Java applets for malicious programs or content. It is much better to stop a virus at the firewall than to count on the desktop virus detection software to catch it. A layered approach like this is highly recommended because it's possible to catch a malicious program at both the firewall and the desktop. It also would improve the likelihood of preventing a virus from getting into your systems if you used a different vendors product at the firewall than you do at the hosts (servers and desktops).

For analysis purposes the firewall also provides logging of all data it handles.

3. Local LAN

IDS – It is important to install IDS devices on the site LAN in order to detect unauthorized use, misuse and abuse of computer systems on the site LAN by internal and external hackers. The WAN Boundary and the Internet boundary will provide some protection from the Internet and other company sites but will not provide any protection from an internal hacker on the site LAN from attacking a system on the same site LAN.

Since most site LANs use switching network infrastructure it is necessary to put IDS devices at several points in the network in order to completely monitor all the internal traffic on the network.

4. Desktop Systems and Servers (host security)

Security protection on the desktop and server systems is the last layer in the layered security approach. It is recommended that these systems have the following:

Malicious Code Scanning - This is a basic requirement for these systems and most commercial anti-virus software does a very good job at detecting malicious code. All email and file transfers are scanned for malicious code. A mistake that is often made, which limits the anti-virus software capabilities, is to not update the virus signatures in a timely manner.

Host based intrusion detection - This software will monitor the integrity of your system files and it will look for patterns of misuse or abuse which can give you a warning before information is stolen or destroyed. It does this by looking at audit logs and by other sources of information on the host. It reports what it finds back to the security management center.

Managing and controlling security policies – A lot of software is available that monitors and controls the security policies on the host system on your network. Its findings are reported back to the security management center on a regular basis where it is analyzed and if necessary actions are taken. Software like this can ensure that users of the system are using passwords that are difficult to crack.

5. Security Management Center (SMC)

The security management center is used to provide central monitoring and control of the security of the entire company's Intranet. It has consoles that are used to control and monitor all the security sensors. It has the tools to analyze and correlate events from sensors over the entire Intranet.

These centers are staffed 24 X 7 and it is highly recommended that large Intranets have 2 security management centers for redundancy purposes.

This center would also be responsible for doing routine vulnerability assessments.

VI. Conclusion

Practical and economically feasible solutions are available that provide the level of security that is needed for today's enterprise networks. Using a layered security is key to providing a very secure environment for your company. No one

solution is the correct answer for everybody so each solution has to be tailored to meet each corporations needs. The good news is there are lots of commercial products available, when used together in the right architecture, can provide the desired solution.

VII. References

Stenger, Richard. "Cost of Code Red Rising." CNN. Aug 8,2001. URL:
http://www.cnn.com/2001/TECH/internet/08/08/code.red.II/

Tella, Matti. "Security on Backbone and Wide Area Network." Dec 1,2001.URL:
http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/backbone_wan.html

Galik, Dan Capt. USN. "Defense in Depth: Security for Network-Centric Warfare." April 1998. URL:
http://www.chips.navy.mil/archives/98_apr/Galik.htm

Galik, Dan Captain; Crotty, David; Steinbaum, Doug. "How Intrusion Detection Systems Fit Into the Strategy." Navy Intrusion Detection Strategy. April 1999. URL:
http://www.chips.navy.mil/archives/99_apr/defense.htm

McKenney, Brian. "Defense in Depth." Feb 2001. URL:
http://www.mitre.org/pubs/edge/february_01/mckenney.htm

Foote, Mary. "Improving Defense in Depth for NASA's Mission Network." Information Security Reading Room. July 11,2001. URL:
http://www.sans.org/infosecFAQ/start/NASA.htm

McIntyre, William A. "Defense in Depth – A Critical Case Study of a Large Enterprise." Information Security Reading Room. May 31,2001. URL:
http://www.sans.org/infosecFAQ/casestudies/large_enterprise.htm

VanMeter, Charlene. "Defense in Depth: A Primer." Information Security Reading Room. Feb 19,2001 URL:
http://www.sans.org/infosecFAQ/start/primer.htm

"Securing the Perimeter, Part 1." Symantec. May 16,2001. URL:
http://enterprisesecurity.symantec.com/article.cfm?articleid=743&PID=9530395&EID=0

"Securing the Perimeter, Part 2." Symantec. Jun 26,2001. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=783&PID=9530395&EID=0

Wells, Mark and Thrower, Woody "Defend Your Enterprise with Layered Security" Symantec. Jun 14,2001. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=767&PID=9530395&EID=0

Wells, Mark; Thrower, Woody. "The Importance of Layered Security." Symantec. June 14,2001. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=769&PID=9530395&EID=0

Broderick, Stuart. "Information Protection – Why Bother?" Symantec. Sept 5,2001. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=855&PID=9530395&EID=0

Broderick, Stuart. "Information Protection – Why Bother? – Part2." Symantec. Sept 5,2001. URL: http://enterprisesecurity.symantec.com/article.cfm?articleid=880&PID=9530395&EID=0

"Symantec NetProwler 3.5" Symantec. Dec 05,2001. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50

Last Updated: July 24th, 2017

Upcoming Training

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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event