Global Information Assurance Certification Paper

BENEFITS OF IMPLEMENTING SECURE COMPUTING'S SIDEWINDER FIREWALL APPLIANCE AT A U.S. ARMY MILITARY INSTALLATION

Andrew Rafla
GSEC Practical Assignment version 1.4b: *Case Study in Information Security*

TABLE OF CONTENTS:

ABSTRACT

When I began as a Network Security Administrator at a nearby military installation, the network backbone was in the process of a gigabit migration. Major changes in both the network and corresponding security architectures required the site to pass a DITSCAP accreditation upon completion of the migration. DITSCAP is the certification and accreditation process that all United States Department of Defense (DoD) installations must complete every three years or earlier if major changes occur to the information system. It is the method which helps users, and security officers ensure that DoD information systems operate at an acceptable level of risk. The process is designed to certify that the IT system meets the accreditation requirements, maintains the accredited security posture throughout the system life cycle, and subsequently ensures the protection of the Defense Information Infrastructure.

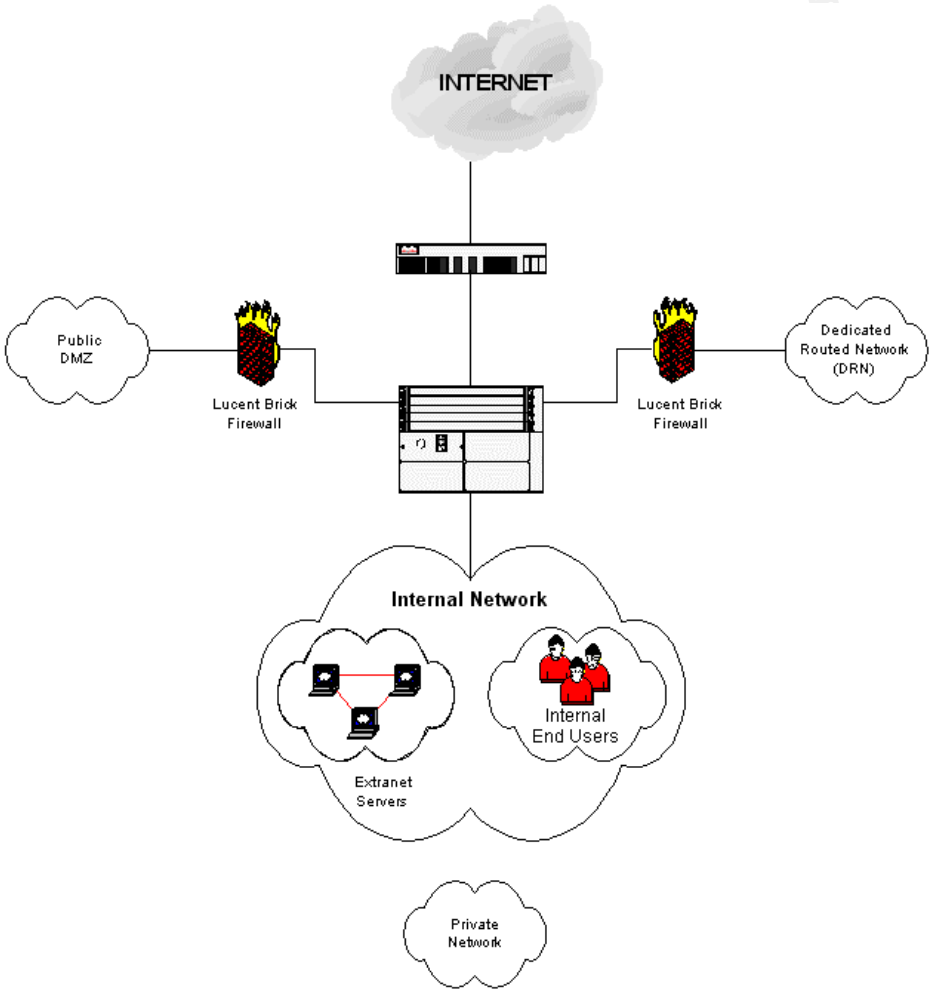
My primary job function was to assist in the development and enhancement of the Sensitive but Unclassified (SBU) network backbone's network security posture. The concept of security operations was to be developed in order to maximize the performance and effectiveness of six major security activities: network mapping/configuration management, boundary protection, vulnerability analysis/risk assessment, intrusion detection, historical correlation, and incident response. These security activities are coupled together within network operations to comprise enterprise security management for the installation's network backbone. Although each of these six activities needed improvement in some way, this paper will discuss my specific role involving the fortification of the installation's *boundary protection* through the use of Secure Computing Corporation's Sidewinder firewall appliance.

CURRENT ENVIRONMENT

Understanding the security posture that was currently in place at the military installation was critical in evaluating its weaknesses and developing an effective plan to mitigate the site's vulnerability to attacks. An initial assessment proved that the site's perimeter protection defense mechanisms had several inadequacies.

As depicted in the figure below, the network was initially segmented into four security zones. The original Private network was configured with an unroutable IP subnet and had no external connectivity. This network functioned as the security management and testing network. A publicly accessible Demilitarized Zone (DMZ) housed all public WWW, DNS, and FTP servers. In addition, a Dedicated Routed Network (DRN) housed tenant networks that depended on the installation's network backbone for Internet connectivity and also required access to specific resources on the Internal network. These tenant networks often support critical military operations at remote sites across the world and depend on accessibility to information located on servers within the Internal network.

Two Lucent Brick Firewalls protected each of these zones, providing application level protection, packet filtering capabilities, and stateful inspection technology. The DMZ and DRN were physically detached from the Internal network in order to ensure that it would not be affected in the case of an attack to either of these zones. In addition, access control from each of these networks to the Internal network was strictly configured in order to provide "least privilege" access. That is, all traffic from these zones to the Internal network was blocked at the Lucent Brick Firewalls unless explicitly allowed for business specific purposes.



The inherent vulnerability in the original architecture lied in the lack of definition and separation between Extranet and Intranet security zones. The Internal network originally housed servers that not only provided access to Internal users, but also to business-specific users on various untrusted networks, such as the DRN and in some cases, the Internet. Virtual LAN (VLAN) technology was initially configured and spanned across the Internal network in order to provide logical separation of resources, services, and business units. The VLAN is a switched network that is logically segmented by functions, business areas, or applications without regard to the physical location of network users. VLANs allowed for physical ports on the same or different switches to be grouped so that

traffic was confined to members of only that group or VLAN. This allowed for better control of traffic as specific ports were configured to allow passage to their respective VLANs. Segmenting the network into distinct broadcast groups, used to control access to specific resources, also provided an additional, but limited, layer of security in the original architecture. One area of concern, VLAN hopping, involves a variety of mechanisms by which packets sent from one VLAN can be intercepted or redirected to another VLAN, threatening network security. Under certain circumstances, attackers can exploit these mechanisms and achieve the capability of sniffing data at the switch level in order to extract passwords and other sensitive information at will (@stake, p1). Relying on this technology to segregate Extranet and Intranet services posed a serious security threat to the sensitive information contained on end users' PCs in the original hybrid Internal network. In addition, the fact that Extranet and Intranet services shared one *physical* network segment meant that the entire Internal network would easily be affected in the case of an attack to a server that currently resided in this zone. This would compromise the accessibility of services and overall performance of the Internal network, affecting all end users. The most effective security approach to mitigate these risks would be to physically divide the Internal network into an Extranet and an Intranet with specific access control mechanisms configured uniquely on each zone.

The original architecture also lacked robust security mechanisms to protect the Internal network which created an additional problem; Cisco routers at the border and interconnecting the various segments of the network were relied on as the primary defense mechanisms. The packet-filtering capabilities of the routers were utilized as extended access control lists (ACLs) were configured and applied to each interface of every router. This was an administrative nightmare because of the numerous ACLs that needed to be uniquely configured and maintained. In addition, long access control lists caused the routers to consume extra CPU cycles and, in turn, often put extra performance-hindering load on them. Most importantly, the packet filtering technology that was relied on as the primary perimeter protection mechanism was limited in its ability to defend the Internal network against the widespread variety of attacks commonly used by hackers. Although the routers were configured to serve as strict access control points, they operate at the Network Layer (OSI Layer 3) and are vulnerable to spoofing, denial of service and other attacks that take place at the Application Layer of the OSI network stack. Implementing a robust firewall solution to filter all incoming and outgoing traffic would protect the Internal network against more sophisticated attacks through essential security mechanisms such as Stateful Packet Inspection and Application Proxies.

Finally, the lack of a firewall appliance limited the sites ability to log incoming and outgoing traffic to the Internal Network. Intrusion Detection Systems (IDS) were originally placed on every segment of the network but their main functionality was to detect common attacks through specific signatures. They were not capable of logging all incoming and outgoing traffic in order to efficiently evaluate access to

specific network resources. For any systems hosting critical applications, Internal firewalls should be used to provide strong access control and support for auditing and logging (Internet Security Policy, 6.6). Furthermore, The Department of the Army Firewall Policy states "the firewall shall produce an audit trail or event log of all violations it identifies [and] report security incidents" (DOIM). In addition to lack of firewall monitoring and logging, the upgrade to a Gigabit backbone limited the effectiveness of Internal IDS systems' ability to keep up with the new throughput demands. Although new IDS systems that could handle the upgraded throughput were being evaluated, implementing a robust firewall system was the first priority in securing the Internal networks. The system would need to support granular logging capabilities in order for security personnel to effectively analyze traffic to/from the Extranet, Intranet and Private networks

SOLUTION: SIDEWINDER FIREWALL

A firewall is a combination of software and hardware that would control the traffic between the Army's Internal networks and all external networks, such as the Internet, DRN, and DMZ. The current inadequacies in the system's architecture and defense mechanisms, as well as the migration to a gigabit Ethernet network backbone, brought the need to implement a robust firewall solution. The key roles that the system would need to support include:

- To provide physical separation of Intranet, Extranet, and Private security zones
- To provide robust access control mechanisms to protect these underlying Internal networks
- To provide granular network traffic logging and alerting capabilities
- To provide extensive security capabilities while supporting the upgraded gigabit throughput of the network's backbone

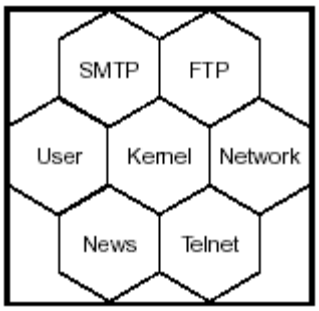
It would essentially provide an additional layer of protection by acting as a perimeter to the Internal networks, with sophisticated access control points that all data must pass through in order to enter or exit any of the underlying network zones.

Secure Computing Corporation's Sidewinder firewall appliance offers a gigabit-capable hybrid firewall solution encompassing the entire range of firewall security mechanisms including packet filtering, stateful inspection, circuit and application level proxies, secured servers, and real-time Strikeback alerts. The following section will provide a brief overview of the robust functionality of Sidewinder 5.2.1.x. and how its extensive features would fulfill the requirements of the new firewall system, thus making it the package of choice.

Type Enforcement and SecureOS

In order to understand the mechanisms by which the Sidewinder firewall would be able to fulfill the site's requirements, it is imperative to investigate the

underlying architecture of the device. Sidewinder's proven track record stems from the fact that it has never been compromised. Many attacks employed by hackers focus on breaking the firewall first by exploiting weaknesses in the operating system. Sidewinder's strong security architecture starts with SecureOS - a customized version of BSD/OS that Secure Computing Corporation has enhanced with its patented security technology called Type Enforcement. This mechanism enables SecureOS to provide a strong separation of the operating system from applications, and the applications from each other.



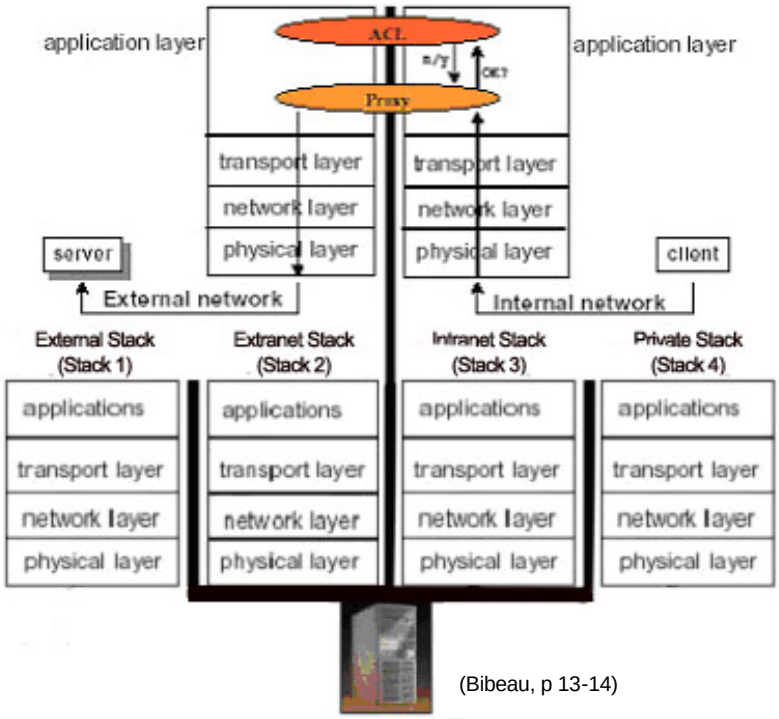
Domain structure "cell" separation on Sidewinder

Secure Computing states that the Type Enforcement security mechanism "resembles a honeycomb where critical system components are placed in separate cells" (Type Enforcement Technology, p 3). That is, each process is confined to a "cell" where it can only access the specific system resources that it needs to do its job. This is accomplished by assigning separate domains, types, and corresponding processes to each firewall element including application proxy subsystems (i.e., WWW, SQL, SMTP, etc.), users and their roles, and each of the separate networks protected by the system (referred to as "burbs").

Physical Separation of Security Zones

One of the primary goals of the firewall implementation was to physically divide the current Internal network into two separate networks, an Intranet and Extranet, with appropriate access control measures placed on each. Type Enforcement technology gives Sidewinder the advantage of maintaining completely separate network stacks for each network interface and its underlying burb. This configuration provides strong separation of data from each of the networks the firewall will connect. Network services are separated so that only pre-defined proxies and filters are permitted to bridge different networks.

By virtue of separate network stacks, Sidewinder ensures all traffic is contained within its own domain until it is forced to the application layer for verification. No traffic is allowed between the various networks unless explicitly authorized up at the application layer. This ensures that only traffic with the appropriate proxy and corresponding entry in Sidewinder's Access Control List (ACL) is passed between burbs. Below is a graphical representation of how this technology is used to provide physical separation of the External, Extranet, Intranet, and Private security zones.



(Bibeau, p 13-14)

Intranet

An Intranet can be defined as a network that employs the same types of services, applications, and protocols present in an Internet implementation, without involving external connectivity (NIST 800-41, p 25). Since Intranets utilize the same protocols and application services present on the Internet, they are vulnerable to much of the same security issues. Therefore, it was imperative that this network be implemented behind the firewall with strong access control mechanisms configured to deny ALL incoming traffic to it. The Intranet would encompass all Internal users and any workstations/servers that contain corporate or other sensitive information. Due to the sensitivity of information contained in this zone, all access from any other zone would be denied at the firewall and access to this burb would be limited to those users and hosts within the Intranet itself. In addition, all outgoing traffic such as HTTP, HTTPS, FTP, SSH, TELNET, etc. would be passed through the firewall's corresponding proxy service. This would enable the source address of all outgoing packets to be hidden, as the IP address of the outside interface of the firewall would appear as the source of the traffic.

Extranet

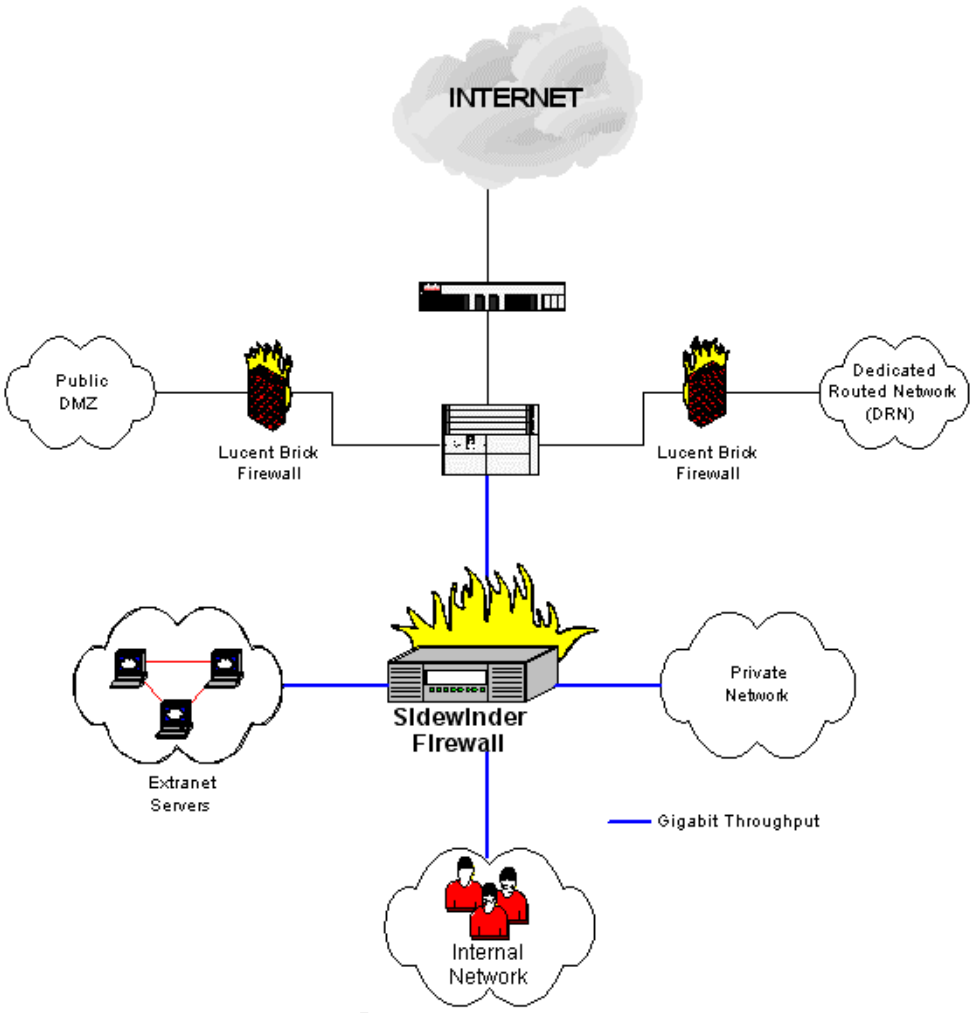
"By definition, the purpose of an Extranet is to provide access to potentially sensitive information to specific remote users or organizations, but at the same time denying access to general external users and systems" (NIST 800-41, p 36). Therefore, an Extranet can be considered an Intranet with limited external access for specific business-to-business needs. The installation's Extranet would be configured so that it is fully accessible from Intranet and Private networks while allowing limited, controlled access from all other untrusted security zones (such

as the DRN and Internet). Furthermore, customers that would require access to specific services in the Extranet must pass and provide proper documentation of their DITSCAP accreditation and must authenticate each communication session through some sort of identification mechanism (i.e. VPN, Radius, NT authentication, etc). This is to ensure that proper security posture is applied on both ends of the communication and that access is limited to only those that need a specific service for business critical purposes. The capability of the Extranet to support any type of external connectivity portrays the need to ensure proper distinction between Extranet and Intranet hosts and services and, accordingly, create a unique access policy for each zone.

Private

The Private security burb consists of a Class A 10.x.x.x network that, similarly to the Intranet, would be completely inaccessible from any other network. This network consists of all security management and testing stations and is also the only security zone that is allowed to connect to the Sidewinder firewall for secure management and remote administration through the COBRA management console. Prior to the implementation of the Sidewinder firewall, the hosts on this network were unable to access any resources from outside the Private network. Because of the lack of Internet connectivity, several tasks, such as updating packages, signatures, etc, became very inefficient. In order to upgrade a system, the corresponding package would need to be downloaded on a host within the Internal network and copied to CD format. From there, the administrator of the system could take the media to the Private network and install the package on the system to be updated. Sidewinder's proxy functionality enabled the Private network to have outbound access to critical services such as HTTP, FTP, SSH, TELNET, etc. while hiding the actual source address of the communication. Similarly to outbound traffic from the Intranet, the outside IP address of the firewall would appear as the source address of all communications from this network.

The new architecture resulting from the implementation of the Sidewinder firewall is noted in the graphic below:



Protection of Attached Networks and Hosts

Sidewinder's Access Control List (ACL) is a database that it uses to control all user access to the Sidewinder's proxies and servers. When an internal or external user requests a network connection, the Sidewinder checks the ACL entries to determine whether to allow the requested connection or deny it. The ACL is essentially where Sidewinder will control the site's security policy (refer to U.S. Army Training and Doctrine Command (TRADOC) Firewall Configuration for more information on US Army firewall policy- *http://www-tradoc.army.mil/tpubs/regs/r25-74/r25-74.htm*). Here, all incoming connections to the Intranet and Private security zones are blocked, business-specific traffic from authenticated external sources to the Extranet is passed, and limited access from the Extranet to the Intranet is also configured to pass. In addition, all outgoing requests from each of the underlying networks are passed through the Sidewinder's corresponding proxy service in order to hide the actual source address of the communication. The Sidewinder ACL database contains the list of rules that determine which networking services users will be allowed to use.

Criteria that is used to allow or deny each request include:

- The source or destination burb - connections can be allowed or denied based upon the source burb, the destination burb, or both.
- The source or destination network object - objects such as IP address, host name, domain name, subnet, or a network group can determine connection requests.
- Types of connection agent - agents include both proxies (connections through the Sidewinder to another system) and servers (service can be provided on the Sidewinder itself).
- Type of service requested

Optional criteria include:

- User requesting the connection - connections can be allowed based upon a group for which the user requesting the connection is a member.
- Authentication - the Sidewinder can be required to authenticate the user prior to granting the connection request.
- Time and day - the ACL entry can be configured to allow or deny a connection based on the time, the day, or both.
- Redirect proxy destination - the Sidewinder can be directed to redirect the inbound connection request to a different destination address or port.
- Special options - connection requests can also be dependent upon special parameters that apply to certain services such as FTP, HTTP or TELNET proxy (ICSA, p7).

ACL processing cannot be bypassed or circumvented and all incoming and outgoing traffic must pass through the firewall and, correspondingly, the ACL rules. In addition to enforcing the firewall policy through the ACL, Sidewinder will monitor all attempts to violate access control rules and will trigger appropriate alarms through Secure Computing's real-time Strikeback alarm mechanism.

Event Monitoring

Two key features of Sidewinder, Event Monitoring and Strikeback Alarms, made this package a premier choice given the new Gigabit environment and our goals of protecting a segmented network. Sidewinder maintains granular logs of all traffic that passes through it to each of the underlying security zones. In addition, it maintains a record of all security-related events. Monitoring events in real time provides the advantage of being able to take immediate action, which can prevent possible damage and collect essential information about the attack just as it is happening. Sidewinder's event monitoring would provide the means to detect possible intrusions and suspicious activity, while providing vital forensic information about them. Strikeback is the part of Sidewinder that takes that information, and responds to the intrusion with swift and appropriate action (Sidewinder Administration Guide, Chapter 16).

The Sidewinder firewall was configured to monitor these specific types of events:

- Access control list threshold violations: This event occurs when the number of times a user is denied access to a service exceeds a predetermined number.

- Attack attempts: This is any type of suspicious occurrence identified by one of the services on Sidewinder; for example, the presence of a suspicious IP address on an incoming connection.
- Mail messages that are rejected by a mail filter: This event occurs when an SMTP mail message does not pass through a configured mail filter.
- Attempted network probes: This event is when a user attempts to connect to a TCP or UDP port that has no service or an unsupported service associated with it.
- Exceeded network traffic threshold: This event occurs when the number of traffic audit events written by the various proxies going through Sidewinder exceeds a specified threshold.
- Attempts to circumvent Type Enforcement: A Type Enforcement violation occurs when an unauthorized user or process attempts to perform an illegal operation on a file protected by Sidewinder.

When Sidewinder detects any of these events, it makes a response based on set policy controls. Because some events may be false positives, thresholds were set in order to specify an allowable limit for a given event over a given period of time. If that threshold is exceeded, one or more of the following responses is triggered:

1. Signal a pager
2. Send an email message
3. Issue an SNMP trap
4. Perform a Strikeback action

Strikeback
Sidewinder's Strikeback capability enables the firewall to obtain essential information about suspicious activity as the possible intrusion is taking place. Strikeback responses were configured to run one or more of the following common Unix system commands when specific event thresholds are exceeded: nslookup, dig, finger, traceroute, and ping. The Sidewinder will take each offending IP address from the audit file and use it as input for the specified command. When an alarm is triggered, Sidewinder executes the selected commands and automatically emails the results to the firewall administrator. This unique alerting mechanism would function as a type of intrusion detection response in that it will alarm the correct personnel to take immediate action when a possible security violation is taking place. Strikeback responses would effectively gather essential forensic information that can be analyzed and used to investigate suspicious activity, proactively adjust policies, and prevent future attacks.

Gigabit Support
The faster the hardware, the better the firewall performs. This is why the two Sidewinder firewalls purchased were built on powerful Dell PowerEdge 2650 servers with dual Pentium III XEON 2.20 GHz processors, 1GB of RAM, and five Gigabit-capable network interfaces. The Sidewinder firewall was the first firewall

product to be optimized at Intel's ASC labs for Pentium XEON performance and would offer a robust security mechanism capable of handling the installation's new Gigabit backbone. Test results for this device, provided by Secure Computing Corporation are as follows (Sidewinder Performance Measurements, p 3):

security filtering	Throughput	Connections/sec accepted
Packet filtering	635.2 Mb/sec	Unlimited
Network proxy	361.6 Mb/sec	2010.8

Table 1: *Test results for gigabit traffic levels*

Although these figures portray Sidewinder's capability to easily handle the backbone's network throughput, the firewall's rule set and features would be configured in order to maximize its efficiency. For example, traffic that requires high throughput and poses little or no intrusion threat was configured to pass through Sidewinder's stateful packet filtering mechanism; this type of filtering achieves the highest possible throughput speeds. In addition, this allowed the multiple ACL lists that were configured on each router to be administered from a single console and, in turn, lightened the extra CPU load that the packet filtering placed on the routers. TCP traffic that requires moderate restrictions was configured to pass through the somewhat more CPU-intensive generic proxy services. This type of traffic includes services such as SSH, DNS, TELNET, FTP, etc from the Internal and Private networks to the Extranet. Lastly, services that pose a serious or critical security threat, like certain proprietary e-business Web traffic or FTP file transfers from external users to the Extranet, was configured to pass through Sidewinder's application level proxies, thus trading off some throughput performance for the highest level of security filtering possible.

IMPACT OF SIDEWINDER IMPLEMENTATION

Implementing the Sidewinder firewall to protect the Extranet, Intranet, and Private networks was a major improvement to this military installation's overall security posture. The robust functionality of the firewall would serve to:

1. Provide *physical* separation of Extranet, Intranet, and Private security zones as opposed to the logical separation that was currently in place using VLAN technology.
2. Provide essential protection mechanisms through packet filtering, application proxy protection, and stateful inspection that all traffic must pass through in order to enter or leave each of the underlying security zones.
3. Provide essential traffic monitoring, security event response, and corresponding alarm notification through Strikeback functionality.
4. Provide a secure gateway to each of the underlying networks capable of supporting the upgraded Gigabit throughput of the installation's backbone.

Several insecurities in the installation's Sensitive but Unclassified Internal network left the site extremely vulnerable to a wide range of attacks currently employed by hackers. In order to ensure a sound security posture, new security tools that would be able to support the upgraded architecture would need to be implemented. The primary area of concern was to integrate a robust firewall solution that would support the new Gigabit backbone and provide essential defense mechanisms that were currently not in place for the Internal network. The site's forthcoming DITSCAP accreditation would require that the proper mechanisms were in place to defend the Internal network(s) and maintain the integrity of the site's information system.

The implementation of the Sidewinder firewall solution would transparently support the upgraded network demands and add essential security mechanisms such as Application Layer protection, Stateful Inspection technology, etc. These functionalities increased the site's ability to defend itself against attacks. In addition, real-time event monitoring, as well as uniquely configured Strikeback response alerts, allow IT Security personnel to proactively monitor attempted intrusions and suspicious activity.

In conclusion, the added protection mechanisms supplied by the implementation of a Sidewinder firewall appliance, along with strict "least privilege" access control policies would assist the Designated Approval Authority in accepting the new minimized level of risk and, therefore, approve the site's new DITSCAP accreditation.

REFERENCES

Sidewinder 5.2.1 Administration Guide. Secure Computing Corporation, Copyright 2002.

Pollino, David and Mike Schiffman. "Secure Use of VLANs: An @stake Security Assessment." @stake, August 2002. URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

Bibeau, Gary. "Site Survey Considerations for Firewall Installation." ParallaX Research Group, September 2003. URL: http://www.parallaxresearch.com/dataclips/pub/infosec/penetration_testing/bibeau/

United States Army Training and Doctrine Command. "U.S. Army Training and Doctrine Command (TRADOC) Firewall Configuration." Department of the Army Headquarters: Fort Monroe, Virginia. June 6, 2001. URL: http://www-tradoc.army.mil/tpubs/regs/r25-74/r25-74.htm

"Sidewinder Firewall Product Functional Summary." ICSA Labs, October 30, 2001. URL: http://www.icsalabs.com/html/communities/firewalls/certification/rxvendors/securesidewinder/pfd.pdf

"Sidewinder Performance Measurements." Secure Computing Corporation, May 2002. URL: http://www.techprodx.com/pdfs/swind_perf_mea_wp.pdf

Wack, John P. and Lisa J. Carnahan. "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls." National Institute of Standards and Technology (NIST) Special Publication 800-10, US Department of Commerce. February 9, 1995. URL: http://csrc.nist.gov/publications/nistpubs/800-10/

"Internet Firewall Policy." Internet Security Policy (section 6). WindowsSecurity.com, October 16, 2002. URL: http://secinf.net/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Internet_Firewall_Policy.html

"Type Enforcement Technology for Access Gateways and VPNs." Secure Computing Corporation, June 2000. URL: http://www.ccmconsult.de/produktinfo/scc/type_enforcement_wp.pdf

US Army DOIM. "The Department of the Arm Firewall Policy." URL: http://www.doim.army.mil/doimdoctemplate.cfm?doimdataid=5

Cutlet, Ken, Jamie Pole, and John Wack. "Guidelines on Firewalls and Firewall Policy." National Institute of Standards and Technology (NIST) Special Publication 800-41, US Department of Commerce. January 2002. URL: http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf