Global Information Assurance Certification Paper

Case Study on a Successful Implementation of Juniper/Netscreen IDP

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2 - Case Study in
Information Security

Submitted by: Stanislav Firstov
Location: Online

Paper Abstract: The purpose of this paper is to detail the enhanced security provided by the installation of Juniper Netscreen IDP products on a large scale website. The pair of Netsceen IDP's serve as protection from nefarious attacks. The IDP devices add to the layered approach to security that allows the network and associated hardware to function efficiently to achieve its goal of ensuring website accessibility while also making sure security is evident.

Table of Contents

Abstract/Summary

Before

-

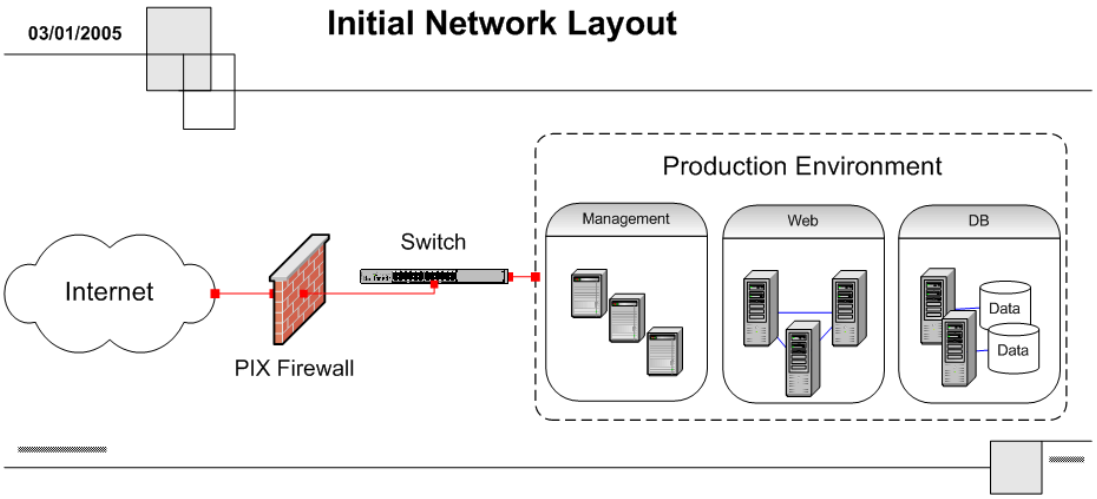
Abstract/Summary

The purpose of this paper is to detail the enhanced security provided by the installation of Juniper Netscreen IDP products on a large scale website. The pair of Netscreen IDP's serve as protection from nefarious attacks. The IDP devices add to the layered approach to security that allows the network and associated hardware to function efficiently to achieve its goal of ensuring website accessibility while also making sure security is evident. The case study details the a implementation of Network Intrusion Detection/Prevention system from Juniper – Netscreen-IDP 100 that have enhanced overall network security.

The production network is very robust and fault tolerant yet the additional protection provided by the IDP devices allows any nefarious attack to be identified and stopped before they can do damage. Additionally, the attacks are stopped before they reach the firewall limiting the possibility that a storm of attack packets could overwhelm the firewall.

Overall, the Netscreen IDP devices have proven to be very capable and effective devices in enhancing security on the network.

Before



The system being described in this paper is a large non commercial web site that is getting approximately 2 millions hits daily.

The environment is comprised of Compaq Windows 2000 Advanced Server cluster running SQL Server 2000 and load balanced web heads running Internet Information Services Version 5 (IIS5).

The current environment is segmented from the primary network by a pair of Cisco PIX firewalls. One of the firewalls was configured to be the primary firewall handling all of the network traffic requests and the other firewall was configured as the secondary firewall handling no traffic unless the primary firewall has a problem. The firewall is the only entry point into the production environment and the firewall performed both filtering and routing duties on the network. The network behind the firewall is segmented into three subnets. These networks are the cores of the production network.

Current Security Posture

The following is a listing of the current network and security systems deployed at the client site for a production system. The following systems, applications, and network elements are found within the production environment. The following devices were reviewed during this analysis;

- **Cisco PIX Primary and Secondary Firewalls:** Interface between the public and private networks.
- **Primary and Secondary Cisco Content Switches:** Switches used in the DMZ to round robin between the web servers and URL redirection.

- **Cisco Switches (192.168.100, 200, 0 subnets):** Primary switches used to connect systems within the subnets.
- **Intrusion Detection System (IDS):** SNORT based system that monitors the network for attacks based on predefined signatures.
- **VPN:** Virtual private network used to connect remote users to the environment for administration.
- **DMZ:** Zone that is used to house public network facing servers and is considered a hostile environment.
- **Database Servers:** Backend Servers used primarily to house data.
- **Authentication Servers:** Servers used to authenticate systems and users within the network.
- **Web Servers:** Public facing servers used to serve content to users.
- **Development Staging Servers:** Servers used to test software before being implemented in the production environment.
- **Search Servers:** Servers used to query the database and send data back to the web server that imitated the request.

Problem Description

Prior to the installation of the IPS system we were receiving numerous false positives alerts from SNORT based IDS and what's most important, malicious traffic did not get blocked. This was very inefficient as people's time was spent investigating these false positives. Sometimes, by the time an alert was analyzed it was too late for any appropriate action. The installation of the IDS system and proper configuration has enhanced overall network security and eliminated many of these false positives.

Since firewall inspects only headers and not the content of data packets, it's still possible to exploit protected by the firewall systems using weaknesses in protocols that are allowed through. That is why a second line of defense is necessary such as intrusion prevention system (IPS). IPS's have gained a considerable amount of interest, and they are an important component of defensive measures protecting computer systems and network from abuse. However, that does not exempt organizations from having a well defined and applied security policy before implementing an IPS, accordingly to "Defense in Depth" layered model.

Current Risks

Even though the web site is protected by the firewall; it is still exposed to attacks from the Internet. A firewall is just a one layer of the "Defense in Depth" security model. It is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. The environment is

constantly evolving and changing fueled by new technology and the Internet. To make matters worse, threats and vulnerabilities in this environment are also constantly evolving. Intrusion detection products are tools to assist in managing threats and vulnerabilities in this changing environment[1]. Mullins, Michael. “Vital intrusion detection”

In reviewing the production network, several risks were apparent with the old network architecture. The first risk identified was that there were several single points of failure in the network. A single point of failure creates a risk to the availability of the systems or networks. By having a single point of failure in the network, should an issue arise that causes the single point to fail the entire network would be inoperable. One failover switch should be placed in each subnet to mitigate the single point of failure. Another risk identified in the architecture is the lack of Intrusion Prevention System (IPS) and lack of monitoring of the complete network.

The types of servers that are normally located within a DMZ network should be the production web servers, search servers and content switches. The web site architecture contains staging and development servers. Traditionally, staging and development servers introduce risk into environments because the security posture of the servers is not maintained to the same levels of a production server. Due to the dynamic nature of the servers, where changes are constantly being made, the security of the servers suffers. Moreover, many accounts are usually needed for developers to access the server to perform their work. These accounts are frequently set-up with little to no security thought. These reasons make staging and development server perfect targets for compromise by attackers, therefore the staging and development servers should be placed on their own network segment and protected by a firewall.

Impact of SANS Training on the Situation

The impact of SANS training has been extensive. First of all it has allowed me to gain an understanding of security principles and how they should be applied to effectively secure an environment. Additionally, by being exposed to various options it has allowed me to evaluate different approaches to security and then make recommendations that can be easily implemented yet yield excellent results to enhance security. Finally, by completing this training it has provided me the foundation to continue to improve my knowledge of security principals and practices.

During

To establish a baseline and determine the appropriate course of action each system was reviewed for its configuration and design for a secure architecture.

It was also viewed from a best practices standpoint in system design. The following is a brief definition for each of the key evaluation sections that were evaluated:

1. Network Design – Overall architecture and configuration of current network.
2. Secure Access – Methods used to access and administer the systems and network devices.
3. IDP Coverage - The ability of the IDP system to monitor all inbound and outbound traffic to and from systems.
4. Environment Separation - The proper segregation of systems into distinct security zones.
5. Monitored for Critical Events - The ability to monitor the systems and trigger an event when it is taking place.
6. Architecture Documented - Having proper network documentation in place with all assets reflected.
7. Version up to date - Most current versions of software in production.
8. Secure Environment – Located in proper security zone to ensure confidentiality, integrity, and availability.
9. Availability – Ensuring that the system is accessible to those systems or users who require services from the network. This is achieved by having redundant components at critical points within the infrastructure.

As a result of this analysis the following corrective actions were recommended and implemented:

The shortcomings noted result in the following:

- The website security posture is open for potential compromise.
- Mean time to restore (MTTR) from failure is high.
- Mean time between failures (MTBF) is low.
- Operational cost is higher than needed.

At a high-level, the following changes were recommended:
Firewall Changes are required as noted here:

- Remove unnecessary Access Control Lists and Interface
- Review and restrict existing access lists
- Restrict access to management console
- Disable TELNET traffic in the environment
- Reconfigure Timeout parameters
- Enable Floodguard Protection

Architectural Changes are required to enhance system security

- Segregate network into DMZ Production, Infrastructure Management, and
- Staging/Development
- Install additional hardware to remove single points of failure
- Install IPS System to cover the entire network
- Update Network Diagrams to reflect current environment

After the implementation of these recommendations and the installation of the Netscreen IDP appliances the security posture for the website and network will be greatly enhanced.

Proposed Solution

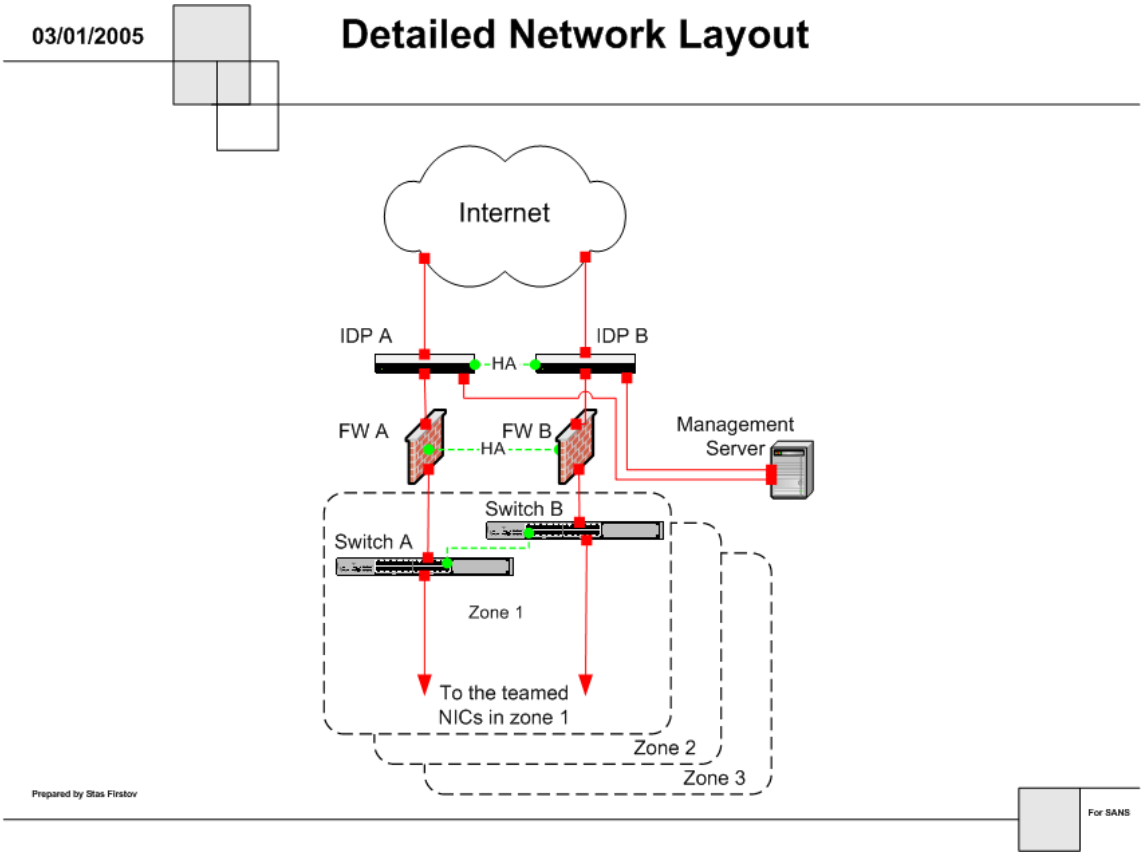
One of the primary solutions as noted above was the purchase and installation of two Netscreen-IDP100 systems in front of the Firewalls in the in-line mode. When IDP is setup in in-line Bridge Mode, all traffic will be coming trough the IDP allowing taking full advantage of IDP attack prevention capabilities and Multi-Method Detection mechanisms. By placing the IDP systems in front of the Firewall both internal and external attacks would be detected by Intrusion Prevention System.

Key features and benefits of the Juniper Networks IDP solutions include the following:

- Multi-method detection system that includes compound signatures, stateful signatures, protocol anomaly, and backdoor detection
- Extensive signature customization, to improve the ability to detect unique attacks and to tailor the signature to meet the customer's requirements
- Closed loop investigation process, to quickly see the big picture and then drill down to the appropriate level of detail to make informed security decisions
- Enterprise Security Profiler (ESP), to gain insight into network and attack activity that accelerates inline deployment and facilitates attack investigation
- Policy Editor, to create and deploy granular security policies that specify what traffic to look at, what attacks to look for in that traffic, and how to respond when an attack has been detected
- Log Viewer, to investigate specific security incidents and to customize the way which information is processed within the system
- Centralized, rule-based management approach, to simplify deployment, configuration, and maintenance
- Fully customizable reporting, to generate up-to-the-minute status on network activity
- IDP clustering, to enable stateful, standalone high availability, minimizing the risk of a single point of failure and maximizing network protection[3]. Juniper Networks. IDP-100 data sheet.

Additionally, the network environment architecture to be upgraded using the most current technology to ensure the confidentiality, integrity, and availability of the network and production website.

The web site contains extremely important information and access to the systems that support the web servers i.e. database servers, search servers, needs to be very restrictive. As outlined in the SANS security course, all connectivity to such servers should be limited to only essential network traffic. The use of Access Control List's (ACL's) and Firewall policies should be used to protect these backend systems. The ACL's and Firewall policies should be granularly written and restrict network traffic to only the users and machines that need access.



The diagram displays both IDP units setup in a Bridge Mode in High Availability Configuration. Both forwarding interfaces eth0 and eth1 for each IDP appliance are stealth interfaces, meaning they do not have an assigned IP address. They support 1000 Base-T Ethernet standard which is more than adequate for the amount of forwarded traffic. The management interface (eth3) for both IDP units has an assigned private IP address and goes to the management server.

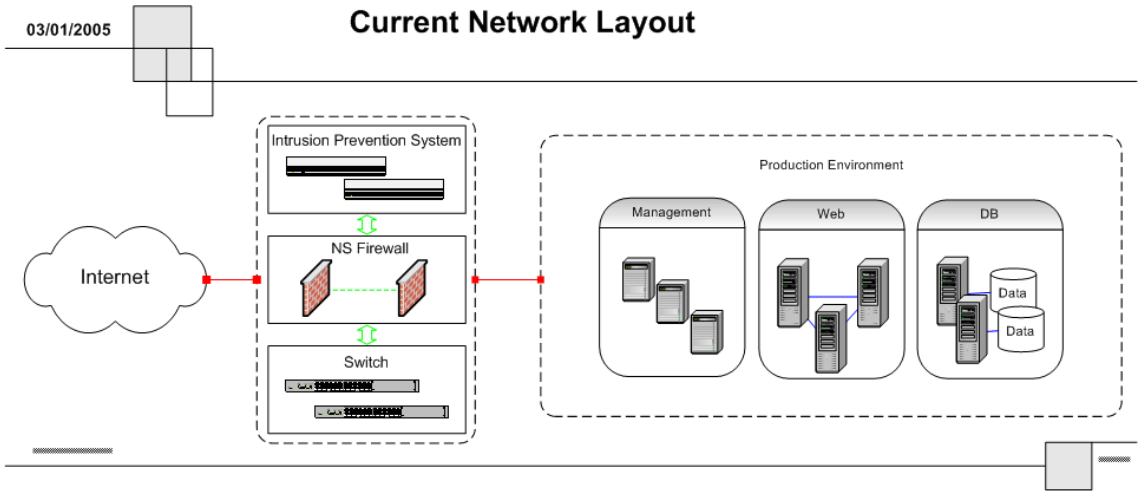
The management server box is a hardened Linux Red Had server running Netscreen Management Server and Netscreen User Interface software.

In the proposed solution it was decided not to use IDP Bypass Unit to

provide fail-open protection. The Netscreen Firewalls behind the IDP appliances will be monitoring network connectivity by pinging default gateway IP address (above the IDP). Combining this feature with monitoring of its external interfaces status the firewalls will take care of a situation when one of the IDP units fails.

Solution Implementation

As noted in the previous sections the IDP100 systems were installed in the network and configured to provide the appropriate protection. Additional recommendations as noted were also implemented to improve the overall security of the network. This will continue to be an ongoing process. As new attacks and vulnerabilities are identified the entire architecture and security devices will be examined to ensure the capability to exploit a noted weakness is minimized.



The management server is used to send out security alerts from IDP units to notify on-call personnel via e-mails. The server is also setup as a log server via syslogd daemon for both IDPs. A rulebase was installed on each IDP sensor via the management software allowing selecting exact conditions and attacks for dropping all malicious attempts. According to Juniper, the IDP vulnerability database should be updated on weekly basis ensuring the network environment is effectively protected.

Monitoring of the web site and production environment is setup via Big Brother software from http://www.bb4.org/ . The monitoring server resides at the level above the IDP and effectively monitors entire environment.

After

The IDP system uses multiple detection methods to identify and prevent attacks. By combining these detection methods and using them simultaneously, IDP accurately and efficiently detects threats to the protected network infrastructure. The IDP Multi-Method Detection (MMD) mechanism integrates the following detection mechanisms:

- Stateful Signatures
- Protocol Anomalies
- Backdoor Detection
- Traffic Anomalies
- IP Spoofing
- Layer 2
- Denial of Service Detection
- Network Honeypot

The installed IDP systems provided three primary weapons in the war against intrusions:

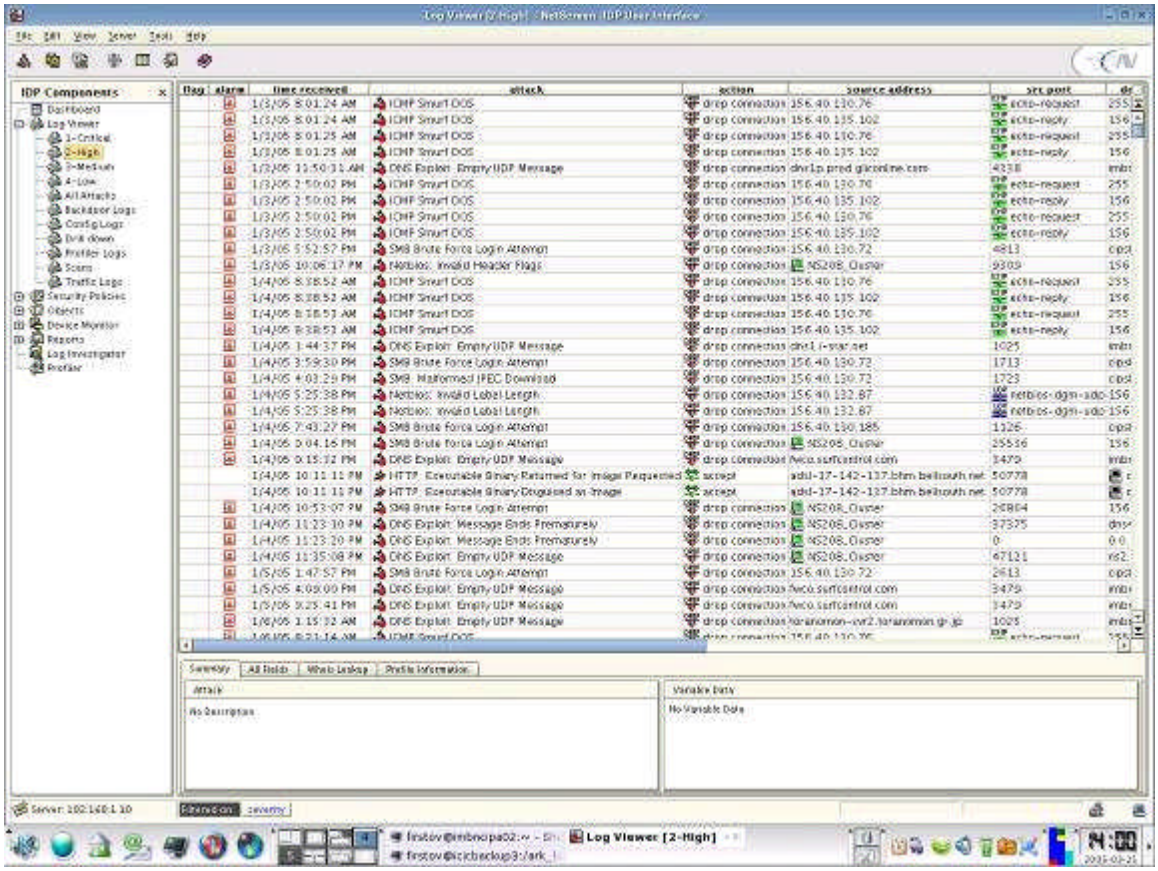
- True attack prevention. IDP can drop malicious packets and/or connections, eliminating the impact of attacks by preventing them from reaching their targets.
- Accurate attack detection. IDP detects attacks using its proprietary MMD mechanism (as noted above).
- Easy of management. IDP provides centralized, rule-based approach, reducing management overhead with integrated incident management[6]. Netscreen, p.89.

For the production network and website to be positioned to handle the increased demand that will be applied to it and for the client to feel confident that it will be free of compromises and various internet attacks, the following high-level recommendations were made and implemented:

1. A thorough review of firewall policies
2. Update network documentation
3. Expand IDS/IDP Coverage as noted in this document
4. Segregate network
5. Install redundant devices

The core security recommendations were essential for the network and website site to operate with little or no disruption to service.

Bellow is the IDP Management server graphical user interface that allows reviewing all attacks and protocol anomalies for analysis.



Solution Testing and Validation

Once the IDP OS was updated to the latest version along with Management Server software, and Security Policy for bridge mode was setup with all customization, it was ready for a test.

To test the solution I have used Nessus Vulnerability Scanner (http://www.nessus.org/) and Security Auditor's Research Assistant (SARA) from http://www-arc.com/sara/ tools freely available for download.

These tools were installed on a Compaq DL-360 box running Fedora Core version 3 Linux. The test box was setup at the above IDP level to perform these security tests. Netscreen IDP devices have successfully blocked all malicious traffic from the network scanners while generating e-mail alerts.

Below is a sample alert generated by the IDP system.

```
From: NetscreenIDP
To: IDP_alarm
Subject: HIGH alarm HTTP:IIS:COMMAND-EXEC-5 detected by IDP
Date: Thu, 10 Mar 2005 07:51:01 -0500
------------------------------------------------------------
Log: 20050309/27097
generated (GMT) : 2005/03/09 23:23:33
received (GMT)  : 2005/03/09 23:35:49
source          : xxx.xxx.xxx.xxx:1742
destination     : xxx.xxx.xxx.xxx:80
protocol        : TCP
attack          : HTTP:IIS:COMMAND-EXEC-5
category        : ATTACK:IDP_ATTACK_MATCH
action          : DROP
------------------------------------------------------------
Attack: HTTP:IIS cmd.exe Command Execution 5
This signature detects attempts to exploit Microsoft Windows Web
servers. Attackers may send a maliciously crafted url containing the
string "cmd.exe" to execute commands on the Web server.
CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-
0886
BugTraq: http://online.securityfocus.com/bid/1912
```

To test the Failover feature of the new environment, we disconnected the power plugs for one of the IDP units while monitoring the network connectivity status. In addition we tried disconnecting a network cable from IDP's forwarding interfaces. Capitalizing network and interface status monitoring at the Firewall level, the connectivity was not disrupted trough the Failover.

Risk Assessment

Since the website is publicly accessible and there are always malicious hackers attempting to gain access the risk remains relatively high that someone may attempt to gain unauthorized access and either deface the website or introduce some type of malicious program in to the network. We must remain vigilant in our efforts to combat such an attack.

The goal of this document was to evaluate various hardware, software and network communications vulnerabilities. As noted above, the identified potential threats for the web site infrastructure were mitigated via installation of the IDP-100 Intrusion Prevention System and implementing of the Failover solution.

There were other potential threats identified during the Risk Assessment procedure, such as web site application vulnerabilities (CGI scripts, etc), problems with physical security and absence of the Incident Response Plan. These problems are not covered in this paper however many were remediate as part of an overall assessment of the security posture of the environment.

Conclusion

The implementation of the IDP devices and a thorough review of client's security policies and implementations have greatly raised the level of security in the environment. I realize that security is an ongoing battle and will continue to conduct scans and assessments as well as review log files and reports to ensure that the environment remains secure. The addition of the Netscreen IDP devices has been one of the major improvements to security on the network and would be highly recommended to anyone looking for a fast and easy way to implement in-line intrusion detection and prevention in their network.

Juniper Networks Intrusion Detection system has proven to be a fairly comprehensive and reliable device to aid in the deterrence of network and application level attacks against the production environment. By capitalizing on the capabilities of these devices and also improving security at the firewalls, routers and switches the overall level of security in the current environment has been improved significantly.

Security will continue to be an ongoing battle and hopefully by successfully completing this training it will raise my level of awareness and expertise in this field.

References

1. Mullins, Michael. “Vital intrusion detection”. TechRepublic. 15 May 2002. <http://insight.zdnet.co.uk/communications/networks/0,39020427,2110249,00.htm>
2. InfoWorld. “Juniper NetScreen-IDP 100”. InfoWorld. 23 May 2003. <http://www.infoworld.com/Juniper_NetScreen-IDP_100/product_46377.html?view=1&curNodeId=0>
3. Juniper Networks. “NetScreen-IDP 10/100/500/1000”. December 2004 <http://www.juniper.net/products/intrusion/dsheet/110010.pdf>
4. Yakabovicz, Edward. “Recommendations for deploying an intrusion-detection system”. TechTarget Network. 01 Nov. 2001. <http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci779268,00.html>
5. SANS Institute. “Intrusion Detection FAQ”. 12 June 2003. <http://www.sans.org/resources/idfaq/id_required.php>
6. Jumiper Networks. “Concepts & Examples Guide NetScreen-IDP Fundamentals” Netscreen documentation ver. 2.1 2003.
7. Microsoft Corporation. “The Security Risk Management Guide”. Microsoft TechNet. 15 Oct. 2004. <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/srappd.mspx>
8. Nel, Louis. “Risk assessment essentials”. ZDNet. 6 Dec. 2002 <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2901057,00.html>
9. Snyder, Joel. “Content is king”. NetworkWorldFusion. 16 Feb. 2004. <http://www.nwfusion.com/reviews/2004/0216ipscontent.html>
10. Desai, Neil. “Intrusion Prevention Systems: the Next Step in the Evolution of IDS”. SecurityFocus. 27 Feb. 2003 <http://www.securityfocus.com/infocus/1670>
11. Technical Incursion Countermeasures. “FAQ: Network Intrusion Detection Systems. Version 0.8.3”. March 21, 2000 <http://www.ticm.com/kb/faq/idsfaq.html#3.6>