Global Information Assurance Certification Paper

Andrew Barratt
GCFW Practical
Version 4.1

The Future of Network Intrusion Prevention

GIAC Enterprises Security Architecture

Date:
Feb 22 2005

Table of Contents

List of Figures

Assignment 1: The Future of Network Intrusion Prevention

Abstract

If considering implementation of Network Intrusion Prevention System (NIPS) technology, understanding the impact on a company's existing defense in depth strategy is essential. It requires understanding of where NIPS would be deployed in an existing topology. It requires understanding of the impact NIPS would have on all traffic passing through this choke point. It requires consideration of the differences between the current types of NIPS solutions available.

This section is an assessment of the NIPS technology currently available. The objective is to determine the impact current NIPS would have on perimeter security if deployed within typical network topologies. Are NIPS ready to be deployed to our networks? Will NIPS eventually replace existing IDS, firewall and/or network antivirus components of perimeter security? These questions will be addressed. This section is deliberately vendor independent.

First things first - Intrusion Detection vs. Intrusion Prevention

This paper uses Dirk Lehmann's definition of *intrusion detection*:

> *The art of detecting inappropriate, incorrect, or anomalous activity.*[1]

The following definition of *intrusion prevention* has been adopted:

> *The art of preventing inappropriate, incorrect, or anomalous activity.*

In order to prevent, we must first detect. This makes intrusion prevention a superset of the functionality required for intrusion detection.

Clarity is in order - IDS, HIDS, NIDS, DIDS, HIPS, and NIPS

Intrusion Detection Systems (IDS) have been around for many years. IDS analyze network traffic and/or system behavior, detect events indicating potential attacks, and generate alerts based on these events. The alerts are later analyzed to identify potential threats, giving administrators opportunity to mitigate. Sometimes time allows administrators to defend against a mounting threat, such as an exploit of a new vulnerability. Sometimes administrators can identify compromised systems. IDS are well accepted as important components of a defense-in-depth strategy. To confuse matters, some intrusion prevention techniques have also been in use by some IDS for many years. These include session termination techniques and dynamic firewall policy

[1] Dirk Lehmann. Siemens CERT. SANS IDS FAQ. http://www.sans.org/resources/idfaq/what_is_id.php

updates.

Host Intrusion Detection Systems (HIDS) are IDS installed as a security measure on a single host. Detect and alert functions are specific to only the host running the HIDS. Many personal firewalls contain HIDS features.

Network Intrusion Detection Systems (NIDS) are IDS installed as a network security measure. Detect and alert functions relate to all network traffic passing through a network. NIDS are typically connected to a span port on a switch to act as a stealthy device on the network. They are commonly configured to have no ability to generate traffic. This in often achieved by configuring no IP address on the IDS interface designated for monitoring. The switch port is also often configured to allow no traffic to be accepted from this IDS interface. Older installations were often patched to hubs with a modified receive-only Ethernet cable achieving the same result.

Distributed Intrusion Detection Systems (DIDS) include multiple IDS over large networks. Typically a central server is used to correlate monitored data, conduct incident analysis, and maintain the known attack data. DIDS provides a more effective and efficient method to identify coordinated attacks across network segments. Often the terms IDS and NIDS are used to describe DIDS.

Host Intrusion Prevention Systems (HIPS) are a new generation of HIDS with significantly more intrusion prevention features. Typically HIPS can use user interaction to allow/deny specific connections, or enable/disable program attempts at using specific functions of an operating system.

Network Intrusion Prevention Systems (NIPS) are a new generation of NIDS with significantly more intrusion prevention features. Typically NIPS are dual homed and are deployed in-line at a network choke point in the same way as a network firewall. Decisions based on typical IDS alerts and are enforced by NIPS. They will typically modify, delay, or block some traffic identified as a threat.

What problem does NIPS mitigate?

As NIDS technology evolved it became well accepted as a requirement for balanced defense in depth strategy. After investigation of NIDS alerts, administrators can determine if an incident has occurred. The result is a retrospective and manual hardening of perimeter and host security. The importance of this function should not be underrated.

Would it be better if an incident never occurred? Yes. NIPS attempt to prevent incidents occurring. NIPS enable changing the strategy from reactive to proactive. Although Gartner[2] published a high profile and controversial report indicating that IDS is

[2] http://www4.gartner.com/Init

dead and the future is IPS, network intrusion prevention is a difficult task to achieve for two reasons.

1. Time does no allow an opportunity for manual investigation.
2. A suitable prevention technique must be prepared in advance and applied in real time.

What problem does NIPS introduce?

False positives

False positives are the biggest threat to the success of NIPS. While false positives waste resource for NIDS administrators, they can be disastrous to a company running NIPS.

A false positive occurs when an IPS incorrectly identifies an IP packet or number of packets as part of an attack. The IPS traps the traffic and therefore implements denial of service. A false positive triggering interruption to significant business activity falls in the same league as an unplanned outage.

Both manufactures and IT managers have a fear of false positives. It is the IT manager who ultimately recommends and/or approves purchase of new technology. If the IT manager approves the deployment of NIPS as part of a solution to lower a company's operational risk, it is the IT manager who will fully own responsibility for the impact of a false positive. Therefore only when IT managers believe the risk of false positives is acceptable will NIPS form a standard component of perimeter protection topology.

What are the factors leading to false positives? Most NIPS solutions depend on a signature database to identify all or some attacks. There is therefore a dependency on vendor signature databases. Just as antivirus signatures sometimes match data unrelated to viruses, NIPS signature databases can incorrectly identify data in transit as part of an attack.

A major contributor to false positives is improper configuration. In order to configure a NIPS using best practice, an administrator should understand all events that will contribute to a diagnosis and trigger preventative action. This can be quite a significant amount of knowledge. Although vendors may market NIPS technology as a simple, low overhead technology, the impact of poor configuration is high which makes attention to detail important.

Doesn't that same apply to firewalls? It is indeed true that firewall administrators must have a sound knowledge of the behavior of their firewalls to minimize outages caused by poor configuration. The most significant difference is that NIPS are newer technology. There are fewer administrators who have the required skills to ensure the same level of correct configuration.

To summarize, the following two issues make false positives a major issue:

1. Detailed understanding of NIPS requires specialist knowledge.
2. The impact of poor configuration can be significant.

The solution is to ensure administrator training is budgeted when considering NIPS. As best practice administration of NIPS requires ongoing attention to new threats, the ongoing resource requirement must not be underestimated.

False Negatives

A false negative occurs when a NIPS has not served its purpose by preventing a specific threat. This is undesirable, but is not feared like the false positive. No negative impact to passing traffic has taken place.

However, if a defense-in-depth strategy has not been enforced, the impact of a false negative is more significant. An example is where NIPS filtering is relied upon instead of implementing a regular workstation patching processes.

How is Deployment Best Achieved?

Implementing NIPS is best achieved by deploying devices in passive mode. The period in which intrusion prevention is disabled depends on the nature of the services utilizing the topology. Where no real-time business critical services in place, companies have enabled prevention within a week of deployment and been satisfied will the level of false positives.

Integration cuts down on false positives. Some IPS solutions scan hosts (passively if required) to identify characteristics of the systems to be protected. A database of vulnerabilities for each system can be identified. The NIPS therefore can base a decision on whether a host is vulnerable to an attack or not. If not, when prevention is enabled, no action need be taken to block traffic. In this way even when attacks are identified, prevention is only applied when required. This is one measure taken to reduce false positives.

Marry or Separate?

Why is NIPS technology implemented on a separate device rather than integrated into existing devices?

Firstly, to a degree, NIPS technology is indeed being integrated into existing firewalls as a set of optional features complementing the more traditional firewall functions. Appliances in particular include some IDS and some NIPS features such as basic DOS protection.

Secondly, as is typical, it was primarily small companies that originally pushed the new technology.

"We're seeing these little companies coming up with innovative techniques that threaten the older established markets."[3]

These companies primarily developed new devices rather than enhancing existing devices owned by larger companies. The established companies in the firewall, IDS and antivirus markets have now moved into the emerging market. The best of the start-ups have been absorbed.

Thirdly, however, at this stage, creating fuller featured NIPS implementations on separate devices makes more sense to both manufacturers and customers. NIPS are not as mature a technology as perimeter firewalls. Integrating significantly new functionality into a mature firewall product carries some risk. For example, if false positives are generated, even if due to configuration issues, then the reputation of the mature firewall is at stake.

In the future, NIPS is likely to mature and become a commonly deployed solution. It is then more likely to be fully integrated with existing firewall, IDS and antivirus solutions on a single device.

As new and enhanced implementations rapidly emerge, vendor solutions can differ significantly.[4]

Get In-Line?

Most, but not all, NIPS solutions are designed to be deployed in-line at a choke point in the perimeter network topology. The advantage of an in-line device is that traffic is more easily changed, blocked or throttled. The device can intercept traffic and in theory can have full control of passing connections, like a network firewall can, in theory. The level of control however comes down to the inspection techniques and prevention techniques utilized.

What about performance? Several vendors provide NIPS technology operating at speeds up to one Gigabit per second making deployment on LANs possible. Performance should not be a show-stopper. If latency sensitive applications are in use, take time to compare performance of different solutions. Many NIPS are primarily marketed to intercept traffic from a WAN link.

What about single point of failure? No doubt that any device in-line is an additional point of failure. Many NIPS can be configured to fail open as a default fail-soft

[3] John Pescatore. Gartner Internet Security Reasearch Directore. 2002. http://www4.gartner.com/Init

[4] Network Word: IPS Tested on a Live Production Network. http://www.nwfusion.com/buzz/2002/intruder.html

measure. The success of this depends on the type of failure. If service availability is a significant concern, it is worth looking at vendor solutions that have redundant components and fewer components that fail more frequently, such as hard disks. In general, high availability (HA) solutions do not yet match what is expected from the firewall market. HA is certainly an area that will be developed further in the future.

Viruses and Worms

An IPS can protect networks from attacks even when host systems are not yet patched. This is an enormous benefit to companies that have patch management processes with slow turnaround. It allows more time to patch vulnerable systems. Until patched, the vulnerable systems are certainly still vulnerable, but not from attacks through the IPS.

NIPS successfully blocked Blaster and Sasser worms from the Los Alamos National Laboratory, US Department of Energy.[5]

A good IPS will identify vulnerabilities specific to each host protected. By filtering on vulnerabilities, rather than just attacks, new attacks using a known vulnerability can be prevented.

Just as for host anti-virus solutions, the vendor analytical team is what allows an IPS to identify new vulnerabilities and new attacks. A good IPS will automatically update its vulnerability database faster than an administrator can patch vulnerable systems.

NIPS and the Future

NIPS technology is rapidly improving. The solutions available now are certainly good for some organizations. The strongest driver toward adoption of NIPS is protection against virus and worms threats from the Internet. Patch management is an area of IT that requires immediate attention. If NIPS solutions find their way into patch management strategies, then the future of NIPS is secured.

However, the issue of false positives will not go away. This makes NIPS unsuitable for some environments. The biggest challenge for NIPS technology will be how well future NIPS devices minimize the impact of false positives. Unfortunately bad news travels and will have a major impact on the adoption of NIPS. Other areas of development for NIPS are in enterprise management and HA. These are areas normally addressed as newer technologies mature.

NIPS for GIAC Enterprises?

[5] SANS Webcast. What works in Intrusion Prevention: A Real World Case Study from Los Alamos National Laboratory, US Department of Energy. Paul Criscuolo. http://www.sans.org/webcasts/archive.php

The next section of this paper presents the design of a secure network perimeter topology for GIAC Enterprises (GIACE). Would NIPS complement the defense-in-depth strategy used in this design? Please use the List of Figures to refer to the GIACE network diagrams in the next section.

When considering NIPS technology, the first crucial decision to make is whether the benefits of attack prevention outweigh the risk and impact of false positives. This is a case of horses for courses.

GIACE would need to measure the frequency and impact of false positives to make an accurate assessment. This would first need to be done in a lab environment, and if a reasonable level of confidence were attained, using an IPS in passive mode on the perimeter network. This may require purchase of equipment before a decision about permanency of use can be determined.

In the GIACE network topology, the firewall is a choke point where multiple networks with different levels of trust intersect. NIPS may be best located between the head office perimeter router and firewall. This would intercept all traffic to and from the Internet. Note however, that the VPN traffic would not be filtered as the encryption prevents visibility.

The Netscreen firewall has intrusion prevention features including DOS related throttling and network-based antivirus protection. The embedded antivirus from Trend Micro utilizes signatures.

The F5 BIG-IP Local Traffic Manager also has intrusion prevention features. Due to its location in the topology, these features protect the DMZ servers from connections sourced from the Internet and also internal networks. Most importantly, the corporate database on the web server(s) is protected from HTTPS when the traffic is inspected after SSL termination.

It is critical that staff managing NIPS have sufficient skills and time resource. Budget for ongoing training to support new infrastructure must also be considered. GIACE is already undergoing significant a change to perimeter topology. Staff will already require training to manage Netscreen firewalls and the BIG-IP Local Traffic Manager. In this regard it may be wise to delay the decision to deploy NIPS until staff are better skilled. It can increase risk to deploy too much new technology in a short time period.

GIACE has indicated it may consider a redundant topology. HA is an area of NIPS technology that requires further development. Current NIPS technology will form a weak link in a GIACE HA solution.

Dedicated NIPS in the GIACE topology would certainly increase defense-in-depth. However, a number of factors make it undesirable at this stage. A degree of intrusion prevention is already on the Netscreen and BIG-IP. There is already significant change in the topology to manage. The HA solutions available for NIPS do not currently meet

GIACE requirements. It is recommended that in the short term GIACE focus on strengthening the skills required to most effectively manage the solution presented in the next section. NIPS are not an immediate requirement for GIACE. However, NIPS technology will only improve and GIACE should review this decision in the future.

Assignment 2: GIAC Enterprises Security Architecture

Goals

Security Stance

GIAC Enterprises (GIACE) has recognized that its current security architecture will need to be updated to mitigate current and new security threats. GIACE does all of its sales via the Internet. Therefore implementing a defense in depth strategy has been identified as critical. GIACE has defined a security policy and requires new security architecture capable of implementing the appropriate protection of its resources and services.

Access Requirements

GIACE has categorized each group that requires access through the security architecture.

1. Customers - companies or individuals that purchase bulk online fortunes
2. Suppliers - companies that supply fortune cookie sayings
3. Partners - international companies that translate and resell fortunes
4. The general public
5. GIACE employees on internal networks
6. GIACE employees in regional satellite offices
7. GIACE sales force using remote access

The corporate database is a MySQL database. It is accessed using an HTML and PHP based web interface. All required functions on the database are available via HTTP or HTTPS. The web interface can be used to authorize access to restricted parts of the database. Only HTTPS access is allowed to parts of the database not available to the general public.

Customers, suppliers and partners require secure access to the GIACE corporate database of fortunes. This can be achieved using SSL with a standard browser. SSL signed certificates from VeriSign or another reputable authority can be used. HTTPS access to the web interface from the Internet must be enabled.

To service customers, online payment services from a third party can be leveraged, or alternatively credit cards such as Visa can be directly accepted. Transactions require access policies to enable connections such as SSL from the web server to the party authorizing transactions.

The general public only requires unencrypted HTTP access to the database.

GIACE employees on internal networks, regardless of the office in which they work, require access to the corporate database via HTTP and HTTPS. They require access to email via POP3 to the GIACE SMTP gateway. Employees require HTTP and HTTPS access to the Internet, preferably using a proxy. Employees on internal networks in regional satellite offices require unrestricted access to the head office internal network, and internal networks of other regional satellite offices. A hub and spoke IPSEC VPN topology will enable inter-office communications.

GIACE sales staff need secure access from their laptops to internal networks. A remote access VPN solution will be implemented.

Data Protection

GIACE has classified all categories of data it handles. GIACE has identified that the contents of its corporate database is the most important resource it needs to protect. It is recognized that the corporate database integrity and availability to customers, suppliers and partners is critical to surviving as an Internet based business.

The corporate database availability to employees and the general public is also important, but not critical if unavailable for short periods. Employee access to Internet data is not regarded as critical if unavailable for short periods. Employee access to other internal data resources is not regarded as critical if unavailable for short periods.

The GIACE security policy includes reference to a standard for data classification. The following data classification matrix represents the data that was considered in the design of new GIACE security architecture. The new architecture provides the most significant defense in depth in relation to protection of the corporate database. The “Architecture Components” section provides detailed description of how defense in depth has been used to address protection of the different levels of data classified.

Data Classification and Protection Matrix

Data Description	Data Classification	Risk to GIACE	Data Location	Protection Strategy
Samples of fortunes	Generally Accessible	Low – Unauthorized access is not a factor. Breach of data integrity not considered a major threat.	1. HO file servers 2. RSO file servers 3. Corporate laptops 4. In transit between HO, RSOs & corporate laptops 5. In transit between HO & customers, suppliers, partners and general public.	Although some security exists to protect this data, no specific resource has been allocated for this purpose. Security only exists if it is primarily used to protect another data category.
Subsets of customer / supplier / partner data from database	Confidential	Medium - Potential loss of current and future customers, suppliers and partners.	1. HO file servers 2. RSO file servers 3. Corporate laptops 4. In transit between HO, RSOs and corporate laptops	1. Protect file servers with perimeter security at HO & RSOs. 2. Protect file servers with host and data security. 3. Implement VPNs for transit of data on un-trusted networks. 4. Staff education.
Subsets of fortunes from database	Confidential	Medium – Potential loss of business to current and future customers. Potential advantage to competition.	1. HO file servers 2. RSO file servers 3. In transit between HO & RSOs 4. In transit to customers from HO 5. In transit from suppliers to HO 6. In transit between partners and HO	1. Protect file servers with perimeter security at HO & RSOs. 2. Protect file servers with host security. 3. Implement VPNs for transit of data on un-trusted networks. 4. Staff education.
Complete linked fortune and customer / supplier / partner database	Secret	High – Most valuable GIACE data resource. Potential loss of current and future customers. Potential advantage to competition.	Corporate Database Server	1. Restrict data to Head Office database servers and backup servers / media. 2. Protect Head Office database servers using defense in depth. 3. Implement host and data security on hosts where data resides.
HR data	Secret	High – Legal and compliance issues affecting right to operate. Employee dissatisfaction.	Head Office Servers.	1. Restrict data to Head Office internal network. 2. Appropriately protect internal network from external networks. 3. Appropriately implement host and data security on hosts where data resides.

Corporate strategic and financial data	Secret	High – Potential loss of future business. Potential advantage to competition.	Head Office Servers	1. Restrict data to Head Office internal network. 2. Appropriately protect internal network from external networks. 3. Appropriately implement host and data security on hosts where data resides.

HO = Head Office
RSO = Regional Satellite Office

Principles

Technology Currently in Use and Employee Skill-set

GIACE currently uses Cisco switches, Cisco routers, Red Hat Linux, Apache, MySQL, HTTP and PHP. Windows XP is used on the desktop. This is not unusual for of a company of this size and focus. The current security architecture is based on Cisco packet filtering and does not implement significant defense in depth.

GIAC recognizes that IT staff skills will need to be updated to support new security architecture. GIAC is prepared to train IT staff in administration of two new network devices. New security tools and functionality based on technologies currently in use are also welcomed. IT Staff will be given opportunity to update their skills on these tools.

IT staff have knowledge of security principles including firewall and VPN technology. They are interested in learning how to support new products. They are interested in building on their Red Hat knowledge by implementing new tools on Red Hat systems.

The selected solution takes into consideration technology in use and the current skill-set of GIACE IT support staff. Two new appliances will be introduced to the IT staff – Juniper Netscreen firewalls and F5 BIG-IP Local Traffic Managers. Additionally some tools on Red Hat Linux will be used which may be new to them. Iptables will be used to configure Netfilter for host security on DMZ hosts. Snort and ACID will be used for intrusion detection. Tripwire will be used for host integrity checking. OPIE will be used for one-time password authentication of administrative access. Sudo will be used for logging and compartmentalization of root privileges.

The new network architecture will have no major impact to the skill-set required of users. However, the use of pre-configured IPSEC clients for remote access will require internal training. Note that SSL clients were seen as a user-friendlier and lower maintenance solution; however GIACE did not consider this factor significant enough to warrant expenditure on a separate SSL based solution. As GIACE scales this may change. An SSL solution can easily be added to the topology.

Performance

GIACE has indicated that GIACE owned technology enabling customers, suppliers and partners to connect to the corporate web servers should add a minimum of latency. GIACE also allows the general public to access samples from its database. Access from the general public is seen to increase the market and attract new customers, it accounts for the majority of traffic to the web server farm. More importantly, it makes predicting future load difficult. If marketing is successful and this site becomes heavily utilized, GIAC wants to be in a position to handle load without immediate requirement to upgrade hardware. Additionally GIACE wants to easily be able to upgrade individual components of the architecture with minimum impact to other components.

To meet these requirements the design is scalable. It has incorporated a load balancing function. At any stage, additional web servers can be deployed behind the load balancer(s). The load balancer also performs SSL acceleration for the web servers. The firewalls use reasonably priced ASIC based technology for minimizing latency, even when also used for VPN termination. Circuits to ISP(s) can be upgraded as required. The "Architecture Components" section covers detailed implementation to address the performance requirements.

Open Source and 3rd Party Support

GIACE has indicated that open source solutions are welcomed. However, GIACE has have stipulated that all hardware and operating systems must have a well respected third party support offering available. Therefore Red Hat ES 3.0 Linux has been implemented for some components.

Budget

No budget has been specified by GIACE. The design supports the GIACE security stance and principles, including the capacity to scale. Given these requirements, cost has been minimized appropriately and is commensurate with the risk and impact to GIACE of a significant incident.

Staff retraining has been minimized. Some functions are implemented on Red Hat Linux with standard GIACE hardware as low cost solutions. The Juniper Netscreen 50 in the head office and the Juniper Netscreen 5GTs in regional satellite offices are the least expensive new product that meets the functionality and performance requirements. The BIG-IP LTM 1500 is the least expensive of the F5 range meeting requirements. The Cisco 3725 has been selected to handle Internet traffic from large ISP links as it is envisaged that large amounts of traffic may be transferred to and from the corporate database in batches. An Ethernet switch module installed to the router provides an inexpensive solution for IDS visibility on both sides of the filtering router.

Both the SSL acceleration and the load balancing solution will be implemented on the BIG-IP Local Traffic Manager. This device also alleviates the need for a separate DMZ switch.

As discussed in the "Technology Currently in Use and Employee Skill-set" above, SSL remote access was not implemented to save on costs. The Juniper Netscreen IPSEC solution is cheaper if the number of users is low.

There are no switches deployed in small branch offices where the number of connected workstations is 4 or less. The hub within the Juniper Netscreen 5GT firewall is populated instead. However, this cost saving measure allows easier network sniffing on the internal RSO network. GIACE has indicated that this is an acceptable risk at this time.

High Availability

GIACE does not see return on investment for implementation of a high availability (HA) security infrastructure at the time of implementation. However, GIACE does not want to be designed into a corner. GIACE requires that the design have the flexibility to be scaled to an HA infrastructure in the future.

Specifically, GIACE sees a potential future requirement for HA capability for some or all components used to allow customers, suppliers and partners to access the GIACE corporate database. The corporate database is maintained on the same servers that act as web servers. Therefore connectivity to the web server farm may require HA in the future.

The perimeter design topology and each individual component are HA capable. Specifically:

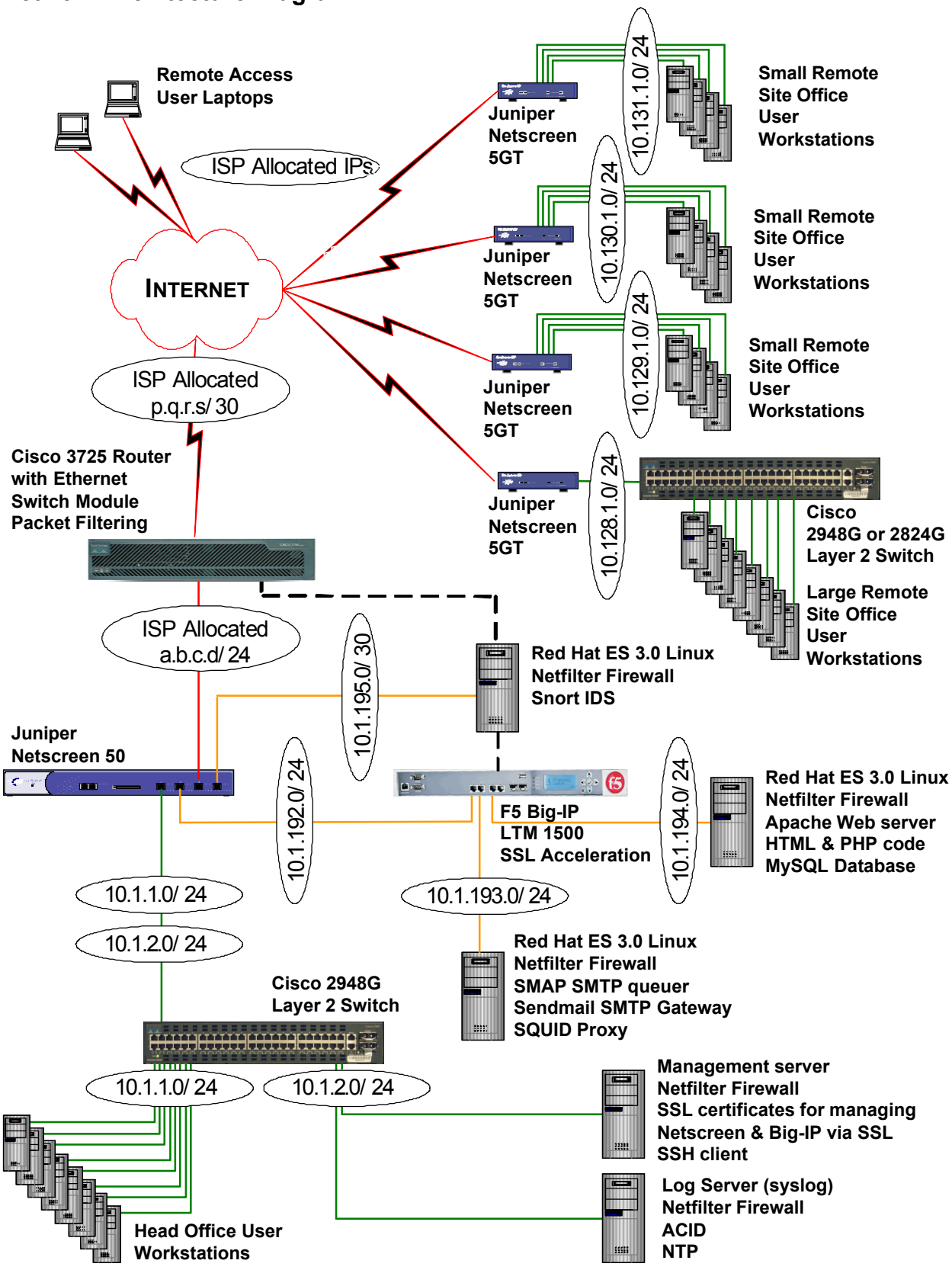
1. The filtering router is HA capable. HA requires purchase of an additional Cisco 3725 router.
2. Multiple ISP circuits can be used, each connected to a separate HA filtering router. If possible, different ISP should be used for each circuit. If possible, each ISP should use separate exchanges, separate building risers and separate building entry points to minimize single points of failure.
3. The head office firewall is HA capable. HA requires purchase of another Juniper Netscreen-50 firewall. VLAN tagging has been implemented in the network design to ensure an interface on the firewall remains available for HA if/when required.
4. Load balancing has been implemented in the design. Multiple web servers can therefore be deployed behind the load balancer(s).
5. The load balancer is HA capable. HA requires purchase of another F5 Big-IP Local Traffic Manager 1500.
6. External DNS is handled by the ISP(s). An ISP with an HA DNS infrastructure should be selected.

Network Diagrams

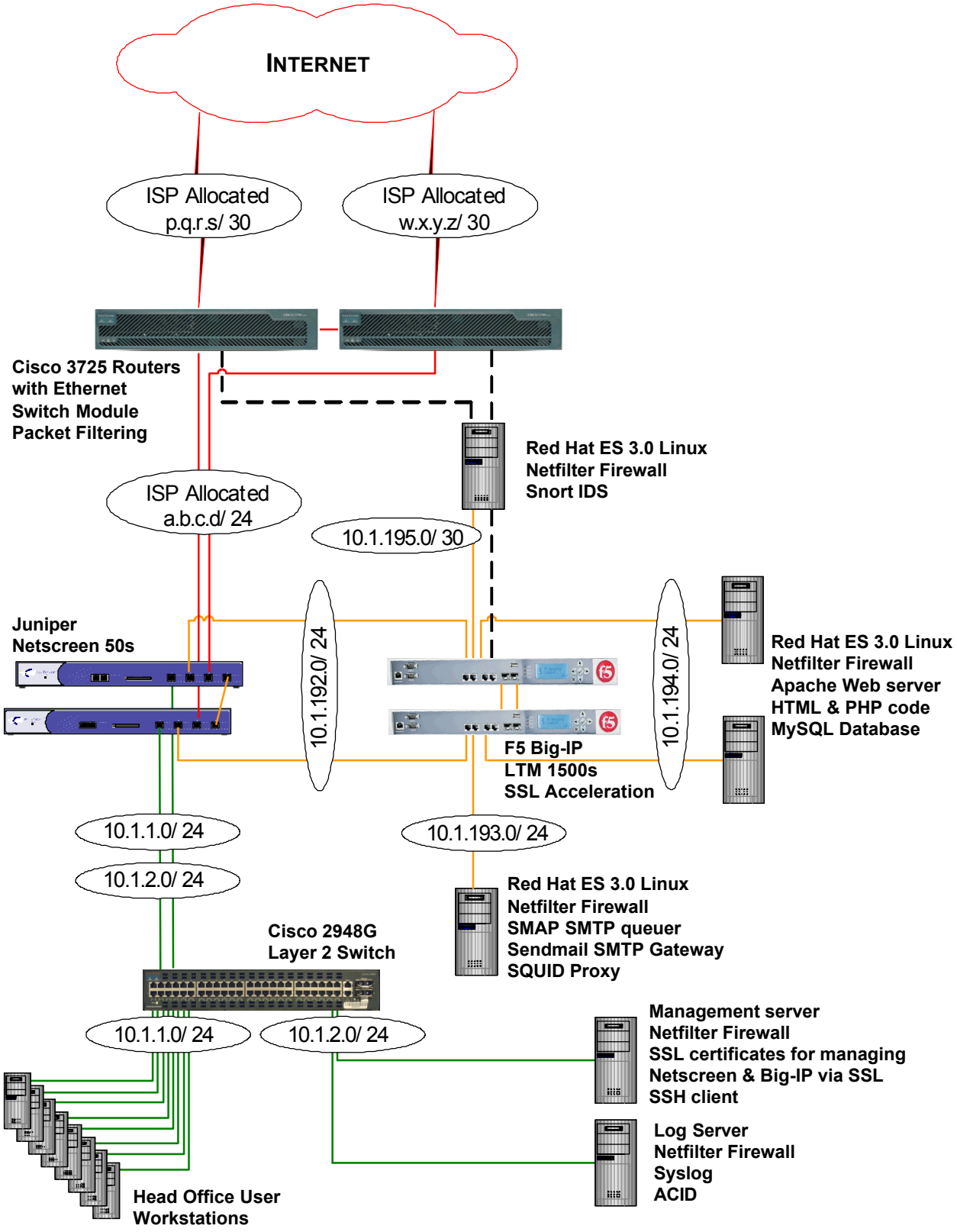
The security architecture is best understood by first referring to the detailed network diagrams. After initial inspection, the following sections can be referenced for further detail.

Note that the HA diagram depicts a potential future topology for the head office. An HA infrastructure is often regarded as cost inhibitive. It may be that if GIACE chose to increase resiliency, then only some components depicted would be configured for HA. The likely candidates are the ISP connections and routers. Deploying the additional web server may be next consideration. The data flows are almost identical between the standard and HA designs.

Network Architecture Diagram



Network Architecture Diagram – High Availability



Data Flows

The data flow table below clarifies how each of the major groups will interact with GIACE. For more detailed discussion and full data flow tables used to define firewall rules, please the later section, “Data Flow through the Firewall”.

Data Flow – Group Access Perspective

Source	Destination	Port(s) Protocol	Description
Customers	Web Server	TCP 80 HTTP	Allow customers to connect from Internet to corporate web server to transfer generally accessible data.
Customers	Web Server	TCP 443 HTTPS	Allow customers to connect from Internet to corporate web server to transfer confidential data.
Suppliers	Web Server	TCP 80 HTTP	Allow suppliers to connect from Internet to corporate web server to transfer generally accessible data.
Suppliers	Web Server	TCP 443 HTTPS	Allow suppliers to connect from Internet to corporate web server to transfer confidential data.
Partners	Web Server	TCP 80 HTTP	Allow partners to connect from Internet to corporate web server to transfer generally accessible data.
Partners	Web Server	TCP 443 HTTPS	Allow partners to connect from Internet to corporate web server to transfer confidential data.
General public	Web Server	TCP 80 HTTP	Allow general public to connect from Internet to corporate web server to transfer generally accessible data.
GIACE employees using remote access (Sales Force)	Mail Gateway	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 110 POP3	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to send and retrieve mail.
GIACE employees using remote access (Sales Force)	Squid Proxy	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 8080	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows users to connect to Squid proxy for HTTP & HTTPS Internet browsing. Note that employees using remote access must connect to the Internet via the proxy. This increases latency, but enforces better security.

GIACE employees using remote access (Sales Force)	Web Server	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 80 HTTP	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to connect to the corporate web server.
GIACE employees using remote access (Sales Force)	Web Server	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 443 HTTPS	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to connect to the corporate web server.
GIACE employees in regional satellite offices (RSOs)	Mail Gateway	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 110 POP3	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to send and retrieve mail.
GIACE employees in regional satellite offices (RSOs)	Squid Proxy	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 8080	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows users to connect to Squid proxy for HTTP & HTTPS Internet browsing. Note that employees in RSO sites must connect to the Internet via the proxy. This increases latency, but enforces better security.
GIACE employees in regional satellite offices (RSOs)	Web Server	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 80 HTTP	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to connect to the corporate web server.
GIACE employees in regional satellite offices (RSOs)	Web Server	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 443 HTTPS	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to connect to the corporate web server.
ISP SMTP gateway	Squid proxy (SMTP gateway)	TCP 25 SMTP	Allow mail server to receive mail from Internet SMTP gateway.

IP Addressing Strategy

GIAC uses non-routable private addresses internally[6]. This is one defense in depth measure that ensures connections to internal network IP addresses initiated from the Internet can not be established. Additionally, if there was a firewall configuration error and outgoing connections were not translated by the firewall, they would not be bi-directional. This strategy also allows GIACE to use 17,891,328 internal addresses. ☺

Routable addresses are supplied by the ISP(s). The routable addresses configured to GIAC devices are:

1. Head office filtering router interfaces (LAN and WAN).
2. Head office firewall Untrust interface.
3. NAT address for corporate web server farm.
4. NAT address for SQUID HTTP/HTTPS server.
5. NAT address for SMAP & Sendmail SMTP server.
6. NAT address for log server.
7. NAT address for management server.
8. Each regional satellite office's firewall Untrust interface.

The routable NAT addresses are translated to/from private addresses on the head office Netscreen firewall. Additional routable NAT addresses can be allocated. For example, it may be desirable for different functions of the web server farm to be available via different IP addresses.

Although web proxy (HTTP/HTTPS) and mail (SMTP) services are located on the same server, the server uses virtual interfaces to ensure separate IP address for each service. This makes mapping the GIACE network slightly more difficult for interested Internet parties.

The private IP address networks are allocated according to the following logic:

1. The 2nd octet indicates which site a network is located in.
2. A 1 in the second octet indicates the head office.
3. The range 128-255 in the 2nd octet indicates an RSO.
4. A 10 in the 2nd octet indicates an inter-office VPN network.

5. The 3rd octet indicates the network location within a site.
6. The range 1-99 in the 3rd octet indicates an internal network.
7. The range 100-127 in the 3rd octet indicates a remote access network.
8. The range 192-227 in the 3rd octet indicates a DMZ network.

[6] http://www.ietf.org/rfc/rfc1918.txt

IP Address Allocation

Network	Netmask	Location	Primary Firewall Zone	Description
a.b.c.d	24	Head Office	Untrust	ISP allocated IP address space. Segment between filtering router and primary firewall.
p.q.r.s	30	Between Head Office and Internet	Untrust	ISP allocated IP address space. WAN segment between filtering router and ISP.
10.1.1.0	24	Head Office	Trust	User access network – head office.
10.1.2.0	24	Head Office	Trust	Management network.
10.1.192.0	24	Head Office	DMZ	F5 BIG-IP Local Traffic Manager segment. Virtual server IPs for connecting to web farm, SMTP gateway and HTTP/HTTPS proxies defined.
10.1.193.0	24	Head Office	DMZ	SMTP gateway and HTTP/HTTPS proxy segment.
10.1.194.0	24	Head Office	DMZ	Web server farm segment.
10.1.195.0	30	Head Office	DMZ	IDS management segment.
10.1.100.0	24	Remote Access VPN	Trust	VPN remote access segment. Remote access users are allocated addresses from this network.
10.10.10.0	24	Inter-office VPN	Spoke	VPN spoke segment. Virtual segment between head office Netscreen 50 and regional satellite office Netscreen 5GTs.
10.128.1.0	24	Regional Satellite Office 1	Spoke1 Tunnel	User access network – regional satellite office 1.
10.129.1.0	24	Regional Satellite Office 2	Spoke2 Tunnel	User access network – regional satellite office 2.
10.130.1.0	24	Regional Satellite Office 3	Spoke3 Tunnel	User access network – regional satellite office 3.
10.131.1.0	24	Regional Satellite Office 4	Spoke4 Tunnel	User access network – regional satellite office 4.

Regional Satellite Offices

Each of the 4 Regional Satellite Offices (RSOs) has the same standard network topology. An RSO uses an ADSL connection to the Internet.

A single ISP will be selected for all four RSOs and head office. The ISP must provide reliable service in all current RSO locations and potential locations for new RSOs. Exceptions are only to be made where high pricing or lack of coverage provided by global ISPs forces selection of a local ISP. Using multiple ISPs increases complexity, adds to administrative management of the relationship with ISPs and reduces leverage if service comes under scrutiny.

Perimeter protection at each RSO is implemented with a Juniper Netscreen-5GT. NetScreen-5GT series incorporates antivirus features using Trend Micro's antivirus technology.

Head Office and Regional Satellite Office Connectivity

An IPSEC based VPN topology utilizing the internet is the best solution for HO to RSO connectivity. GIACE uses no latency sensitive applications and has no future requirement for them. Dependence on the reliability of the internet is deemed acceptable.

The cost of leased lines between sites for a company the size of GIACE is inhibitive. Although cheaper, ISDN is still cost inhibitive and does not provide significant reliability over internet VPN. ISDN would only be used where in an RSO where ADSL is not offered.

The hub and spoke solution will scale easily as more RSOs are established. GIACE has indicated that RSO to RSO communication would only be used for low bandwidth and low latency requirements in the future. Therefore using the HO site as the hub is the best topology. The Juniper Netscreen 50 at the HO site will form the head end of four VPNS. The four tail ends will be terminated on the Juniper Netscreen 5XTs at each RSO.

RSO Netscreen 5GTs only allow traffic from the internal RSO network traffic to the internet via VPN to the head office. Mail and web browsing from an RSO utilizes the head office proxy infrastructure. Although this does increase latency, it enforces strong security to break all Internet bound user connections.

Remote Access for Employees

Some employees, including the sales force, do not work in the HO or RSOs every day. These employees require a solution to allow access to the HO and RSO internal

© SANS Institute 2000 - 2005 Author retains full rights.

networks. These employees use laptops and can connect to the Internet via IPASS[7] for Internet roaming.

Remote access is secured using IPSEC. An IPSEC client is loaded to each laptop. The Netscreen 50 firewall at the head office terminates the VPNs. Netscreen is currently the fastest device for terminating IPSEC VPNS. Policies can be enforced on traffic from the VPNs. This includes use of the Trend Micro antivirus solution embedded in the Netscreen.

Note that SSL is a solution that may be adopted in the future. As the number of remote access users increase, the cost of implementing an SSL termination device is further justified. SSL is available as part of all standard Web browsers, therefore SSL eliminates the need for client software deployment and ongoing maintenance.

Architecture Components

Significant most features of the architecture components have already been discussed in the context of other sections. Therefore, for some components in this section, descriptions will be brief and will not restate details already covered.

Juniper Netscreen Firewall

The Juniper Netscreen 50 is an impressive appliance[8] and is well respected. It has been selected as the HO firewall to serve three primary purposes.

1. Enforcement of GIACE perimeter security policy.
2. Enable secure communication between HO and RSOs.
3. Enable secure remote access for employees with laptops.

The Netscreen firewall is running ScreenOS 5.0.0 release9. This is the latest release of version 5.0.0 firmware. It has been well tested in the wild.

The ASIC based Netscreen 50 is a high performance firewall for GIACE's requirements. The Netscreen 50 will continue to perform as more IPSEC VPNs are introduced. It has been selected to scale. The HA capabilities of the Netscreen may be used by GIACE in the future, including sub-second failover.

The Netscreen 50 does not support SSL termination for HTTPS traffic to the web server farm. The BIG-IP Local Traffic Manager has been implemented to support this and can inspect to layer 7.

The Netscreen 50 has IPS features that can optionally be enabled. The Netscreen firewall can detect many known DOS attacks and can throttle traffic from identified IP

[7] http://www.roamintl.com/about.html
[8] http://www.juniper.net/products/integrated/dsheet/110003.pdf

addresses accordingly. The Netscreen has an embedded antivirus from Trend Micro which utilizes a regularly downloaded signature database.

A detailed description of the firewall implementation including data flow tables and configuration follows in a later section.

Cisco Perimeter Router

The perimeter router is a Cisco 3725[9] with an Ethernet switch network module[10]. The router will be loaded with Cisco IOS Release 12.3 or latest Cisco recommended IOS. The Cisco 3725 is the first GIACE device to see Internet traffic and was selected to handle periods of high utilization from the Internet, including DOS attack. Lengthy access lists are implemented on the router for ingress and egress traffic. The Ethernet switch module is used to connect the IDS to the monitor traffic on the LAN interface of the router.

A detailed description of the router implementation including access list detail and full router configuration follows in a later section.

F5 BIGIP Load Balancing & SSL Acceleration

The F5 BIG-IP Local Traffic Manager 1500 with SSL module running v9 has been selected for load balancing and SSL acceleration. The BIG-IP is a leader in SSL acceleration. It is an impressive device[11] which also contributes to the defense-in-depth protection of the corporate database located on the web server(s). This is GIACE's most important resource. NIPS features on the BIG-IP provide protection that can be applied to the decrypted HTTPS traffic.

The BIG-IP is capable of performing important functions that provide an additional perimeter between the GIACE web server farm and Internet:

1. Provides TCP termination, independently managing client and server side connections.
2. Blocks known layer 7 attacks using customized event-based attack filtering.
3. Additional packet filtering, DOS and SYN flood attack protection.
4. Uses higher-standard AES for secure SSL acceleration when HTTP clients support it.
5. Encrypts cookies increasing level of user identity trust.
6. VLAN mirroring for IDS monitoring of attached networks.
7. Load balancing for Internet web server farm.

---

[9] http://www.cisco.com/en/US/products/hw/routers/ps282/ps283/

[10] http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_chapter09186a00800b168c.html#wp1022409

[11] http://www.f5.com/f5products/v9intro/ltm/Datasheet_BIG-IPLTM.pdf

8. HA capability for potential future requirements.

The BIG-IP is used instead of a switch in the DMZ. It allows scaling to utilize a web server farm and is also HA capable. VLAN mirroring options are impressive and allow the IDS to monitor traffic after SSL decryption.

Snort IDS

Like many companies, GIACE sees benefit in implementing an IDS infrastructure, but is unwilling to invest heavily in the function. This is an area of technology where open source and commercial solutions are quite competitive.

Snort 2.3.0[12] was chosen to perform real-time traffic analysis and logging. ACID was chosen as the management console. It will be used to for protocol analysis, content matching, and detection of attacks and probes. Of particular importance to GIACE are attempts at OS fingerprinting, stealth port scanning, buffer overflows and SMB probes.

GIACE has staff with Red Hat skills. Red Hat Enterprise Edition 3.0 or Fedora Core 3 is a suitable OS selection for GIACE IDS servers[13]. The decision between the two is primarily based on whether GIACE prefers reliance entirely on the open source community for IDS, or prefers to use a commercially supported OS to be consistent with other GIACE infrastructure.

The IDS will monitor both Untrust and DMZ zones. Please refer to the network diagram for clarification. The most heavily utilized IDS interface will be monitoring traffic between the filtering router and the perimeter firewall. The filtering router will be configured to block a significant amount of Internet sourced traffic. There will be no IDS directly monitoring unfiltered traffic sourced from the Internet.

The other IDS monitoring interface will be connected to the BIG-IP Local Traffic Manager. There are two ways BIG-IPs can be configured to mirror traffic to an IDS - VLAN mirroring and clone pools. Using the VLAN mirroring feature ensures layer two inspection is taking place. This removes reliance on the configured pools and higher layer BIG-IP inspection.

The IDS infrastructure will be used in passive mode with no connection killing (TCP resets) to be sent. This ensures that the IDS systems will have no impact on production traffic so that false positives pose no direct risk. The BIG-IP can also enforce this GIACE policy, regardless of how the IDS behave by setting the mirror_vlan_forwarding variable to disable.[14] The same functionality can be achieved on the Cisco switches using the switched port analyzer (SPAN) feature.[15]

---

[12] http://www.snort.org/
[13] http://fedora.redhat.com/about/rhel.html
[14] http://www.f5.com/solutions/deployment/mirroring_to_inspection_device45.html
[15] http://www.cisco.com/warp/public/473/41.html

Squid Web Proxy Cache

Squid web proxy cache version 2.5 (stable) 8 will run on Red Hat Enterprise Edition 3.0 with Netfilter firewall. This proxy will be used for caching outgoing web connections only. GIACE currently has 50 employees. There is therefore no requirement to use an appliance for this purpose. A Linux solution on GIACE standard server hardware will meet the performance demand.

Squid is free software[16] licensed under the GNU General Public License[17]. GIACE can rely on the open source community for support or can select an appropriate company for support from the long list maintained on the squid website.[18]

Squid supports SSL, extensive access controls, and full request logging. Squid can terminate SSL connections. It must be configured with configure with *--enable-ssl*. Squid can also tunnel any protocol using the CONNECT request method, however when configured this way the proxy doesn't understand or interpret the contents.

GIACE can configure the Netscreen firewall to authenticate the outgoing web requests.

Webalizer[19] can be run on the log server. Webalizer is a well respected and fast log analysis tool that can be used with the Squid logs. It is also free software licensed under the GNU General Public License. Webalizer produces easily configurable usage reports in HTML format, for viewing with a standard web browser. Squid logs can be pulled from the cache server to the log server via an automated script using SCP.

Note that browsers on employee workstations will use proxy.pac files to determine which resources are Internet based. There are good internet resources for tips on how this can be done[20]. The proxy.pac files can be delivered form a local server each time the first instance of a browser is opened.

Mail Gateway

The GIACE mail gateway will run on the same server as the Squid web proxy cache. Mail gateways are prime targets for attack and abuse. The server will use Red Hat Enterprise Edition 3.0 with Netfilter firewall. It will be protected from the Internet at a network level by the filtering router, the Netscreen firewall, and the BIG-IP LTM.

The gateway will accept POP3 from GIACE user workstations and laptops via the Netscreen firewall. It will run SMTP for communication with the ISP mail gateways. Only known hosts access to the SMTP server will be configured so that it will not

[16] http://www.gnu.org/philosophy/free-sw.html
[17] http://www.gnu.org/copyleft/gpl.html
[18] http://www.squid-cache.org/Support/services.html
[19] http://www.mrunix.net/webalizer/
[20] http://www.craigjconsulting.com/proxypac.html and http://www.craigjconsulting.com/setproxy.html

become an open relay server.

Postfix[21] is generally regarded as a simpler and more secure mainstream MTA alternative to Sendmail. As it is available by default on Red Hat and it would therefore be covered by Red Hat support contracts. It is also supported by a very active users' mailing list. Postfix does not impose unusual Unix management practices. It is fast and allows spam blocking from known spam sources. GIACE could also consider a mail queuer so that the SMTP port only provides an uninteresting subset of SMTP commands.

The POP3 variant APOP can be implemented to avoid sending unencrypted passwords. An encoded hash of the user's password is sent from the email client to the server. Note that another option is to use IMAP with SSL encryption for client authentication and data transfer.

DNS

Internal and external DNS will be separated. There is no need for internal addressing and naming to be available to external parties. RSOs and corporate laptops connected via VPN will have access to internal DNS, hosted on the HO internal networks.

GIACE's external DNS domain will be hosted by the ISP. The ISP selection will be made assuming ISP DNS domain hosting is a requirement. Note that outgoing, Internet destined HTTP & HTTPS will be proxied in the DMZ. The SMTP gateway is on the same host in the DMZ. Therefore this host is the only device that will need to resolve external DNS.

A future requirement may require new connectivity from internal resources to Internet destinations. In this case, an existing proxy can be used or new proxy deployed to the DMZ to securely meet the requirement. Again, the proxy server does the external DNS lookup.

Benefits and disadvantages of external hosting of GAICE DNS follow:

Benefits:

1. Less administrative overhead for GIAC - No need to implement and maintain an Internet facing DNS server.
2. Increased security – DNS servers are a prime target for hackers. By selecting the appropriate ISP, the DNS service may be well protected and GIACE has one less target on its networks.
3. Redundancy – The ISP, if selected appropriately, will have a DNS server farm behind redundant load balancers and network infrastructure. The ISP should therefore provide an HA service.

Disadvantages:

[21] http://www.postfix.org/

1. Less control of DNS changes – timing, errors and outages.
2. Cost – Outsourcing DNS may be more expensive than maintaining DNS on an existing proxy server.

NTP

GIAC devices use a protected GIACE NTP server. This is more secure than directly using external NTP. The GIAC NTP server is the only device that will establish NTP sessions to the Internet, minimizing exposure to Internet NTP threats. The log server running Red Hat Enterprise Edition 3.0 and Netfilter firewall will be used as the NTP server.

Logging

GIAC devices send syslog to a protected log server. The GIAC log server will run Red Hat Enterprise Edition 3.0 and Netfilter firewall. The Netscreen firewall is configured to allow syslog to the log server only from the IPs of the other GIACE devices.

Cisco Switches

Cisco 2948G switches have been selected for the internal network as they support private VLANS and VLAN tagging. They can be used in an HA configuration. The out-of-band management port can be patched directly to the management network which is protected by the Netscreen firewall. The latest Cisco recommended IOS will be applied.

Laptops

Corporate laptops will all have an identical build with a personal firewall solution and an antivirus solution. It will be policy that laptops are connected to the corporate network on a weekly basis to receive patches, full policy and antivirus updates.

Backup Strategy

The corporate database is backed up directly to two identical tapes on a daily basis. One tape is securely stored onsite. The other tape is securely stored offsite. No unencrypted backup data or configuration files are passed over the network.

Configuration files and tripwire output are downloaded to the management server. Rsync over SSH (TCP 22) or is run from daily from cron on the management server to each Linux host in the DMZ. SCP is run from daily from cron on the management server to the F5 Big-IP LTM in the DMZ to downloaded configuration files.

Credit Card Transactions

GIACE needs to ensure management of online transaction processing is secure and is in line with the requirements of credit card service providers. As an example, Visa card will be briefly discussed.

If Visa card is accepted, GIACE owns responsibility of providing tools and controls to verify a cardholder's identity and validity of a transaction. The website authorization related design should take into account Visa security recommendations.[22]

For real-time processing, Visa authorization requests need to be established from the merchant processor to VisaNet via the internet.[23] This means that the BIG-IP, Netscreen firewall and Cisco perimeter router will need to allow authorization requests to VisaNet via the internet from the GIACE web farm. Discussions with Visa would need to take place to determine the protocol(s) and port(s) to be used. However it is safe to assume that HTTPS or an equivalent encrypted protocol would be used.

[22] Visa Usability Findings and Recommendations, March 2004. http://usa.visa.com/download/business/accepting_visa/ops_risk_management/usability_recommendations.pdf?it=r4|/business/accepting_visa/ops_risk_management/vbv%2Ehtml|Usability%20Recommendations

[23] Visa e-Commerce Merchants' Guide to Risk Management http://usa.visa.com/download/business/accepting_visa/ops_risk_management/visa_risk_management_guide_ecommerce.pdf

Assignment 3: GIACE Firewall and Router Policies

Security Stance

All traffic from the Internet must pass through the GIACE perimeter router and then the directly connected Netscreen firewall. The perimeter router will use extended access lists to packet filter the majority of simple attacks. The filters should decrease the chance of successful attacks on and through the firewall. The firewall is a dedicated security device and uses stateful filtering and NIP features to prevent attacks.

Both devices are only effective if configured correctly. Both devices are configured to allow traffic to pass based on the concept of least privilege. Connections are only permitted if required. Required connections are locked down to only the necessary source and destination IPs, and only the necessary ports.

The configurations are reviewed regularly as a part of the GIACE Security Policy. When new requests to open access are made, an assessment of requirements is made to ensure no unnecessary connectivity is implemented. The type of connection is scrutinized to identify potential new vulnerabilities that may relate. In particular, connections initiating from the Internet are kept to a minimum.

Data Flow through the Firewall

The Netscreen firewall chokes traffic between three zones. By referring to the network diagram, the three zones can be clearly identified. The Untrust zone includes the perimeter router and all Internet hosts. The DMZ zone includes the GIACE IDS, proxy and web hosting devices and the BIG-IP Local Traffic Manager.

Data flows are tabulated below based on inter-zone communication. Juniper Netscreen firewalls can enforce allocation of each address to a specific zone. Firewall interfaces are created within zones. Policies are created between zones. Additionally, intra-zone blocking can be enabled and policies can be created between addresses in the same zone. Intra-zone blocking denies communication between devices in the same zone unless a policy specifically allows it. If an alternate path for communication other than the firewall exists, then firewall policies are irrelevant.

The ‘Trust’ zone comprises all networks that route traffic through the firewall’s ingress interface ‘ethernet1’ which is the first interface. The ‘DMZ’ zone comprises all networks that route traffic through the firewall’s ingress interface ‘ethernet2‘ and ‘ethernet4’ which are the second and fourth interfaces. The ‘Untrust’ zone comprises all networks that route traffic through the firewall’s ingress interface ‘ethernet3’ which is the third interface.

The internal networks 10.1.1.0/24 and 10.1.2.0/24 are separated at layer 3 by the Juniper Netscreen 50 firewall. The firewall trust interface uses virtual LANs (IEEE 802.1Q[24]) with the Cisco 2948G switch so that a single physical firewall interface can be configured on both networks. With intra-zone blocking enabled for the Trust zone, the two networks can not communicate unless policies allow. In this case no such policies exist, so the internal management network is separated from the internal user networks and remote access users. This is a deliberate security measure.

Data Flow - Internet to DMZ
(Head Office Netscreen zones Untrust to DMZ, and VPN Spoke to DMZ)

Source	Destination	Port(s) Protocol	Description
Customers	Web Server (Big-IP Virtual Server IP address)	TCP 80 HTTP	Allow customers to connect from Internet to corporate web server to transfer generally accessible data.
Customers	Web Server (Big-IP Virtual Server IP address)	TCP 443 HTTPS	Allow customers to connect from Internet to corporate web server to transfer confidential data.
Suppliers	Web Server (Big-IP Virtual Server IP address)	TCP 80 HTTP	Allow suppliers to connect from Internet to corporate web server to transfer generally accessible data.
Suppliers	Web Server (Big-IP Virtual Server IP address)	TCP 443 HTTPS	Allow suppliers to connect from Internet to corporate web server to transfer confidential data.
Partners	Web Server (Big-IP Virtual Server IP address)	TCP 80 HTTP	Allow partners to connect from Internet to corporate web server to transfer generally accessible data.
Partners	Web Server (Big-IP Virtual Server IP address)	TCP 443 HTTPS	Allow partners to connect from Internet to corporate web server to transfer confidential data.
General public	Web Server (Big-IP Virtual Server IP address)	TCP 80 HTTP	Allow general public to connect from Internet to corporate web server to transfer generally accessible data.
GIACE employees using remote access (Sales Force)	Mail Gateway (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 110 POP3	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to send and retrieve mail.

[24] http://www.ieee802.org/1/pages/802.1Q.html

GIACE employees using remote access (Sales Force)	Squid Proxy (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 8080	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows users to connect to Squid proxy for HTTP & HTTPS Internet browsing. Note that employees using remote access must connect to the Internet via the proxy. This increases latency, but enforces better security.
GIACE employees using remote access (Sales Force)	Web Server (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 80 HTTP	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to connect to the corporate web server.
GIACE employees using remote access (Sales Force)	Web Server (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 443 HTTPS	IPSEC VPN is used to connect from employee laptop to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows employees using remote access to connect to the corporate web server.
GIACE employees in regional satellite offices (RSOs)	Mail Gateway (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 110 POP3	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to send and retrieve mail.
GIACE employees in regional satellite offices (RSOs)	Squid Proxy (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 8080	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows users to connect to Squid proxy for HTTP & HTTPS Internet browsing. Note that employees in RSO sites must connect to the Internet via the proxy. This increases latency, but enforces better security.
GIACE employees in regional satellite offices (RSOs)	Web Server (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 80 HTTP	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to connect to the corporate web server.

GIACE employees in regional satellite offices (RSOs)	Web Server (Big-IP Virtual Server IP address)	IPSEC - UDP 500 IKE & IP 50 ESP to Head Office firewall then TCP 443 HTTPS	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. The head office Netscreen firewall has policies from the spoke zone, where the VPN is terminated, to the DMZ zone. This allows RSO employees to connect to the corporate web server.
ISP SMTP gateway	Squid proxy (SMTP gateway)	TCP 25 SMTP	Allow mail server to receive mail from Internet SMTP gateway.

Data Flow - DMZ to Internet

(Head Office Netscreen zones DMZ to Untrust)

Source	Destination	Port(s) Protocol	Description
Web server	VisaNet via Internet	TCP 443 HTTPS	Allow web server to send authorization requests to Visa for real time transaction processing.
Squid proxy (SMTP gateway)	ISP DNS servers	TCP 53 DNS	Allow proxy server to resolve addresses from Internet Domain Name Servers.
Squid proxy (SMTP gateway)	All legitimate Internet address space.	TCP 80 HTTP	Allow proxy server to communicate with Internet web servers.
Squid proxy (SMTP gateway)	All legitimate Internet address space.	TCP 443 HTTPS	Allow proxy server to communicate with Internet web servers.
Squid proxy (SMTP gateway)	ISP SMTP gateway	TCP 25 SMTP	Allow mail server to send mail to Internet SMTP gateway.

Data Flow - DMZ to Head Office Management Network

(Head Office Netscreen zones DMZ to Trust)

Source	Destination	Port(s) Protocol	Description
IDS	Log server	UDP 514 SYSLOG	Allow managed devices to send logs to log server.
Big-IP	Log server	UDP 514 SYSLOG	Allow managed devices to send logs to log server.
Squid proxy (SMTP gateway)	Log server	UDP 514 SYSLOG	Allow managed devices to send logs to log server.
Web server	Log server	UDP 514 SYSLOG	Allow managed devices to send logs to log server.
IDS	Log server (NTP server)	UDP 123 NTP	Allow time synchronization to internal NTP server.
Big-IP	Log server (NTP server)	UDP 123 NTP	Allow managed devices to send logs to log server.
Squid proxy (SMTP gateway)	Log server (NTP server)	UDP 123 NTP	Allow managed devices to send logs to log server.
Web server	Log server (NTP server)	UDP 123 NTP	Allow managed devices to send logs to log server.

Data Flow - Head Office User Network to DMZ

(Head Office Netscreen zones Trust to DMZ)

Source	Destination	Port(s) Protocol	Description
GIAC employees in Head Office	Mail Gateway (Big-IP Virtual Server IP address)	TCP 110 POP3	Allow users to send and retrieve mail.
GIAC employees in Head Office	Squid Proxy (Big-IP Virtual Server IP address)	TCP 8080	Allow users to connect to Squid proxy for HTTP & HTTPS Internet browsing.
GIAC employees in Head Office	Web Server (Big-IP Virtual Server IP address)	TCP 80 HTTP	Allow users to connect to corporate web server.
GIAC employees in Head Office	Web Server (Big-IP Virtual Server IP address)	TCP 443 HTTPS	Allow users to connect to corporate web server.
Internal database administrators in Head Office	Web Server (MySQL DB)	TCP 22 SSH	Allow DB administrators to connect to corporate web server which is the MySQL server. DB administrator workstations require DHCP static IP allocation.
Network security administrators in Head Office	Web Server (MySQL DB)	TCP 22 SSH	Allow network security administrators to connect from the management server for support purposes.
Network security administrators in Head Office	Big-IP management IP address	TCP 22 SSH	Allow network security administrators to connect from the management server for support purposes.
Network security administrators in Head Office	Big-IP management IP address	TCP 443 HTTPS	Allow network security administrators to connect from the management server for support purposes.
Network security administrators in Head Office	Squid Proxy (SMTP gateway)	TCP 22 SSH	Allow network security administrators to connect from the management server for support purposes.
Network security administrators in Head Office	IDS	TCP 22 SSH	Allow network security administrators to connect from the management server for support purposes.

Data Flow - Regional Satellite Offices to Head Office Internal Network
(Head Office Netscreen zones spoke to Trust)

Source	Destination	Port(s) Protocol	Description
GIACE employees in regional satellite offices (RSOs)	Head Office User Network	ANY	IPSEC VPN is used to connect from each RSO Netscreen 5GT firewall to the head office Netscreen 50 firewall via Internet. A policy allows access to the User Network. Note that NIPS checks are made on this connection.

Data Flow - Head Office Internal Network to Regional Satellite Offices
(Head Office Netscreen zones Trust to spoke)

Source	Destination	Port(s) Protocol	Description

Head Office User Network	GIACE employees in regional satellite offices (RSOs)	ANY	IPSEC VPN is used to connect from the head office Netscreen 50 firewall to each RSO Netscreen 5GT firewall via Internet. A policy allows access to the satellite office network. Note that NIPS checks are made on this connection.

Data Flow - Remote Access Users to Head Office Internal Network
(Head Office Netscreen zones Untrust to Trust)

Source	Destination	Port(s) Protocol	Description
Remote Access users	Head Office User Network	ANY	IPSEC VPN is used to connect from remote access laptops to the head office Netscreen 50 firewall via Internet. A policy allows access to the User Network. Note that NIPS checks are made on this connection.

Data Flow - Head Office Internal Network to Remote Access Users
(Head Office Netscreen zones Untrust to Trust)

Source	Destination	Port(s) Protocol	Description
Remote Access users	Head Office User Network	ANY	IPSEC VPN is used to connect from remote access laptops to the head office Netscreen 50 firewall via Internet. A policy allows access to the User Network. Note that NIPS checks are made on this connection.

Data Flow - Perimeter Router to Log Server
(Head Office Netscreen zones Untrust to Trust)

Source	Destination	Port(s) Protocol	Description
Perimeter Router	Log server	UDP 514 SYSLOG	Allow perimeter router to log to the Log Server.

Data Flow - Head Office User Network to Head Office Management Network
(Head Office Netscreen zones Trust to Trust - intra-zone blocking enabled)

Source	Destination	Port(s) Protocol	Description
ANY	Management network. 10.1.2.0/24	ANY	DENY all traffic to management network from other trust zone networks.

Data Flow - Default Deny Stance
(Head Office Netscreen zones Global to Global)

Source	Destination	Port(s) Protocol	Description
ANY	ANY	ANY	DENY and LOG all traffic not matching permitted data flows.

Policies between the global zone and global zone are by default executed last in the Netscreen rules. This is where the explicit deny and log all rule must exist.

Access Lists on Perimeter Router

Appendix A contains the full configuration of the perimeter router including annotated access lists.

Extended access lists have been implemented on the perimeter router. They allow high performance ingress and egress packet filtering. Reflexive access lists can be CPU and memory intensive. Reflexive access lists have not been implemented to ensure maximum performance. All ingress and egress traffic must also pass through the Netscreen firewall which has ASIC technology enabling high performance stateful inspection.

Traffic to private use (RFC 1918), multicast and reserved address spaces are blocked in both ingress & egress access lists. Address space allocations must be reviewed regularly[25] to update access lists in the future.

The egress access lists only permit traffic from legitimate GIACE source addresses. Most significantly, this restricts source IP spoofing from compromised GIAC hosts that may attempt to participate in DDOS attacks from GIACE to the Internet. The order of the access lists is important. They are processed top-down on a first-match basis.

Routing

All traffic from GIACE has source IP translated by the Netscreen firewall to an address on the same network segment as the LAN interface of the router. This simplifies routing on the perimeter router. The router only requires the automatically assigned routes for the two attached segments and a default route to the ISP next hop. No dynamic routing protocols are used. Therefore a range of attacks on BGP processing need not be mitigated by GIACE as they arise in the future.

Management Access

An access list has been implemented to filter access to manage the router. Only SSH from only a single NAT IP to the LAN interface is permitted. Only the GIACE management station has source IP translated to this NAT IP.

SNMP is not used to manage the perimeter router. Therefore a range of attacks on SNMP processing need not be mitigated by GIACE as they arise in the future.

Context Based Access Control

The perimeter router is not currently configured to block known viruses and worms. GIACE has considered the Cisco Firewall Feature Set for implementing Context Based

[25] Internet Protocol V4 Address Space. http://www.iana.org/assignments/ipv4-address-space

© SANS Institute 2000 - 2005 Author retains full rights.

Access Control (CBAC) on the perimeter device. However, using CBAC to filter all TCP and UDP packets for malicious viruses and worms is very CPU intensive. Although it is a good security measure, GIACE has decided at this stage that the performance overhead is undesirable. Defense in depth is further provided by the Snort IDS, Netscreen firewall, F5 Local Traffic Manager and host firewalls.

Appendix A. Perimeter Router Configuration Listing

This configuration was implemented on a Cisco 2500 running IOS 12.0. However, Cisco's most current recommendation should be used as a guideline for the IOS version loaded to the perimeter router. To load this configuration to different Cisco routers, minor changes, such as interface naming, may be required. Additionally, if using a high-end router enable Cisco Express Forwarding (CEF)[26] with command "ip cef". Most high-end Cisco routers support CEF to improve performance. CEF also offers some security benefits, such as RPF (Reverse Path Forwarding). RPF allows blocking packets that claim to originate from within an internal network, but present themselves on an external interface.

Public IP addresses have been sanitized in this configuration. To load this configuration, first replace the following addresses with real ISP allocated IP addresses:

a.b.c.?/24	Network IPs between GIACE perimeter router and GIACE firewall
p.q.r.?/30	Network IPs between GIACE perimeter router and ISP router

```
!--- Generate keepalive packets on idle (for incoming management connections).
service tcp-keepalives-in
!--- Include timestamp with the date and time on debug messages.
service timestamps debug datetime msec localtime show-timezone
!--- Include timestamp with the date and time on log messages.
service timestamps log datetime msec localtime show-timezone
!--- Apply password encryption to all passwords, including username, authentication key,
!--- privileged command, console and virtual terminal line access, and BGP neighbor passwords.
service password-encryption
!
!--- Set the router hostname.
hostname R1
!
!--- Change the buffer to limit the number of messages (lines) stored on the router to 5000.
logging buffered 5000 debugging
!--- An enable secret password uses MD5 to produce a one-way hash.
!--- Note that enable password uses a weak encryption algorithm and should not be used.
enable secret 5 $1$tzL0$FrfME1ZiY2XXZfKUUKpe1.
!
!--- Use Cisco proprietary encryption (7) for password.
!--- Unfortunately Cisco has no immediate plans to support a stronger encryption algorithm for
!--- Cisco IOS user passwords. Sanitise when sending configuration information in e-mail.
username ABarratt password 7 02070A4B0A0B1F726C
!--- Retrict use of the subnet zero adresses - not required for interface configuration.
no ip subnet-zero
!--- The IP header source route option allows the source IP host to set a packet's route through
!--- the IP network. This can be used as part of an attack strategy.
no ip source-route
!--- Disable finger. Unnecessary service that can be used to gather infomation.
no ip finger
!--- Allow negotiation of MTU size larger than 576 bytes (MSS 536 bytes).
!--- This is important for minimising fragmentation including VPN traffic.
ip tcp path-mtu-discovery
!--- Disable bootp. Unnecessary service that can be used as part of an attack strategy.
no ip bootp server
!--- Disables router using names in IOS commands.
no ip domain-lookup
!
!--- Set clock to local timezone. Will affect timestamps in logs.
clock timezone AEST 11
!
```

[26] Cisco Express Forwarding (CEF). http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm

```
!--- LAN interface settings. This interface faces the GIACE, with the firewall as the next hop.
interface Ethernet0
 description Internal facing subnet
!--- IP a.b.c.e applied to the interface which is on a /24 network.
 ip address a.b.c.e 255.255.255.0
!--- Access list 102 is applied to LAN interface to filter internet destined egress traffic.
 ip access-group 102 in
!--- Prevent resend of a packet through the same interface on which it was received.
 no ip redirects
!--- Smurf attacks send echo requests from a spoofed source address to a directed broadcast.
!--- This can cause all hosts to respond to an echo request, creating a lot of network traffic.
 no ip directed-broadcast
!--- No requirement for proxy ARP in this topology. Proxy arp can be used to spoof.
 no ip proxy-arp
!--- Cisco Discovery Protocol not required for this topology and should be disabled globally
!--- (and can also be disabled on each interface for best practise).
 no cdp enable
!
!--- The WAN interface faces the internet, with the ISP WAN router as the next hop.
interface Serial0
 no ip address
!--- IP directed broadcasts are unnecessary and can be used as part of an attack strategy.
 no ip directed-broadcast
!--- Frame relay is configured.
 encapsulation frame-relay IETF
!--- Multicast route caching is disabled.
 no ip mroute-cache
!--- Quality of Service (QOS) Distributed Weighted Fair Queuing DWFQ disabled.
 no fair-queue
!
interface Serial0.1 point-to-point
 description WAN link to ISP
!--- IP p.q.r.t applied to the interface which is on a /30 network.
 ip address p.q.r.t 255.255.255.252
!--- Access list 101 is applied to this interface to filter ingress traffic from the internet.
 ip access-group 101 in
!--- Prevent resend of a packet through the same interface on which it was received.
 no ip redirects
!--- Disable IP unreachable messages on WAN interface. IP unreachable messages can be used to map
!--- out the network topology.
 no ip unreachables
!--- Smurf attacks send echo requests from a spoofed source address to a directed broadcast.
!--- This can cause all hosts to respond to an echo request, creating a lot of network traffic.
 no ip directed-broadcast
!--- No requirement for proxy ARP in this topology. Proxy arp can be used to spoof.
 no ip proxy-arp
!--- Cisco Discovery Protocol not required for this topology and should be disabled globally
!--- (and can also be disabled on each interface for best practise).
 no cdp enable
!--- Associate this subinterface with a DLCI.
 frame-relay interface-dlci 16
!
!--- Ensure unused interface shutdown.
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
!--- Ensure unused interface shutdown.
interface Serial2
 no ip address
 no ip directed-broadcast
 shutdown
!
!--- Ensure unused interface shutdown.
interface Serial3
 no ip address
```

```
 no ip directed-broadcast
 shutdown
!
!--- Ensure unused interface shutdown.
interface BRI0
 no ip address
 shutdown
!
!--- Required for subnetting a block of IP address. The WAN interface is on a /30 network.
ip classless
!--- Default route to the ISP WAN router.
ip route 0.0.0.0 0.0.0.0 p.q.r.u
!
!--- Set log level to informational messages.
logging facility local6
!--- Set the syslog server.
logging a.b.c.i
!
!--- Create access list to be applied to virtual ttys to restrict management access to router.
!--- Permit SSH to the LAN interface - only if SSH supported on the hardware.
access-list 100 permit tcp host a.b.c.j host a.b.c.e eq 22
!--- Permit telnet to the LAN interface - only if SSH not supported on the hardware.
!--- For newer hardware models, telnet access should not be permited and only SSH should be
!--- used to manage the router over the network. SSH encrypts router passwords on the network.
access-list 100 permit tcp host a.b.c.j host a.b.c.e eq 23
!--- Deny and log all other network access to virtual ttys.
!--- This line must appear last in the access list.
access-list 100 deny   ip any any log
!
!--- Create access list to be applied to ingress traffic on the WAN interface.
!--- (Traffic from the internet.)
!---
!--- Refer to these sources for reserved and private addresses:
!---   http://www.ietf.org/rfc/rfc1918.txt
!---   http://www.iana.org/assignments/ipv4-address-space
!---   http://www.isi.edu/~bmanning/dsua.html
!---
!--- IANA reserved.
access-list 101 deny ip 0.0.0.0 0.255.255.255 any
access-list 101 deny ip 1.0.0.0 0.255.255.255 any
access-list 101 deny ip 2.0.0.0 0.255.255.255 any
access-list 101 deny ip 5.0.0.0 0.255.255.255 any
access-list 101 deny ip 7.0.0.0 0.255.255.255 any
!--- IANA private use. RFC 1918.
access-list 101 deny ip 10.0.0.0 0.255.255.255 any
!--- IANA reserved.
access-list 101 deny ip 23.0.0.0 0.255.255.255 any
access-list 101 deny ip 27.0.0.0 0.255.255.255 any
access-list 101 deny ip 31.0.0.0 0.255.255.255 any
access-list 101 deny ip 36.0.0.0 1.255.255.255 any
access-list 101 deny ip 39.0.0.0 0.255.255.255 any
access-list 101 deny ip 41.0.0.0 0.255.255.255 any
access-list 101 deny ip 42.0.0.0 0.255.255.255 any
access-list 101 deny ip 49.0.0.0 0.255.255.255 any
access-list 101 deny ip 50.0.0.0 0.255.255.255 any
!--- APNIC reserved.
access-list 101 deny ip 58.0.0.0 1.255.255.255 any
access-list 101 deny ip 60.0.0.0 0.255.255.255 any
!--- ARIN reserved.
access-list 101 deny ip 70.0.0.0 1.255.255.255 any
!--- ARIN reserved. IANA reserved.
access-list 101 deny ip 72.0.0.0 7.255.255.255 any
!--- RIPE reserved.
access-list 101 deny ip 83.0.0.0 0.255.255.255 any
access-list 101 deny ip 84.0.0.0 3.255.255.255 any
!--- RIPE reserved. IANA reserved.
access-list 101 deny ip 88.0.0.0 7.255.255.255 any
```

```
!--- RIPE reserved. IANA reserved. Various reserved.
access-list 101 deny ip 96.0.0.0 31.255.255.255 any
!--- Localhost class A. Note that although this range is also covered by the
!--- above line, it is important, so specified explicitly.
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
!--- End node auto-configuration when no DHCP server found.
access-list 101 deny ip 169.254.0.0 0.0.255.255 any
!--- IANA private use. RFC 1918.
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
!--- Test Net
access-list 101 deny ip 192.0.2.0 0.0.0.255 any
!--- IANA private use. RFC 1918.
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
!--- IANA reserved.
access-list 101 deny ip 197.0.0.0 0.255.255.255 any
!--- APNIC reserved.
access-list 101 deny ip 221.0.0.0 0.255.255.255 any
!--- IANA multicast.
access-list 101 deny ip 224.0.0.0 31.255.255.255 any
!--- IANA reserved. Unspecified class.
access-list 101 deny ip 240.0.0.0 15.255.255.255 any
!
!--- LAN network.
access-list 101 deny ip a.b.c.d 0.0.0.255 any
!--- WAN interface IP.
access-list 101 deny ip host p.q.r.t any
!--- WAN interface broadcast address.
access-list 101 deny ip host p.q.r.v any
!
!--- Permit ICMP type 3 code 4 messages to GIACE perimeter router WAN IP and GIACE firewall.
!--- This allows ICMP messges indicating fragmentation needed where no fragmentation bit set.
!--- This is particularly important as VPN traffic will pass through this router.
access-list 101 permit icmp any host p.q.r.t packet-too-big
access-list 101 permit icmp any host a.b.c.f packet-too-big
!--- Permit ICMP type 0 code 0 messages to GIACE perimeter router WAN IP and GIACE firewall.
!--- This allows ICMP messges echo replys to only GIACE perimeter router WAN IP and the
!--- GIACE firewall.
access-list 101 permit icmp any host p.q.r.t echo-reply
access-list 101 permit icmp any host a.b.c.f echo-reply
!--- Deny all other ICMP messages.
access-list 101 deny   icmp any any
!
!--- Deny access to unnecessary and troublesome service ports.
!--- NETBIOS
access-list 101 deny tcp any any range 137 139
access-list 101 deny udp any any range 137 139
!--- Microsoft-DS
access-list 101 deny tcp any any eq 445
!--- TFTP
access-list 101 deny tcp any any eq 69
!--- shell
access-list 101 deny tcp any any eq 514
!--- SNMP and SNMPTRAP
access-list 101 deny tcp any any range 161 162
access-list 101 deny udp any any eq 162
!
!--- Permit connection intiatiation to web server on http port and log.
access-list 101 permit tcp any host a.b.c.g eq 80 syn log
!--- Permit connection intiatiation to web server on https port and log.
access-list 101 permit tcp any host a.b.c.g eq 443 syn log
!--- Permit connection intiatiation to mail server on smtp port and log.
access-list 101 permit tcp any host a.b.c.i eq 25 syn log
!
!--- There is no requirement to permit UDP, other than DNS.
!--- Permit DNS udp to only the GIACE network visible to the internet.
access-list 101 permit udp any a.b.c.d 0.0.0.255 eq 53
!
```

```
!--- Finally, permit established tcp sessions to only the GIACE network visible to the internet.
!--- This permits return packets from internet for tcp sessions initiated from GIACE network.
access-list 101 permit tcp any a.b.c.d 0.0.0.255 established
!
!--- Create access list to filter egress traffic. To be applied to the LAN interface.
!--- (Traffic destined to the internet from the GIACE internal network.)
!--- The log-input switch is used in most matches as an additional measure to ensure
!--- no additional system is patched to the LAN interface network.
!
!--- Refer to these sources for reserved and private addresses:
!---   http://www.ietf.org/rfc/rfc1918.txt
!---   http://www.iana.org/assignments/ipv4-address-space
!---   http://www.isi.edu/~bmanning/dsua.html
!---
!--- IANA reserved.
access-list 102 deny ip any 0.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 1.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 2.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 5.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 7.0.0.0 0.255.255.255 log-input
!--- IANA private use. RFC 1918.
access-list 102 deny ip any 10.0.0.0 0.255.255.255 log-input
!--- IANA reserved.
access-list 102 deny ip any 23.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 27.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 31.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 36.0.0.0 1.255.255.255 log-input
access-list 102 deny ip any 39.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 41.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 42.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 49.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 50.0.0.0 0.255.255.255 log-input
!--- APNIC reserved.
access-list 102 deny ip any 58.0.0.0 1.255.255.255 log-input
access-list 102 deny ip any 60.0.0.0 0.255.255.255 log-input
!--- ARIN reserved.
access-list 102 deny ip any 70.0.0.0 1.255.255.255 log-input
!--- ARIN reserved. IANA reserved.
access-list 102 deny ip any 72.0.0.0 7.255.255.255 log-input
!--- RIPE reserved.
access-list 102 deny ip any 83.0.0.0 0.255.255.255 log-input
access-list 102 deny ip any 84.0.0.0 3.255.255.255 log-input
!--- RIPE reserved. IANA reserved.
access-list 102 deny ip any 88.0.0.0 7.255.255.255 log-input
!--- RIPE reserved. IANA reserved. Various reserved.
access-list 102 deny ip any 96.0.0.0 31.255.255.255 log-input
!--- Localhost class A. Note that although this range is also covered by the
!--- above line, it is important, so specified explicitly.
access-list 102 deny ip any 127.0.0.0 0.255.255.255 log-input
!--- End node auto-configuration when no DHCP server found.
access-list 102 deny ip any 169.254.0.0 0.0.255.255 log-input
!--- IANA private use. RFC 1918.
access-list 102 deny ip any 172.16.0.0 0.15.255.255 log-input
!--- Test Net
access-list 102 deny ip any 192.0.2.0 0.0.0.255 log-input
!--- IANA private use. RFC 1918.
access-list 102 deny ip any 192.168.0.0 0.0.255.255 log-input
!--- IANA reserved.
access-list 102 deny ip any 197.0.0.0 0.255.255.255 log-input
!--- APNIC reserved.
access-list 102 deny ip any 221.0.0.0 0.255.255.255 log-input
!--- IANA multicast.
access-list 102 deny ip any 224.0.0.0 31.255.255.255 log-input
!--- IANA reserved. Unspecified class.
access-list 102 deny ip any 240.0.0.0 15.255.255.255 log-input
!
!--- Permit ICMP type 8 code 0 messages to the internet from the GIACE firewall.
```

```
!--- This allows ICMP echo requests from only the GIACE firewall.
access-list 102 permit icmp host a.b.c.f any echo log-input
!--- Deny all other ICMP messages. This prevents many techniques used to map network topology.
access-list 102 deny   icmp any any log-input
!
!--- Deny access to unnecessary and troublesome service ports.
!--- NETBIOS
access-list 102 deny tcp any any range 137 139 log-input
access-list 102 deny udp any any range 137 139 log-input
!--- Microsoft-DS
access-list 102 deny tcp any any eq 445 log-input
!--- TFTP log-input
access-list 102 deny tcp any any eq 69 log-input
!--- shell
access-list 102 deny tcp any any eq 514 log-input
!--- SNMP and SNMPTRAP
access-list 102 deny tcp any any range 161 162 log-input
access-list 102 deny udp any any eq 162 log-input
!
!--- Finally, permit access from only the GIACE network adress space visible to the internet.
!--- This is the same network the router LAN interface is connected to.
access-list 102 permit ip a.b.c.d 0.0.0.255 any log-input
!
!
!--- Disable Cisco Discovery Protocol globally. Not required for this topology.
no cdp run
!--- Set banner with appropriate message. Wording is important if legal action is required.
banner login ^CCCCC
Authorised access ONLY

This system is the property of GIAC Enterprises

Disconnect IMMEDIATLEY if you are not an authorised user !

This login has been logged

Contact admin@GIAC.com for help

^C
!
!--- Console port.
line con 0
!--- Enable user identification on the console for configured local user(s).
 login local
!--- Prevent remote access to the console port via reverse-telnet.
 transport input none
!--- Auxiliary port.
line aux 0
!--- Virtual terminal lines.
line vty 0 4
 access-class 100 in
!--- Enable user identification on the virtual terminal lines for configured local user(s).
 login local
!--- Don't attempt to open telnet for unknown commands.
 transport preferred none
!--- Enable telnet service for virtual terminal lines - only if SSH not supported on hardware.
!--- For newer hardware models, telnet access should not be permited and only SSH should be
!--- used to manage the router over the network. SSH encrypts router passwords on the network.
 transport input telnet
!--- Disable nested transport from the router.
 transport output none
!

end
```

Appendix B. Firewall Configuration Listing

The GIACE head office Netscreen 50 firewall configuration is listed. Please refer to data flow tables to for comments. Public IP addresses have been sanitized in this configuration. To load this configuration, first replace the following addresses with real ISP allocated IP addresses:

a.b.c.?/24	Network IPs between GIACE perimeter router and GIACE firewall
p.q.r.?/30	Network IPs between GIACE perimeter router and ISP router

```
set clock ntp
set clock timezone 11
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set service "TCP8080" protocol tcp src-port 1-65535 dst-port 8080-8080
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "netscreen"
set admin password "nPb6O1rIGWDIcstC5sIFfTDtxkPqPn"
set admin scs password disable username netscreen
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone id 100 "spoke1"
set zone "Trust" block
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "spoke1" tcp-rst
set zone "Trust" screen alarm-without-drop
set zone "Trust" screen icmp-flood
set zone "Trust" screen udp-flood
set zone "Trust" screen winnuke
set zone "Trust" screen port-scan
set zone "Trust" screen ip-sweep
set zone "Trust" screen tear-drop
set zone "Trust" screen syn-flood
set zone "Trust" screen ip-spoofing
set zone "Trust" screen ping-death
set zone "Trust" screen ip-filter-src
set zone "Trust" screen land
set zone "Trust" screen syn-frag
set zone "Trust" screen tcp-no-flag
set zone "Trust" screen unknown-protocol
set zone "Trust" screen ip-bad-option
set zone "Trust" screen ip-record-route
set zone "Trust" screen ip-timestamp-opt
set zone "Trust" screen ip-security-opt
set zone "Trust" screen ip-loose-src-route
set zone "Trust" screen ip-strict-src-route
set zone "Trust" screen ip-stream-opt
set zone "Trust" screen icmp-fragment
set zone "Trust" screen icmp-large
set zone "Trust" screen syn-fin
```

```
set zone "Trust" screen fin-no-ack
set zone "Trust" screen limit-session source-ip-based
set zone "Trust" screen syn-ack-ack-proxy
set zone "Trust" screen block-frag
set zone "Trust" screen limit-session destination-ip-based
set zone "Trust" screen component-block zip
set zone "Trust" screen component-block jar
set zone "Trust" screen component-block exe
set zone "Trust" screen component-block activex
set zone "Untrust" screen alarm-without-drop
set zone "Untrust" screen icmp-flood
set zone "Untrust" screen udp-flood
set zone "Untrust" screen winnuke
set zone "Untrust" screen port-scan
set zone "Untrust" screen ip-sweep
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ip-spoofing
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "Untrust" screen syn-frag
set zone "Untrust" screen tcp-no-flag
set zone "Untrust" screen unknown-protocol
set zone "Untrust" screen ip-bad-option
set zone "Untrust" screen ip-record-route
set zone "Untrust" screen ip-timestamp-opt
set zone "Untrust" screen ip-security-opt
set zone "Untrust" screen ip-loose-src-route
set zone "Untrust" screen ip-strict-src-route
set zone "Untrust" screen ip-stream-opt
set zone "Untrust" screen icmp-fragment
set zone "Untrust" screen icmp-large
set zone "Untrust" screen syn-fin
set zone "Untrust" screen fin-no-ack
set zone "Untrust" screen limit-session source-ip-based
set zone "Untrust" screen syn-ack-ack-proxy
set zone "Untrust" screen block-frag
set zone "Untrust" screen limit-session destination-ip-based
set zone "Untrust" screen component-block zip
set zone "Untrust" screen component-block jar
set zone "Untrust" screen component-block exe
set zone "Untrust" screen component-block activex
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set zone "DMZ" screen alarm-without-drop
set zone "DMZ" screen icmp-flood
set zone "DMZ" screen udp-flood
set zone "DMZ" screen winnuke
set zone "DMZ" screen port-scan
set zone "DMZ" screen ip-sweep
set zone "DMZ" screen tear-drop
set zone "DMZ" screen syn-flood
set zone "DMZ" screen ip-spoofing
set zone "DMZ" screen ping-death
set zone "DMZ" screen ip-filter-src
set zone "DMZ" screen land
set zone "DMZ" screen syn-frag
set zone "DMZ" screen tcp-no-flag
set zone "DMZ" screen unknown-protocol
set zone "DMZ" screen ip-bad-option
set zone "DMZ" screen ip-record-route
set zone "DMZ" screen ip-timestamp-opt
set zone "DMZ" screen ip-security-opt
```

```
set zone "DMZ" screen ip-loose-src-route
set zone "DMZ" screen ip-strict-src-route
set zone "DMZ" screen ip-stream-opt
set zone "DMZ" screen icmp-fragment
set zone "DMZ" screen icmp-large
set zone "DMZ" screen syn-fin
set zone "DMZ" screen fin-no-ack
set zone "DMZ" screen limit-session source-ip-based
set zone "DMZ" screen syn-ack-ack-proxy
set zone "DMZ" screen block-frag
set zone "DMZ" screen limit-session destination-ip-based
set zone "DMZ" screen component-block zip
set zone "DMZ" screen component-block jar
set zone "DMZ" screen component-block exe
set zone "DMZ" screen component-block activex
set zone "spoke1" screen alarm-without-drop
set zone "spoke1" screen icmp-flood
set zone "spoke1" screen udp-flood
set zone "spoke1" screen winnuke
set zone "spoke1" screen port-scan
set zone "spoke1" screen ip-sweep
set zone "spoke1" screen tear-drop
set zone "spoke1" screen syn-flood
set zone "spoke1" screen ip-spoofing
set zone "spoke1" screen ping-death
set zone "spoke1" screen ip-filter-src
set zone "spoke1" screen land
set zone "spoke1" screen syn-frag
set zone "spoke1" screen tcp-no-flag
set zone "spoke1" screen unknown-protocol
set zone "spoke1" screen ip-bad-option
set zone "spoke1" screen ip-record-route
set zone "spoke1" screen ip-timestamp-opt
set zone "spoke1" screen ip-security-opt
set zone "spoke1" screen ip-loose-src-route
set zone "spoke1" screen ip-strict-src-route
set zone "spoke1" screen ip-stream-opt
set zone "spoke1" screen icmp-fragment
set zone "spoke1" screen icmp-large
set zone "spoke1" screen syn-fin
set zone "spoke1" screen fin-no-ack
set zone "spoke1" screen limit-session source-ip-based
set zone "spoke1" screen syn-ack-ack-proxy
set zone "spoke1" screen block-frag
set zone "spoke1" screen limit-session destination-ip-based
set zone "spoke1" screen component-block zip
set zone "spoke1" screen component-block jar
set zone "spoke1" screen component-block exe
set zone "spoke1" screen component-block activex
set interface "ethernet1" zone "Trust"
set interface "ethernet1.1" tag 5 zone "Trust"
set interface "ethernet1.2" tag 6 zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
set interface "ethernet4" zone "DMZ"
set interface "tunnel.1" zone "spoke1"
unset interface vlan1 ip
set interface ethernet1.1 ip 10.1.1.1/24
set interface ethernet1.1 route
set interface ethernet1.2 ip 10.1.2.1/24
set interface ethernet1.2 nat
set interface ethernet2 ip 10.1.192.0/24
set interface ethernet2 route
set interface ethernet3 ip a.b.c.f/24
set interface ethernet3 route
set interface ethernet4 ip 10.1.195.1/24
set interface ethernet4 route
```

```
set interface tunnel.1 ip 10.10.10.1/24
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1.1 ip manageable
set interface ethernet1.2 ip manageable
unset interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set interface ethernet4 ip manageable
unset interface ethernet1 manage telnet
unset interface ethernet1 manage snmp
unset interface ethernet1 manage web
unset interface ethernet2 manage ping
set interface "ethernet3" mip a.b.c.h host 10.1.2.10 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet3" mip a.b.c.i host 10.1.192.11 netmask 255.255.255.255 vrouter "trust-vr"
set interface "ethernet3" mip a.b.c.g host 10.1.192.12 netmask 255.255.255.255 vrouter "trust-vr"
set console page 0
set hostname ns50
set address "Trust" "Database admin workstation" 10.1.1.10 255.255.255.255
set address "Trust" "Head Office User Network" 10.1.1.0 255.255.255.0
set address "Trust" "log server" 10.1.2.10 255.255.255.255
set address "Trust" "management server" 10.1.2.11 255.255.255.255
set address "Untrust" "ISP DNS server" j.k.l.m 255.255.255.255
set address "Untrust" "ISP SMTP gateway" r.s.t.u 255.255.255.255
set address "Untrust" "Perimeter Router LAN Interface" a.b.c.e 255.255.255.255
set address "Untrust" "VisaNet authorization server" l.m.n.o 255.255.255.255
set address "DMZ" "F5 BIG-IP Local Traffic Manager" 10.1.192.10 255.255.255.255
set address "DMZ" "Snort IDS" 10.1.195.10 255.255.255.255
set address "DMZ" "Snort IDS - virtual IP" 10.1.192.13 255.255.255.255
set address "DMZ" "Web and DB server" 10.1.194.10 255.255.255.255
set address "DMZ" "Web and DB server - virtual IP" 10.1.192.12 255.255.255.255
set address "DMZ" "Web proxy and SMTP" 10.1.193.10 255.255.255.255
set address "DMZ" "Web proxy and SMTP - virtual ip" 10.1.192.11 255.255.255.255
set address "spoke1" "10.1.1.0/24" 10.1.1.0 255.255.255.0
set address "spoke1" "10.10.10.0/24" 10.10.10.0 255.255.255.0
set address "spoke1" "10.128.1.0/24" 10.128.1.0 255.255.255.0
set user "ab" uid 1
set user "ab" ike-id u-fqdn "ab@sec_frcookies.com" share-limit 1
set user "ab" type  auth ike xauth
set user "ab" remote ipaddr "10.1.100.1"
set user "ab" password "ubs"
set user "ab" "enable"
set user-group "roam_g" id 1
set user-group "roam_g" user "ab"
set ike gateway "p1_spoke" address a.b.c.f Main outgoing-interface "ethernet3" preshare
"uT3K/a3oNCX4hbs+GnCBYtQ0MQn5+BB6xw==" proposal "pre-g2-aes128-sha"
set ike gateway  "p1_spoke" nat-traversal
unset ike gateway "p1_spoke" nat-traversal udp-checksum
set ike gateway "p1_spoke" nat-traversal keepalive-frequency 5
set ike gateway "p1_roam" dialup "roam_g" Aggr outgoing-interface "ethernet3" preshare
"zQPJIxPvNQ9wAHsaAZCdBIggatn3eZwdVeCRUEppUGzWHhIyFJmm1RU=" proposal "pre-g2-des-sha"
unset ike gateway "p1_roam" nat-traversal udp-checksum
set ike gateway "p1_roam" nat-traversal keepalive-frequency 5
set ike gateway "p1_roam" xauth
set ike respond-bad-spi 1
set vpn "p2_spoke1" gateway "p1_spoke" no-replay tunnel idletime 0 proposal "g2-esp-aes128-sha"
set vpn "p2_spoke1" id 1 bind interface tunnel.1
set vpn "g2_roam" gateway "p1_roam" no-replay tunnel idletime 0 proposal "nopfs-esp-3des-sha"
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set policy id 9 from "Trust" to "DMZ"  "Head Office User Network" "Web proxy and SMTP - virtual
ip" "POP3" permit log
set policy id 2 from "Trust" to "spoke1"  "Head Office User Network" "10.128.1.0/24" "ANY" permit
log
set policy id 3 from "spoke1" to "Trust"  "10.128.1.0/24" "Head Office User Network" "ANY" permit
log
set policy id 4 from "Untrust" to "Trust"  "Dial-Up VPN" "Head Office User Network" "ANY" tunnel
vpn "g2_roam" id 5 pair-policy 5 log
```

```
set policy id 5 from "Trust" to "Untrust"  "Head Office User Network" "Dial-Up VPN" "ANY" tunnel
vpn "g2_roam" id 5 pair-policy 4 log
set policy id 6 from "Untrust" to "spoke1"  "Dial-Up VPN" "10.10.10.0/24" "ANY" tunnel vpn
"g2_roam" id 6 pair-policy 7 log
set policy id 7 from "spoke1" to "Untrust"  "10.10.10.0/24" "Dial-Up VPN" "ANY" tunnel vpn
"g2_roam" id 6 pair-policy 6 log
set policy global id 8 name "deny and log if no matches" from "Global" to "Global"  "Any" "Any"
"ANY" deny log
set policy id 10 from "Trust" to "DMZ"  "Head Office User Network" "Web proxy and SMTP - virtual
ip" "TCP8080" permit log
set policy id 11 from "Trust" to "DMZ"  "Head Office User Network" "Web and DB server - virtual
IP" "HTTP" permit log
set policy id 12 from "Trust" to "DMZ"  "Head Office User Network" "Web and DB server - virtual
IP" "HTTPS" permit log
set policy id 15 from "Trust" to "DMZ"  "Database admin workstation" "Web and DB server" "SSH"
permit log
set policy id 16 from "Trust" to "DMZ"  "management server" "Web and DB server" "SSH" permit log
set policy id 13 from "Trust" to "DMZ"  "management server" "F5 BIG-IP Local Traffic Manager"
"SSH" permit log
set policy id 14 from "Trust" to "DMZ"  "management server" "F5 BIG-IP Local Traffic Manager"
"HTTPS" permit log
set policy id 18 from "Trust" to "DMZ"  "management server" "Web proxy and SMTP" "SSH" permit log
set policy id 17 from "Trust" to "DMZ"  "management server" "Snort IDS" "SSH" permit log
set policy id 19 from "DMZ" to "Trust"  "Snort IDS" "log server" "SYSLOG" permit log
set policy id 20 from "DMZ" to "Trust"  "F5 BIG-IP Local Traffic Manager" "log server" "SYSLOG"
permit log
set policy id 21 from "DMZ" to "Trust"  "Web proxy and SMTP" "log server" "SYSLOG" permit log
set policy id 22 from "DMZ" to "Trust"  "Web and DB server" "log server" "SYSLOG" permit log
set policy id 23 from "DMZ" to "Trust"  "Snort IDS" "log server" "NTP" permit log
set policy id 24 from "DMZ" to "Trust"  "F5 BIG-IP Local Traffic Manager" "log server" "NTP"
permit log
set policy id 25 from "DMZ" to "Trust"  "Web proxy and SMTP" "log server" "NTP" permit log
set policy id 26 from "DMZ" to "Trust"  "Web and DB server" "log server" "NTP" permit log
set policy id 27 from "Untrust" to "Trust"  "Perimeter Router LAN Interface" "MIP(a.b.c.h)"
"SYSLOG" permit log
set policy id 28 name "Incoming access to web server." from "Untrust" to "DMZ"  "Any"
"MIP(a.b.c.g)" "HTTP" permit log
set policy id 29 name "Incoming access to web server." from "Untrust" to "DMZ"  "Any"
"MIP(a.b.c.g)" "HTTPS" permit log
set policy id 30 name "Incoming access to mail server." from "Untrust" to "DMZ"  "Any"
"MIP(a.b.c.i)" "MAIL" permit log
set policy id 31 from "DMZ" to "Untrust"  "Web and DB server" "VisaNet authorization server"
"HTTPS" nat src permit log
set policy id 32 from "DMZ" to "Untrust"  "Web and DB server" "ISP DNS server" "DNS" nat src
permit log
set policy id 33 from "DMZ" to "Untrust"  "Web proxy and SMTP" "Any" "HTTP" nat src permit log
set policy id 34 from "DMZ" to "Untrust"  "Web proxy and SMTP" "Any" "HTTPS" nat src permit log
set policy id 35 from "DMZ" to "Untrust"  "Web proxy and SMTP" "ISP SMTP gateway" "MAIL" nat src
permit log
set policy id 36 from "spoke1" to "DMZ"  "10.128.1.0/24" "Web proxy and SMTP - virtual ip" "POP3"
permit log
set policy id 37 from "spoke1" to "DMZ"  "10.128.1.0/24" "Web proxy and SMTP - virtual ip"
"TCP8080" permit log
set policy id 38 from "spoke1" to "DMZ"  "10.128.1.0/24" "Web and DB server - virtual IP" "HTTP"
permit log
set policy id 39 from "spoke1" to "DMZ"  "10.128.1.0/24" "Web and DB server - virtual IP" "HTTPS"
permit log
set vpn "p2_spoke1" proxy-id local-ip 10.10.10.0/24 remote-ip 10.128.1.0/24 "ANY"
set ssh version v2
set ssh enable
set scp enable
set config lock timeout 5
set ntp server "10.1.2.10"
set ntp server backup1 "0.0.0.0"
set ntp server backup2 "0.0.0.0"
set snmp port listen 161
set snmp port trap 162
```

```
set vrouter "untrust-vr"
set route 10.10.10.0/24 vrouter "trust-vr"
set route 10.1.1.0/24 vrouter "trust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route  10.128.1.0/24 interface tunnel.1
set route  10.1.100.0/24 interface ethernet3 gateway a.b.c.e
set route  0.0.0.0/0 interface ethernet3 gateway a.b.c.e
exit
```

Appendix C. Firewall HA Configuration Listing

GIACE has indicated that HA may be a future requirement. The configuration required for GIACE to run HA on Netscreen 50s follows. Monitoring of each of three zones is included. The primary and secondary firewalls in a pair must both be configured for HA. The ethernet4 interface must be in zone HA. This is default, so no configuration line can be seen for this. The HA configuration used on the primary firewall follows. Public IP addresses have been sanitized.

```
set nsrp cluster id 1
    -> Define unique cluster.
    -> Never define the same cluster id on another firewall pair sharing a network!
set nsrp rto-mirror sync
    -> Synchronize real time objects to ensure stateful failover (no connects drop).
set nsrp vsd-group id 0 priority 80
    -> Set lower priority on primary firewall.
set nsrp vsd-group id 0 preempt
    -> Attempt to become master after failover if failure condition no longer exists.
set nsrp vsd-group id 0 preempt hold-down 300
    -> Wait 300 seconds after failover before attempting to become the master.
set nsrp monitor interface ethernet1
set nsrp monitor interface ethernet2
set nsrp monitor interface ethernet3
    -> Monitor link status on all three non-HA interfaces.
set nsrp secondary-path ethernet1
    -> use trust interface as a secondary path for HA traffic
set nsrp track-ip ip
    -> enable monitoring via ping
set nsrp track-ip threshold 20
    -> failover if cumulative weight for ALL tests is 20 or higher
set nsrp track-ip ip 10.1.2.10 interface ethernet1
set nsrp track-ip ip 10.1.2.10 weight 11
set nsrp track-ip ip 10.1.2.11 interface ethernet1
set nsrp track-ip ip 10.1.2.11 weight 11
    -> If both the management server and log server do not respond to ping then failover.
set nsrp track-ip ip 10.1.192.10 interface ethernet2
set nsrp track-ip ip 10.1.192.10 weight 7
set nsrp track-ip ip 10.1.193.10 interface ethernet2
set nsrp track-ip ip 10.1.193.10 weight 7
set nsrp track-ip ip 10.1.194.10 interface ethernet2
set nsrp track-ip ip 10.1.194.10 weight 7
    -> If the Big-IP, the proxy server and the web server do not respond to ping then failover
    -> The actual IPs of the proxy server and the web server are used here, not the Big-IP
    virtual server IPs. This reduces the chance of a false positive failover.
set nsrp track-ip ip a.b.c.d interface ethernet2
set nsrp track-ip ip a.b.c.d weight 7
set nsrp track-ip ip a.b.c.e interface ethernet2
set nsrp track-ip ip a.b.c.f weight 7
set nsrp track-ip ip a.b.c.g interface ethernet2
set nsrp track-ip ip a.b.c.g weight 7
    -> If both filtering routers do not respond including the HSRP address, then failover.
```

The HA configuration used on the secondary firewall configuration is identical to the above with the following exceptions:

1. The priority is set to 100.
2. The preempt configuration is omitted.
3. The track-ip configuration is omitted to ensure when many tracked hosts do not respond both firewalls will not become inactive.

References

Autoconfigure Scripts for Proxy Settings. Craig Johnson Consulting. April 22, 2004
http://www.craigjconsulting.com/proxypac.html
http://www.craigjconsulting.com/setproxy.html

BIG-IP Local Traffic Manager
http://www.f5.com/f5products/v9intro/ltm/Datasheet_BIG-IPLTM.pdf

Cisco 3725 Multiservice Access Router
http://www.cisco.com/en/US/products/hw/routers/ps282/ps283/

Cisco Ethernet Switch Modules
http://www.cisco.com/en/US/products/hw/modules/ps2797/products_module_installation_guide_chapter09186a00800b168c.html#wp1022409

Cisco Express Forwarding (CEF).
http://www.cisco.com/warp/public/cc/pd/iosw/iore/tech/cef_wp.htm

Configuring the Catalyst Switched Port Analyzer (SPAN) Feature
http://www.cisco.com/warp/public/473/41.html

F5 Deployment Guide
http://www.f5.com/solutions/deployment/mirroring_to_inspection_device45.html

Fedora Project
http://fedora.redhat.com/about/rhel.html

From Intrusion Detection to Intrusion Prevention. Joanne Cummings. Network World. 23 September 2002.
http://www.nwfusion.com/buzz/2002/intruder.html

Gartner
http://www4.gartner.com/Init

The GNU Project
http://www.gnu.org/philosophy/free-sw.html
http://www.gnu.org/copyleft/gpl.html

IDS Evasion Techniques and Tactics. Kevin Timm. Security Focus. May 7, 2002.
http://www.securityfocus.com/infocus/1577

Internet Protocol V4 Address Space.
http://www.iana.org/assignments/ipv4-address-space

Intrusion Detection, Honeypots and Incident Handling Resources
http://www.honeypots.net/ids/links

Juniper Networks Intrusion Detection and Prevention
http://www.juniper.net/products/intrusion/

Juniper Networks Netscreen-25/50
http://www.juniper.net/products/integrated/dsheet/110003.pdf

Network Intrusion-Prevention Systems. IPS Tested on a Live Production Network. Network World, 02/16/04.
http://www.nwfusion.com/reviews/2004/0216ips.html

Network Intrusion Prevention Systems, the Next Big Thing? GIAC Certified Intrusion Analyst (GCIA) Practical Assignment. Peter Storm. November 15 2003.
http://www.giac.org/practical/GCIA/Pete_Storm_GCIA.pdf

Network Working Group. Request for Comments 1918. Address Allocation for Private Internets.
http://www.ietf.org/rfc/rfc1918.txt

The Postfix Home Page
http://www.postfix.org/

Proxy Caches
http://www.web-caching.com/proxy-caches.html

Roam International. Global Internet Roaming. IPassConnect.
http://www.roamintl.com/about.html

SANS IDS FAQ.
http://www.sans.org/resources/idfaq/what_is_id.php

SANS Webcast. July 28 2004. What Works in Intrusion Prevention. Los Alamos National Laboratory on Intrusion Prevention Systems: A Real World Case Study Featuring: Paul Criscuolo
https://www.sans.org/webcasts/show.php?webcastid=90514

SANS Webcast. December 9 2004. What Works in Intrusion Prevention Appliances. Featuring: Chris Aidan, Information Security Manager, Pearson Education
https://www.sans.org/webcasts/show.php?webcastid=90520

SANS Webcast. January 20 2005. What Works in Intrusion Prevention. Featuring: Donald Wray, Chief Information Security Officer for the US State of Indiana.
https://www.sans.org/webcasts/show.php?webcastid=90533

SANS Webcast. January 25 2005. What Works in HIPAA Compliance Using Intrusion Prevention. Featuring: Bonnie Norman, System Security Engineer - WellStar Health System.
https://www.sans.org/webcasts/show.php?webcastid=90538

Snort. The Open Source Network Intrusion Detection System.
www.snort.org/

Squid Support Services
http://www.squid-cache.org/Support/services.html

Visa Usability Findings and Recommendations, March 2004.
http://usa.visa.com/download/business/accepting_visa/ops_risk_management/usability_recommendations.pdf?it=r4|/business/accepting_visa/ops_risk_management/vbv%2Ehtml|Usability%20Recommendations

Visa e-Commerce Merchants' Guide to Risk Management
http://usa.visa.com/download/business/accepting_visa/ops_risk_management/visa_risk_management_guide_ecommerce.pdf

The Webalizer
http://www.mrunix.net/webalizer/