Global Information Assurance Certification Paper

Securing GIAC Enterprises' Network Perimeter

By Dana McLaughlin
GCFW Practical v4.0 – SANS@Home course
19 December 2004

Abstract/Summary:

Securing GIAC Enterprises' Network Perimeter discusses the company's technical defense-in-depth security architecture including its IP addressing scheme, use of default deny requirements, use of Citrix, use of firewalls and routers, and the tunneling of traffic from regional offices into the head office. The rule base for the PIX primary firewall is outlined. The merging of a warehouse / manufacturing facility using wireless into the company's existing network is also discussed.

Table of Contents

Assignment 1 – GIAC Enterprises, Warehouse Network Operations

GIAC Enterprises (G.E.)has expanded into the fortune cookie manufacturing business. To accommodate this expansion, G.E. has built a warehouse / manufacturing facility in San Francisco. This facility will control and house the fortune cookie manufacturing and shipping processes and will have 15 employees.

The warehouse operation will make the fortune cookies using the sayings the company produces. The fortune cookies sales will be in addition to the sales of the sayings. Production must support maintaining a specific amount of sayings in stock, support sayings in multiple languages, and support special orders of saying. It also must support the production of fortune cookies with sayings in the multiple languages and for special orders without slowing the direct sales sayings production. Due to the dual path with dependency production needs, integration between the sales, ordering, inventory, and shipping systems and accuracy of the inventory data will be very important to maintain appropriate production levels.

As warehouses can be nightmares for cabled electronic systems, wireless systems are becoming more common. The new applications and systems being installed at the warehouse take advantage of this medium. Wireless PDAs will be used on the shipping floor to interface with the shipping application while and wireless laptops on the manufacturing floor to control the manufacturing systems.

To achieve the goals of this expansion, work must be done to modify existing company resources and processes and to ready the new facility. Following are some of the large tasks that must be completed, divided between modification of the existing and readying the new. The tasks are not necessarily in the order that they would be accomplished.

Modifying existing applications, systems, and infrastructure:

Task 1. Add the needed features to the sales, ordering, and inventory applications and databases to support the fortune cookie products.

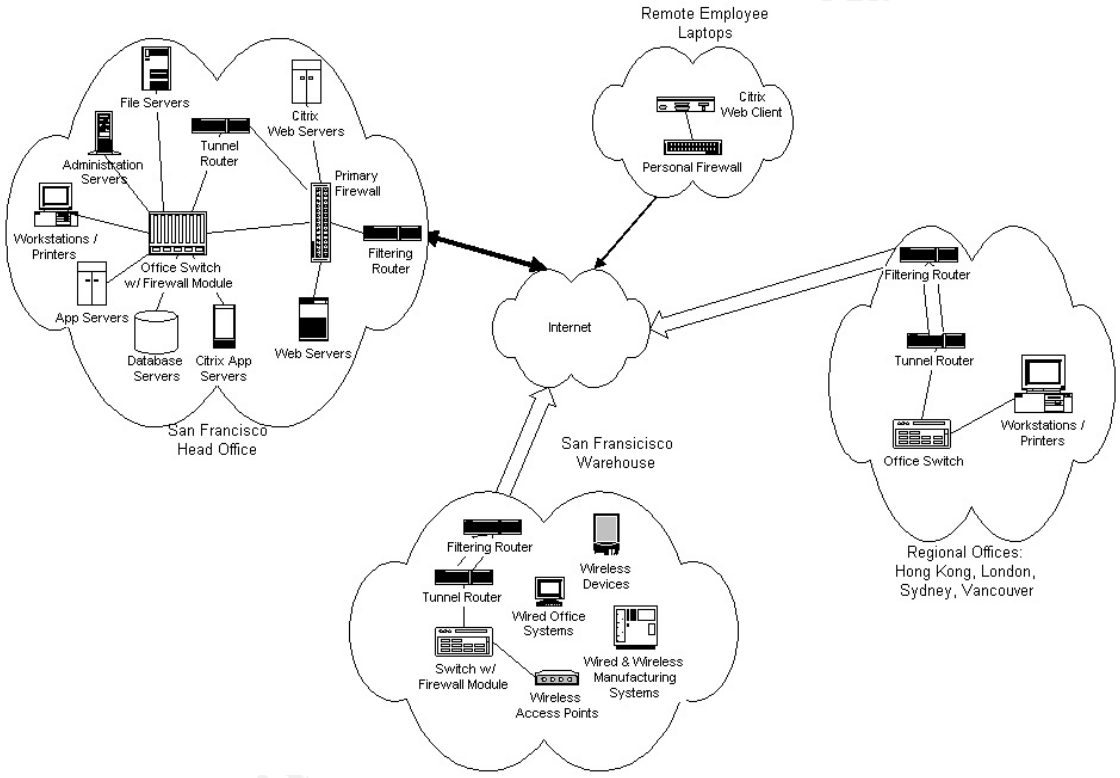
The addition of these features doesn't affect the services these applications use, so this doesn't affect the current network or perimeter and therefore will not be discussed in more detail in this document.

Task 2. Merge the current fortune cookie sayings shipping and manufacturing processes into a new combined sayings and cookie processes.

These process changes don't affect the current network or perimeter and thus will not be discussed in more detail in this document.

Task 3. Modify the network design to add the warehouse network requirements.

The new GIAC Enterprises network design with the warehouse included will be as follows:



As with the regional offices, a static encrypted IPSEC tunnel encapsulated in GRE connects the warehouse to the head office. All traffic leaving the warehouse network must pass though the tunnel before going anywhere else.

Addressing for the warehouse internal network will be consistent with the addresses assigned to the regional offices and will be as follows:

Warehouse	**Host Address Range**	**Address Mask**
Workstations / Printers	10.45.70.1-126	255.255.255.128
Manufacturing Systems	10.45.70.129-190	255.255.255.192
Shipping Systems	10.45.70.193-222	255.255.255.224

Tunnel Router to FWSM[1]	10.45.70.249-254	255.255.255.248

The external address range assigned to the warehouse will be consistent with those documented for GIAC Enterprises and will be as follows:

Warehouse	**Host Address Range**	**Address Mask**
Warehouse	159.145.28.1-2	255.255.255.252

Task 4. Reevaluate the security risks to the existing network.

The use of wireless operations at the warehouse in combination with the generally trusted tunneled communications with the head office, causes wireless to be a major security concern. Wireless networks flow outside of traditional network boundaries and their boundaries are invisible to the eye. They extend outside of a company's walls and can sometimes be connected to by a system that is miles away.

These networks are usually by default very open, allowing anyone who can 'hear' them to connect and use them just listen to all of the conversations passing in the clear. This is not acceptable for company that needs to maintain its data integrity, have high system availability, and maintain reasonable confidentiality of its information and that of its partners and customers.

Interference can be a problem with wireless networks. Using a microwave or a Bluetooth device can cause nearby wireless network devices to lose connection. Jamming devices also exist that someone could deliberately use against a wireless network.

Wireless use is a requirement for the chosen warehouse operations so a level of risk must be accepted. The risk can be greatly reduced to an acceptable level if:

a) the wireless network is controlled with access restricted to approved GIAC Enterprise systems only (allowed lists of mac addresses, all other denied)
b) a business-approved level of encryption applied to the communications (a level that is compatible with the systems being used)
c) the wireless system allowed access to other systems and networks on an as needed basis only
d) ensure the wireless devices have ad-hoc mode (peer-to-peer) disabled

Task 5. Integrate the warehouse network into the existing network, applying any new security measures to the existing network.

[1] Firewall Services Module

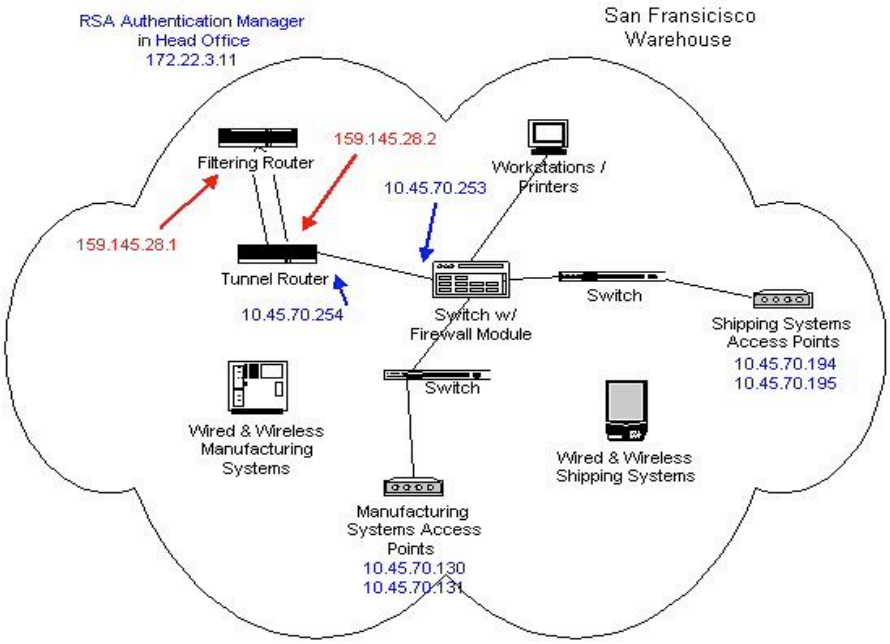
When the warehouse network is configured and ready for operation, the routing tables and access lists of the existing company network will be updated to include the new information and the tunnel activated. Servers that have implemented access filters will need to add the warehouse access, as required. Any scripts that examine traffic or parse logs for specific networks will need to be edited to include the new network. As determined in item 4, risks have increased for the existing network, but no additional security measures will be added to the existing network. Instead, extra security measures will be taken at the warehouse.

Task 6. Move the current fortune cookie sayings manufacturing and printing systems and processing to the new facility.

At the time of the move, the system addressing will need to be changed, firewalls changed to match the new addresses, and possibly some server, application, and database changes made. To limit problems, the move will need to be well coordinated and testing thorough.

Readying the warehouse facility for operation:

Task 1. Implementation of the warehouse network infrastructure and security measures.



The warehouse central switch is a Cisco Catalyst 6503[2] with a firewall services module[3] that is located in a secured closet in the office. A Cisco Catalyst 2950G 48 EI[4] switch is located in a secured closet on the manufacturing floor for those systems that require network connections (including the access points). A Cisco Catalyst 2950 24[5] switch is located in a secured closet on the shipping floor for those systems that require network connections (including the access points). The floor switches are connected to the warehouse's central switch. The switches' management addresses are part of the warehouse workstations and printers network segment, not hosts on the floor segments. Management of the switches is done by personnel at the head office.

The firewall services module on the 6503 acts as the router for the three main warehouse segments. It follows the same requirement as all other firewalls in the company – allow only that which is specifically required and deny all else. The firewall is an extra layer of defense put in place to shield the rest of GIAC Enterprises network resources from the warehouse's wireless operations.

Unlike the head office's external router, the router outside of the warehouse's firewall is a tunnel router configured like those in the regional offices. The filtering router outside of that also follows the regional office configuration pattern. Management of the firewall and routers is done by personnel at the head office.

Two Cisco Aironet 1200 access points[6] are used on each the shipping and manufacturing floors. They are configured using WLAN 802.11b, 128 bit WEP encryption, and 802.1x authentication, and to restrict MAC address connections to just those specifically allowed. The existing RSA Authentication Manager located in the head office will act as the Radius server for the 802.1x authentication when the link is activated. The shipping access points only allow connection from the MAC addresses of the shipping PDAs while the manufacturing access points only allow connection from MAC addresses of the manufacturing laptops. As with the firewall, routers, and switches, the access points are managed by personnel in the head office.

---

[2] Cisco 6503 introduction: http://www.cisco.com/en/US/products/hw/switches/ps708/index.html
[3] Cisco firewall services module introduction: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html
[4] Catalyst 2950G introduction: http://www.cisco.com/en/US/products/hw/switches/ps628/ps3821/index.html
[5] Catalyst 2950 24 introduction: http://www.cisco.com/en/US/products/hw/switches/ps628/ps627/index.html
[6] Cisco Aironet 1200 data sheet: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html

The shipping system uses specially programmed HP iPAQ Pocket PCs (series h4350)[7] that use WLAN 802.11b, 128 bit WEP, and 802.1x[8]. Their Bluetooth and infrared features are disabled. The manufacturing system uses specially programmed Compaq laptops with Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapters also using WLAN 802.11b, 128 bit WEP, and 802.1x[9]. The onboard infrared and ethernet ports are disabled.

The building's exterior walls are fairly thick and made of cement with steel reinforcement and a brick façade. The manufacturing floor has no large doors to the outside and no windows. It has two large doors to the shipping floor. The shipping floor has two large doors (which are expected to be frequently open) to loading ramps but no windows. The warehouse office has decoratively barred windows at the front but no large doors.

Wireless scanning and testing inside and outside the warehouse showed the following.

- The manufacturing floor network was detectable when from outside the space when a door was open. If a door to the shipping room and the shipping room had a loading door open, the network was detectable outside on the shipping side of the building but connection became very spotty from across the street from shipping. The doors to shipping will be open intermittently each day but only when needed.
- On the manufacturing floor a few dead spots did exist but they were not where the laptops would be used.
- The shipping floor was detectable in the some of the offices across the street when its doors were open.
- No dead spots were found on the shipping floor.
- Both networks were detectable from the office near the doors onto the floors. Outside of the office, a network was only detectable if the door to its floor was open.
- The access points denied access from an unauthorized MAC address.
- The communication streams were encrypted.

From the results of the scans and tests, GIAC Enterprises determined that the access point locations and antenna outputs were suitable. They also determined that the planned wireless systems security configuration was appropriate.

---

[7] HP iPAQ Pocket PC h4350 (FA172A) Specifications: http://h10010.www1.hp.com/wwpc/us/en/sm/WF06a/215348-64929-215381-314903-f62-349051.html

[8] HP iPAQ Pocket PC h4100 and h4300 series – Frequently asked questions [WLAN] http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/en/sm/pocketpc/faq_h4300.html - wlan

[9] Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter data sheet: http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a00801ebc29.html

Task 2. Installation and testing of the fortune cookie manufacturing systems.

Networking and perimeter changes may need to be made to meet the requirements of these systems. Careful coordination of this task is necessary to facilitate good communications and cooperative troubleshooting.

Task 3. Installation and testing of the new shipping system.

Like task 2 above, networking and perimeter changes may need to be made to meet the requirements of these systems. Careful coordination of this task is necessary to facilitate good communications and cooperative troubleshooting.

Task 4. Purchase and configuration of office systems.

The workstations and printers must follow the same configuration requirements as those in the rest of the company. Applications are still managed centrally by the head office using Citrix. Exceptions to the requirements must be approved by the head office.

Assignment 2 – GIAC Enterprises, Perimeter Security Architecture

GIAC Enterprises Company and Operation Brief:

GIAC Enterprises (G.E.) markets fortune cookies sayings to customers around the globe. It supports this effort with 50 employees located primarily in or near the head office in San Francisco, and in or near the four regional offices - London, Sydney, Hong Kong, and Vancouver. The sales force employees primarily operate remotely from the offices.

In order to maintain a limited number of technical support staff, all company servers are located in the head office. G.E. has also chosen to have employees use Citrix web clients to access company systems and applications, thus limiting the cost of expensive desktops and workstation management issues. Static encrypted tunnels are used to link the regional offices to the head office with configurations forcing all traffic from these offices to pass through the head office before connecting to resources outside of the company. Outside sales employees access systems and applications in the head office via the Internet using ssl Citrix web clients.

GIAC Enterprises relies heavily on Internet services to support its customer and supplier base. G.E. supports different communications models for these different entities.

- Customers purchase bulk online fortunes directly from G.E. via G.E.'s online store. This process uses ssl communications with self-managed account information and passwords.
- A select group of Suppliers sell fortune cookie sayings (in English) to G.E. These suppliers transfer the sayings directly into individual repositories on G.E.'s ftp server using ssh[10]. Specific Translators sell their translated sayings to G.E. These translators use the same general process as the Suppliers for the transfer.
- A select set of international companies partner with G.E. to translate the fortunes. These Translation partners download G.E.'s English version sayings in bulk from a read only copy of G.E.'s complete repository available to their accounts on a web server using ssl. Translators can then sell the translated sayings.
- General information about G.E. is available to the public via the company's Internet web site using http.

[10] Ssh definition: http://en.wikipedia.org/wiki/Ssh

Defense in Depth Security Model:

The Internet is an extremely useful medium for business and consumers but it is also fraught with dangers. As noted in the September 2004 Symantec Internet Security Threat Report, covering the first six months of 2004 and summarized in their September 20 press release[11], monetary attacks are on the rise. Attacks against e-commerce have risen 400% from the previous six months. The report also noted that web applications were becoming popular relatively easy to exploit targets, that usually allow an attacker to bypass traditional perimeter controls. Along with that, the time between a vulnerability announcement and the release of exploit code has been decreasing, with the average time now being only 5.8 days according to the report. These worrying statistics, among many others, demonstrate a need for many layers of security in an organization so that if one layer of security is breached, another will hopefully stop, slow down, or at a minimum record an attack. This layered model provides defense in depth security.

GIAC Enterprises (G.E.) has implemented a Defense in Depth model. This

model includes its people, technology and operations as generally illustrated in the diagram[12] from and described in the Defense in Depth document published by the National Security Agency. This paper on the architecture of GIAC Enterprises security discusses the main technology items in G.E.'s implementation.

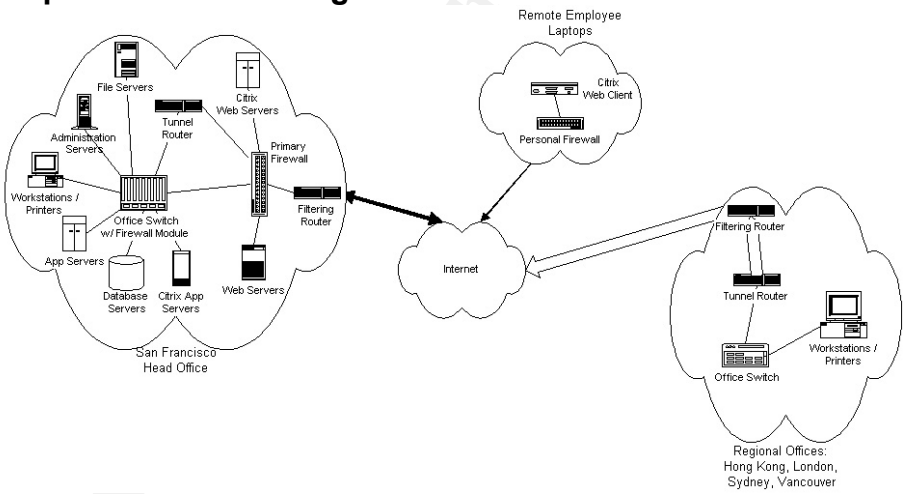
[11] Symantec Internet Security Threat Report Identifies More Attacks Now Targeting E-Commerce, Web Applications http://biz.yahoo.com/bw/040920/195026_1.html
[12] Defense in Depth http://nsa2.www.conxion.com/support/guides/sd-1.pdf, also available at http://www.nsa.gov/snac/support/defenseindepth.pdf

Default Deny:
GIAC Enterprises' security policy requires that the company take a default deny stance with its networks and systems, i.e. deny all that isn't explicitly allowed. This stance keeps the company's vulnerability exposure as low as possible.

The policy requires that firewalls and routers apply this rule to both ingress[13] and egress[14] traffic controlled by each firewall and router. Firewalls must limit access to the lowest possible denominator that requires the access. For instance, if all workstations on a segment require access, allow only the workstations access while denying printers from the same segment. In the case of the routers, the default deny stance may be modified in how strict the rules are, depending on the function of the router. Filtering routers that act like firewalls should have more strict rules than routers that are running internal company segments.

The default deny requirement for servers means that they must only run those services that are necessary for the business. This also means that when services and applications allow (and it makes sense for the operation of them) access must be restricted to just those entities that are required.

GIAC Enterprises Network Diagram:



IP Addressing Scheme:
GIAC Enterprises uses an assortment of private IP addresses[15] internally. Due to the vast range of private addresses, use of these addresses allows the company to configure the internal network without any of the limitations, restrictions, or costs associated with assigned routable addresses. These

[13] Ingress definition http://www.webopedia.com/TERM/I/ingress_traffic.html
[14] Egress definition http://www.webopedia.com/TERM/E/egress_traffic.html
[15] RFC 1918 (rfc1918) – Address Allocation for Private Internets http://www.faqs.org/rfcs/rfc1918.html

addresses should also be blocked by responsible entities from routing on the Internet, thus limiting direct Internet exposure.

Address assignment is done through dhcp reservations, i.e. statically assigned by mac[16] address, with a very few exceptions where this isn't possible. This allows for easier recognition of systems that shouldn't be on the network or that are misconfigured. Static assignment also allows for easier tracking of specific system activity over time.

Segmentation is used to maximize traffic flow control locations between segments with different system functions. This allows for more opportunity to limit traffic between segments to that which is needed for the business and therefore limit avenues of attack or vulnerability. Segment addressing is spread out among different address ranges for ease of recognition internally which aides troubleshooting, auditing, and log monitoring activities. Addressing in this manner also makes it more difficult for an unauthorized internal scan to map out the network without being recorded by any active logging or monitoring systems.

The regional office internal addresses will all begin with the 10.45 octets and are as follows:

Office	Host Address Range	Address Mask
London workstations / printers	10.45.30.1-62	255.255.255.192[17]
Vancouver workstations / printers	10.45.40.1-62	255.255.255.192
Hong Kong workstations / printers	10.45.50.1-62	255.255.255.192
Sydney workstations / printers	10.45.60.1-62	255.255.255.192

The head office has several segments with internal addressing assignments as follow below. As the tunnel router controls the 10.45 network for routing purposes, the segment between it and the perimeter firewall is also in the 10.45 range. The segments that are screened off from the rest by the perimeter, the Citrix web servers and web servers segments, are addressed using the 172.19 address range to be much more obvious to security and system administrators when they are looking at logs and the like involving activity with these systems. This change also allows for some obfuscation of the internal addressing scheme. The file server, administration server, and database server segments, along with

[16] MAC Address definition, http://en.wikipedia.org/wiki/MAC_address
[17] Subnet Masking and Addressing http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42ape.htm

the test and development segment, are in the 172.22 address range controlled by an internal firewall in the switch. All other head office segments are in the 192.168 address range.

Head Office Segment	Host Address Range	Address Mask
Tunnel Router to Perimeter (offices)	10.45.1.1-6	255.255.255.248
Citrix Web Servers (citrix)	172.19.3.1-14	255.255.255.240
Web Servers (webservices)	172.19.4.1-14	255.255.255.240
Expansion (disabled)	172.19.5.1-2	255.255.255.252
Administration Servers	172.22.3.1-14	255.255.255.240
File Servers	172.22.4.1-14	255.255.255.240
Database Servers	172.22.5.1-14	255.255.255.240
Test / Development	172.22.249.1-14	255.255.255.240
Switch to Perimeter	192.168.1.1-6	255.255.255.248
Core to Tunnel Router	192.168.2.1-6	255.255.255.248
Workstations / Printers	192.168.20.1-126	255.255.255.128
Citrix Servers	192.168.101.1-30	255.255.255.224

Note: As the regional offices have very few systems, GIAC Enterprises determined that segmentation of these offices into a workstation segment and a printer segment was too cumbersome. Printers and routers from the segments shouldn't be allowed the same access to systems or the Internet that the workstations need. To solve that issue, it was decided that all (including the head office) workstation / printer segments would be assigned addresses in a manner that allow access lists and translations to affect the workstations. Example: At the head office, the workstations (not printers) must be addressed between 192.168.20.65-126 (the upper half of the configured segment address range), which corresponds the subnet mask 255.255.255.192.

Caveat: Segment addressing patterns can be determined by interpreting scan results, sniffed information, logs, picking through paper that was improperly thrown into the trash, etc. Use of private addresses and segmentation cannot be used alone as security, instead it is just one portion of a Defense-in-Depth security architecture. Also, care must be taken to not over segment the network, as that can cause throughput degradation as well as cause management of the network to be too cumbersome.

External addressing is as follows:

Note: As GIAC Enterprises is in negotiations with a new ISP, external addresses represented in this document are listed using the 159.145 class B range that is

now assigned to the State of California[18]. These addresses must be replaced with the static addresses assigned by the new ISP once the new contract is in place.

Office	Host Address Range	Address Mask
Head Office	159.145.18.1-254	255.255.255.0
London	159.145.38.1-2	255.255.255.252
Vancouver	159.145.48.1-2	255.255.255.252
Hong Kong	159.145.58.1-2	255.255.255.252
Sydney	159.145.68.1-2	255.255.255.252

Restricted Internet Presence for Company Offices:
No resource is unlimited, especially when it applies to skilled personnel and their ability to effectively manage and monitor many systems across a distance. GIAC Enterprises has determined that the best use of its technical resources is through centralization. Servers, technical personnel, and monitoring systems are located in the Head Office in San Francisco. This centralization extends to the management of the company's Internet presence. GIAC Enterprises has only one gateway for internal to external traffic flow. The systems in the regional offices are tunneled in to the Head Office, and must pass out through that office's perimeter firewall to reach sites on the Internet.

AES IPSec tunnels encapsulated in GRE join the tunnel router in each regional office (Cisco 2611XM Multiservice Router[19] running IOS release 12.3(8)T) with the tunnel router (a Cisco 3825 Integrated Services Router[20] also running 12.3(8)T) in the head office, essentially establishing virtual private networks (vpns) that extend GIAC Enterprises' internal network to all offices. Only the tunnel traffic is allowed through the regional filtering routers. No other traffic from the office is allowed out. This allows the head office perimeter firewall to control all of G.E.'s Internet traffic.

Caveat: Encryption and tunneling can be expensive to bandwidth. As each of the regional offices are using connections of at least T1 speeds to the Internet, with the head office maintaining a 100Mb line, and the use of Citrix's web client for all application access, the cost to the bandwidth is acceptable. With these VPNs coming in to the main office and terminating behind the perimeter firewall, a risk exists that an attacker (person, system, or application) could access the head office network from a compromised regional office. G.E. has placed a network IDS between the head office tunnel router and the central switch to monitor for

[18] Revealed through a WHOIS search on www.arin.net.
[19] Cisco 2911XM introduction: http://www.cisco.com/en/US/products/hw/routers/ps259/ps4830/index.html
[20] Cisco 3825 introduction: http://www.cisco.com/en/US/products/ps5857/index.html

and report on non-Citrix traffic. An internal firewall is also used at the head office to shield the most sensitive servers (database, file, and test/development) from unauthorized direct connection.

Routers:
Several routers are in place throughout GIAC Enterprises' network. They serve as routers, filters, or simple firewalls depending on their placement and configuration. Each externally accessible (Internet facing) router interface, that is capable of being configured in this manner, is configured to administratively drop packets that are disallowed using the 'no ip unreachables' command.

Filtering routers are placed in front of the head office perimeter firewall, in front of each of the regional office's tunnel router (a Cisco 2611XM). These routers act as shields for the system / network that is directly behind it.

The filtering router at the head office is in front of a firewall. As the firewall is configured to take a close look at the traffic that comes to it, the filtering router is set to inspect at a more general level. It allows most traffic to pass by but blocks invalid source address traffic – i.e. traffic addressed with private source addresses or special use addresses[21] and spoofed GIAC Enterprises addresses (sources coming from the 159.145.18 range). Management access of the router is only allowed from specific head office addresses.

The filtering routers in the regional offices act more like firewalls for those locations. They block all but the company's tunnel traffic and traffic from the filtering router itself. Management access of the routers is only allowed from specific head office addresses.

All company internal routers do some filtering for the segments they control. They only allow traffic from source addresses that belong on the segment to pass through the router. This policy set blocks systems that are spoofing the source address and mis-addressed / misconfigured systems for exiting the segment.

Company policy requires that those employees who connect to the office from a home office using a high-speed link use a router that supports NAT (network address translation).

Note: GIAC Enterprises has chosen the 2611XM and 3825 routers because they have the throughput and current features required for company operations. The routers also allow the company to possibly expand its networking services to newer technology such as Voice over IP. As the company owns several 2611XMs, in order to keep maintenance costs down, the company maintains a

[21] RFC 3330 – Special-Use IPv4 Addresses, http://www.faqs.org/rfcs/rfc3330.html

spare 2611XM at the head office for emergency purposes. If necessary, it can be preconfigured and sent by FedEx to a regional office.

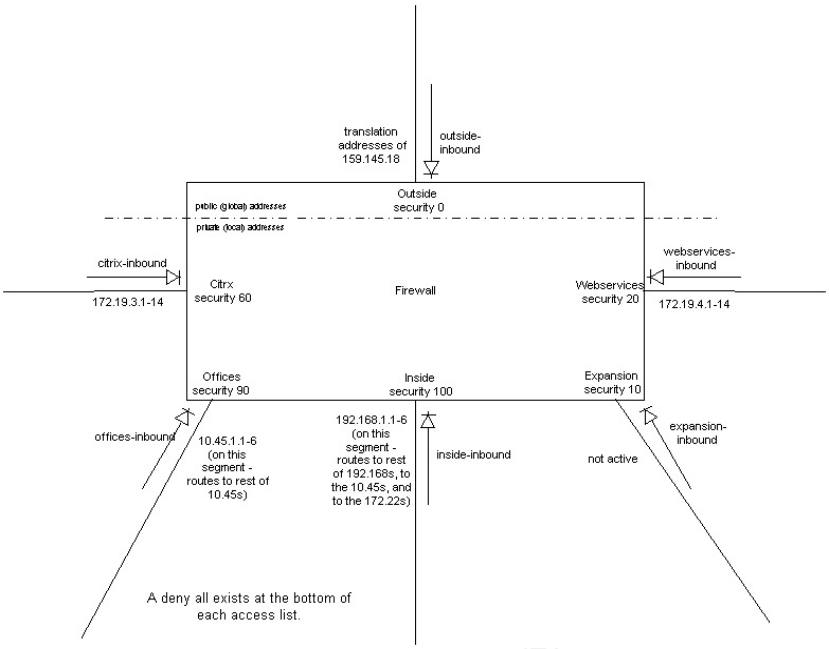
Caveat: Routers can act as filters but too much filtering can slow their operation down dramatically. If a lot of filtering is required, a firewall should be purchased.

Head Office Perimeter Firewall:
The primary firewall for GIAC Enterprises is located at the Head Office. This firewall follows the default deny policy in only allowing ingress and egress traffic to pass that is specifically allowed.

The firewall chosen by G.E. is a Cisco Pix 515E Security Appliance with an unrestricted software license (PIX-515E-UR)[22] with an added interface (PIX-4FE) to have the maximum number of interfaces (6). Also installed is a matching failover unit (PIX-515E-FO) for redundancy. Having a 'backup' firewall allows G.E. to pay for a lower cost maintenance, SMARTnet 8x5xNBD[23] with little worry about downtime. They are both running Pix version 6.3 software. This firewall met the company's need of multiple interfaces, and good speed, and was relatively inexpensive.

The Pix is a stateful inspection firewall with a few add-ons. Its primary purpose is to track of session state. Its rules can be specific down to the source and destination port combinations but it does not allow for application layer rules. A few application 'fixups[24]' are available to handle unusual operating protocols (such as ftp) without having to create very complicated rule sets around them. These 'fixups' are able to be activated or deactivated but not otherwise configured. They do not act like application firewalls for those protocols. It also has a few built-in IDS signatures but which are active in each specific OS version varies and isn't well documented. This device should only be considered a firewall, not an IDS.

[22] Cisco PIX 515E Security Appliance Data Sheet:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html
[23] 8x5xNBD: eight hours a day, 5 days a week, service / repair / replacement parts delivered the next day, see Table 1 on
http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_datasheet09186a008009249 1.html
[24] Application Inspection (Fixup):
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278b.html



The PIX firewall requires its interfaces to be assigned security levels. The higher the security level (number), the more trusted the interface is. A higher level (more trusted) interface is allowed by default to establish a connection to a lower level interface but not vise versa. The diagram above shows the security levels applied to the perimeter firewall's interfaces.

As GIAC Enterprises requires a default deny policy, this pattern of higher security can automatically connect to lower is unacceptable – thus access lists are activated on the inbound side of all interfaces to interrupt that process. These access lists allow specific activity to pass through them and then deny all.

Caveat: The Pix cannot stop or detect an application layer attack (such as a sql injection attack). Due to current company budget constraints and ongoing changes in the web applications, the security officer's request for reverse proxy to place in from of the Internet accessible servers has been put on hold. Instead, the Windows servers that could be have been upgraded to Windows Server 2003, URLScan is enabled, monitored, and maintained. Activity logs are closely monitored and patches are applied to all applicable systems and applications as soon as possible. SNORT listeners have also been activated on the citrix and webservices segments.

Network-based IDS:
Funds for security are not endless. In order for GIAC Enterprises to stretch its budget, it reviewed areas where open source and very low cost products could be used in the security architecture. SNORT v 2.1 was chosen due to its

reputation and the fact that the company has technical and security personnel experienced with Linux and the application.

The choice made by the company was not to expect immediate notification of an intrusion as it just doesn't have the staff to manage such a requirement. Instead G.E. uses SNORT to log possible intrusions with the staff can then review daily (or if an issue has come to light).

SNORT is deployed with silent listeners (sniffing interfaces) at the head office perimeter firewall interface for the Citrix web servers, the web servers interface, and at the inside interface. There is also one listening at the tunnel router interface between it and the head office switch. Intermittently a mobile system with SNORT installed is placed to monitor the outside interface of the firewall for testing and auditing purposes.

Each system running a silent listener has an active NIC connected to the head office's administration server segment. The day's binary data is sent to the central log server each night.

Caveat: This installation is very low priced technology-wise but high priced in administrative costs. Should the staff familiar with SNORT leave the company or become too busy with other duties, this solution may no longer be viable.

Central Application Delivery / Citrix:
The company uses Citrix for central application delivery using Citrix's web client. From a business point of view, use of Citrix allows the company to extend the use of existing workstations and laptops by offloading the processing and application management to the Citrix application servers. Due to the functionality of Citrix, the applications run locally on the Citrix application servers with screen updates sent to the client. In this manner, employees with older / slower workstations and those across slow links notice little if any delay in keyboard and mouse operations.

As access to GIAC Enterprises' Citrix infrastructure is controlled using the Citrix's Secure Gateway, which creates in essence an ssl vpn[25] through which the employee is able to run all of their applications, this operational model becomes part of the security architecture. Having the applications running on central servers means that there are less reasons for employees to have administrative level access to workstations. It also facilitates the use of thin client workstations. Restricting access to user level only reduces the possibility of having employees install unauthorized or incompatible software running on the workstations. It also greatly reduces the possibility of malware being able to infect the system.

[25] What is Citrix's SSL VPN Strategy?: http://www.brianmadden.com/content/content.asp?id=214

Running a minimum number of services on the workstations limits their possible number of vulnerabilities.

Caveat 1: The use of central applications almost always has exceptions to the rule. Some system, application, or job function will require use of a specialized workstation. Exceptions should be tracked and the user of such a system know what system use is and isn't allowed. This means a good acceptable use policy must be in place.

Caveat 2: Depending on how many and what applications are centrally delivered, the management of the Citrix application servers can be very complex. Testing and patching can be fraught with problems, possibly making the servers vulnerable to attack. Ensuring that users of the applications have user only rights and ensuring patches are applied as soon as possible can mitigate this issue. When feasible, separating more vulnerable applications (such as IE) and those that are more sensitive or critical to the organization (such as database applications) onto separate Citrix servers may also help reduce the risk of an attack causing damage.

One Time Passwords:
GIAC Enterprises (G.E.) has implemented the use of SecurID cards for external employee access to its applications (accessible via the Citrix infrastructure). A server running RSA's Authentication Manager manages SecurID authentication. Use of one time passwords makes it very difficult for an account name / password combination to be compromised.

Caveat: Loss of a fob means loss of access. Also, if the PIN is written on a sticky and stuck to the fob, the added security is basically null and void. The GIAC Enterprises Remote Access policy outlines appropriate and inappropriate management of the fob.

Central Anti-Virus w/ AV on Servers, Workstations, and Laptops:
The company was using standalone versions of Cheyenne Anti-Virus when it discovered that several viruses were active on company workstations. Workstations were getting infected without the employees' knowledge and in a few cases, the anti-virus had alerted the employee that a virus was detected but could not be cleaned – and the employee ignored the warning. These issues and the move to using Citrix for application delivery required that a new approach be taken.

GIAC Enterprises now uses Trend Micro's OfficeScan and Server Protect Enterprise versions using their central management consoles. This has allowed the company to update all internally operating workstations and its Novell, Windows, and Citrix servers automatically through a central system. Routine

scans can be activated from a central system. All alerts are sent to the central system as well as key technical staff who can then ensure that the issue is managed appropriately.

Clients are configured to not allow a user to unload the application. Laptop builds install the anti-virus client configured for roaming mode to allow it to maintain updated signatures while not in the office.

Caveat: Support for the Linux servers – including the ftp server is not yet active in GIAC Enterprises. The sayings submitted by the Suppliers and Translators are currently scanned during the transfer of the data from the ftp server to the preprocessing Windows-based server. G.E. is currently testing Trend Micro's Linux compatible product.

Personal Firewalls on Laptops:
GIAC Enterprises installs ZoneAlarm Pro on each of its externally used laptops. The application is configured to automatically update. The firewalls are initially configured to allow dns, citrix-ica, http, https, and time activity. Employees have the capability of disabling the firewall but sign the laptop use policy acknowledgment, which indicates that they will not disable application or modify its configuration without prior approval from the head office.

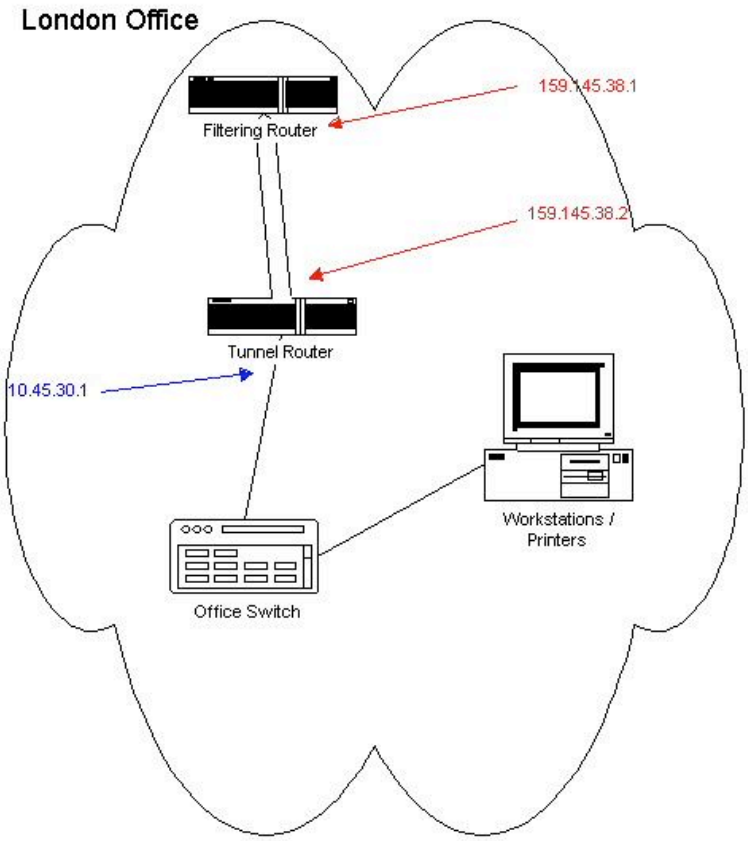
Internal Firewall:
GIAC Enterprises' internal network is considered trusted but is really spread across the globe. A worm on the inside, or an intruder, would have direct access to infrastructure systems, servers, workstations, etc. To make the inside not quite so soft and chewy, G.E. has installed a firewall services module into its central Cisco Catalyst 6506 at the head office. This firewall is being used to vault off (shield) the file server, administration server, and database server segments from each other and from the rest of the internal network. It is also shielding the test and development segment from the production systems.

The firewall is configured using the same principles as the primary (perimeter) firewall. Only specific services to and from specific addresses are allowed to pass through the firewall. All other access is blocked.

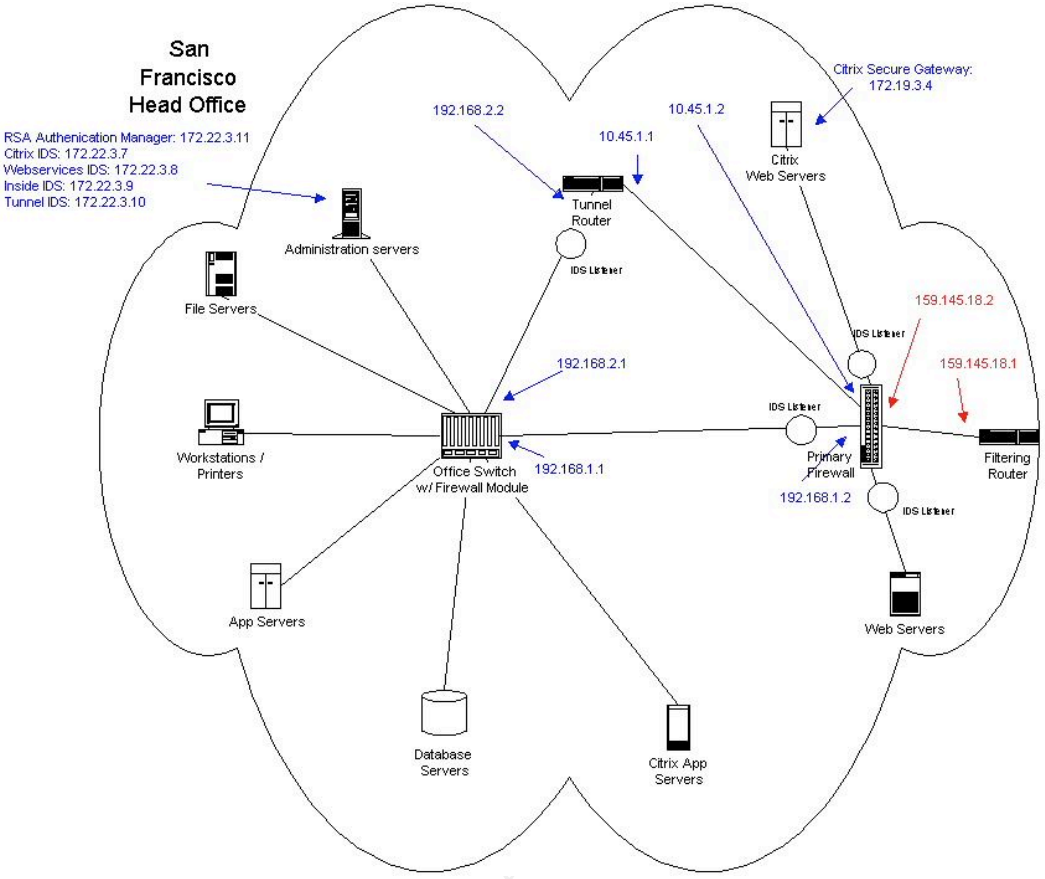
Caveat: As with the Pix firewall, this is a stateful inspection system, not an application layer firewall. Application layer vulnerability mitigation for the shielded servers is managed by ensuring patches are kept up to date, access to applications is limited to just those who need it, and logs are monitored routinely.

Security Component Addressed Diagrams:

Following are diagrams showing the location of GIAC Enterprises main security technology components. Regional office components are represented by one diagram with like component addresses differing only in the third octet, which is different for each office. Red indicates Internet routable addresses, blue indicates private addresses.



Regional Offices:
Hong Kong, London,
Sydney, Vancouver



Assignment 3 – GIAC Enterprises, Primary Firewall Rule Base

As mentioned in the GIAC Enterprises, Security Architecture (Assignment 2) section, a default deny policy is in place for the primary firewall. This policy limits access through the firewall, both ingress and egress, to only the specific ports needed.

Passwords:

The firewall passwords are encrypted using the 'enable password [password] [encrypted]' and 'passwd [password] [encrypted]' commands. They will show in the configuration as follows.

enable password Y6C71FKMxafk71FG encrypted
passwd J728k6m588/08nwB encrypted

Note: Tools, such as 'Cain and Abel' are available on the internet that can decrypt these passwords. Backup configuration copies are kept in a controlled, limited access directory. Any print outs made are kept confidential and shredded when no longer needed.

Access Lists:

The access lists are all firewall centric – inbound to it. (See the diagram in the GIAC Enterprises, Perimeter Security Architecture, Head Office Perimeter Firewall section.) The lists are named, using the format of '[interface name]-inbound[#]' with the number rotating between 1 and 2. This allows the modified access list to be copied to the firewall while the older access list is still in place and active. Once the modified / newer version is on the firewall, the firewall 'access-group [access-list name] in interface [interface name]' command is used to immediately activate the newer list, thus limiting the amount of time down or open time. The older list is then deleted using the no access-l [access-list name] command.

The access list information below is listed in the order that it is configured. The firewall honors the order of the entries from first to last. It will activate the first match found for a packet. Each access list will end with the following lines to deny any non-specified traffic from passing.

access-list [access-list name] deny icmp any any
access-list [access-list name] deny ip any any

The Outside List:
The outside-inbound list is the access-list used by the gateway which inspects Internet sourced traffic coming into the GIAC Enterprises network. This list first denies access for traffic using source addresses that shouldn't be traveling on the Internet and therefore shouldn't be allowed to connect to any GIAC Enterprise system and thus is listed first in the list. Note: This set of denies is also blocked on the filtering router in front of the firewall. This is a duplicate of that set should the router let something through or the router's access list get changed.

Access-list outside-inbound1 deny ip 0.0.0.0 255.0.0.0 any
access-list outside-inbound1 deny ip 10.0.0.0 255.0.0.0 any
access-list outside-inbound1 deny ip 127.0.0.0 255.0.0.0 any
access-list outside-inbound1 deny ip 169.254.0.0 255.255.0.0 any
access-list outside-inbound1 deny ip 172.16.0.0 255.240.0.0 any
access-list outside-inbound1 deny ip 192.0.2.0 255.255.255.0 any
access-list outside-inbound1 deny ip 192.168.0.0 255.255.0.0 any
access-list outside-inbound1 deny ip 192.192.0.0 255.255.0.0 any

The NATed addresses for GIAC Enterprises are the 159.145.18 address range. Addresses from this range should never be source addresses coming to the company and thus are denied in the same manner as those above.

access-list outside-inbound1 deny ip 159.145.18.0 255.255.255.0 any

The gre tunnel traffic from the external office tunnel router outside interface is allowed in to the translated address for the head office tunnel router. All other gre traffic is denied. These are constant connections so they are listed high in the access list to eliminate extra traversal of the list.

access-list outside-inbound1 permit gre host 159.145.28.2 host 159.145.18.8
access-list outside-inbound1 permit gre host 159.145.38.2 host 159.145.18.8
access-list outside-inbound1 permit gre host 159.145.48.2 host 159.145.18.8
access-list outside-inbound1 permit gre host 159.145.58.2 host 159.145.18.8
access-list outside-inbound1 permit gre host 159.145.68.2 host 159.145.18.8
access-list outside-inbound1 deny gre any any

General access is allowed to the main GIAC Enterprises web server's http and https ports but only if it is coming from a standard client source port, ie one above 1023. The web server is one of the most active systems for Internet activity so access is listed high in the list.

access-list outside-inbound1 permit tcp any gt 1023 host 159.145.18.36 eq www
access-list outside-inbound1 permit tcp any gt 1023 host 159.145.18.36 eq https

General ssl access, with source port of above 1023, is allowed to the Citrix Nfuse server to allow employees who have been given RSA SecurID cards access to agency systems from their Internet location. The frequency of this access is fairly high but not as high as the web server access, so it gets listed after it.

access-list outside-inbound1 permit tcp any gt 1023 host 159.145.18.94 eq https

Secure FTP access to the GIAC Enterprise's FTP server is allowed for each specific cookie sayings supplier and translator using the format below. Uploads are less frequent so they are place lower in the list but are placed together in source order for ease of management.

access-list outside-inbound1 permit tcp host 159.34.18.5 gt 1023 host 159.145.18.24 eq ssh

SMTP access to GIAC Enterprises' e-mail server is allowed from client port addresses. Again, this activity is less frequent and thus is lower in the list.

access-list outside-inbound1 permit tcp any gt 1023 host 159.145.18.12 eq smtp

General DNS queries are allowed to the external address dns server from client port addresses. This is generally not a highly utilitized activity and thus is lower in the list.

access-list outside-inbound1 permit udp any host 159.145.18.21 eq domain

The Inside List:
This inside-inbound list is used by the inside interface to inspect traffic coming from the internal GIAC Enterprises network to the firewall.

Note: If the firewall throughput and power are not being taxed, readability of the access list may be more important for ordering than which rules get used the most. If this is the case, ordering the access list by source address first and then destination port may be helpful. This same ordering can be used with other access lists but can be problematic for the outside list. In this situation, the outside list can be order by destination address and then destination port.

Each Citrix application server acts much like a workstation for the purposes of general access to the Internet. G.E. has approved by policy general access to port 80 (www), port 8080 (an alternate http port), port 443 (https), and port 21 (ftp). Use must comply with the company's acceptable use policy. As the applications servers are highly utilized all access list entries for them are fairly high in the list.

Note: All workstation address ranges will also have these same allows.

access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 any eq www
access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 any eq 8080
access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 any eq https
access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 any eq ftp

Each Citrix application server is allowed to connect to the company's e-mail server. Example below.

access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 host 172.19.4.6 eq pop3
access-list inside-inbound1 permit tcp host 192.168.101.3 255.255.255.255 gt 1023 host 172.19.4.6 eq smtp

One Citrix application server is allowed to connect administratively to servers on the citrix and webserver interfaces. Individual allows for specific protocols on the specific servers is configured. Example for terminal services below:

access-list inside-inbound1 permit tcp 192.168.101.3 255.255.255.255 gt 1023 host 172.19.3.4 eq 3389

A utility server gets the supplied sayings from the ftp server.

access-list inside-inbound1 permit tcp host 172.22.4.7 gt 1023 host 172.19.4.5 eq ssh

The Offices List:
The offices-inbound list is used by the offices interface to allow only the gre tunnels traffic to pass from the head office tunnel router to the regional office tunnel routers as follows.

access-list offices-inbound1 permit gre host 10.45.1.1 host 159.145.38.2
access-list offices-inbound1 permit gre host 10.45.1.1 host 159.145.48.2
access-list offices-inbound1 permit gre host 10.45.1.1 host 159.145.58.2
access-list offices-inbound1 permit gre host 10.45.1.1 host 159.145.68.2
access-list offices-inbound1 deny gre any any

The Citrix List:
The citrix interface controls access from the externally accessible NFuse server. While this list is small, order of the permits isn't very important.

The Nfuse server (with Citrix Secure Gateway installed on it) communicates with the RSA Authentication Manager to authenticate user access.

access-list citrix-inbound1 permit tcp host 172.19.3.4 gt 1023 host 172.22.3.11 eq www
access-list citrix-inbound1 permit udp host 172.19.3.4 gt 1023 host 172.22.3.11 eq 5500

The server is allowed to query the internal dns server.

access-list citrix-inbound1 permit udp host 172.19.3.4 gt 1023 host 172.22.3.6 eq domain

Nfuse inter-connects to the Citrix application servers.

access-list dmz1-inbound1 permit tcp host 172.19.3.4 gt 1023 192.168.101.0 255.255.255.224 eq www
access-list dmz1-inbound1 permit tcp host 172.19.3.4 gt 1023 192.168.101.0 255.255.255.224 eq citrix-ica

The server synchronizes with the internal time server.

access-list citrix-inbound1 permit udp host 172.19.3.4 eq ntp host 172.22.3.5 eq ntp

The Webservices List:
The webservices interface controls access from the externally accessible GIAC Enterprises systems mentioned in the Outside List section, with the exception of the Citrix server. When each server has the same requirements, the examples below will be using the web server's address.

Each server synchronizes with the internal time server. Below is an example:

access-list webservices-inbound1 permit udp host 172.19.4.4 eq ntp host 172.22.3.5 eq ntp

A web server application queries the SQL Server.

access-list inside-inbound1 permit tcp host 172.19.4.4 gt 1023 host 172.22.5.4 eq 1521

Each server on this segment gets backed up by the NetBackup server that resides on the File Server segment. As this process only occurs once a night, these entries are generally found low in the list. Below is an example of the allows for this process.

access-list webservices-inbound1 permit tcp host 172.19.4.4 range 700 999 host 172.22.4.4 range 400 699
access-list webservices-inbound1 permit tcp host 172.19.4.4 range 4700 4999 host 172.22.4.4 range 4400 4699
access-list webservices-inbound1 permit tcp host 172.19.4.4 range 700 999 host 172.22.4.4 range 13720 13721
access-list webservices-inbound1 permit tcp host 172.19.4.4 range 4700 4999 host 172.22.4.4 range 13720 13721
access-list webservices-inbound1 permit icmp host 172.19.4.4 host 172.22.4.4

The Expansion List:
The expansion interface is currently disabled. During testing of the firewall and before the interface was disabled, an access list was applied to the interface that had the below two lines. This step was done as a precaution for the possibility of a system getting placed there that shouldn't be and getting access to the Internet.

access-list expansion-inbound1 deny icmp any any
access-list expansion-inbound1 deny ip any any

Logging:
The firewall logs to a central log server on the administration servers segment. Logging is kept at as high a level as possible without logging an overwhelming amount of information. Higher levels of logging can be very useful in troubleshooting and in security monitoring. 'Informational' logs application level access (ftp, http, etc), access list denies, the session builds and teardowns, and translation assignments.

logging on
logging buffered warnings
logging trap informational
logging history informational
logging host inside 172.22.3.4

General ICMP Deny:
The firewall should not answer any pings from the outside (Internet facing) interface.

icmp deny any echo outside

Pix IDS Signatures:
The Pix has some built-in IDS signatures[26] that it can look for. Which are active with which OS version is questionable but the IDS feature can and should be activated.

ip audit info action alarm
ip audit attack action alarm

Limiting Management Connections:
A very limited number of workstations and one restricted use Citrix application server need management access to the firewall. The following command is the configuration example for encrypted access.

ssh 192.168.20.46 255.255.255.255 inside

[26] System Log Messages 400000-400051, http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guide_chapter09186a00800eca3d_4container_ccmigration_09186a00801e8937.html - wp1032267

References:

1) Network Working Group. “RFC 1918 – Address Allocation for Private Networks.” Internet RFC/STD/FYI/BCP Archives. Feb 1996. 19 Dec 2004, URL: http://www.faqs.org/rfcs/rfc1918.html

2) Network Working Group. “RFC 3330 – Special-Use Ipv4 Addresses.” Internet RFC/STD/FYI/BCP Archives. Sept 2002. 17 Dec 2004, URL: http://www.faqs.org/rfcs/rfc3330.html

3) Cisco. “Subnet Masking and Addressing.” 18 Dec 2004, URL: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42ape.htm#xtocid5

4) NSA. “Defense in Depth.” 29 Nov 2004. URL: http://nsa2.www.conxion.com/support/guides/sd-1.pdf

5) Cisco. “Cisco PIX Firewall and VPN Configuration Guide, Version 6.3.” 15 Dec 2004. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html

6) Convery, Sean, et.al. “Cisco SAFE: Wireless LAN Security in Depth – version 2.” 16 Dec 2004. URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

7) HP. “HP iPAQ Pocket PC h4350 (FA172A) Specifications.” 18 Dec 2004. URL: http://h10010.www1.hp.com/wwpc/us/en/sm/WF06a/215348-64929-215381-314903-f62-349051.html

8) HP. “HP iPAQ Pocket PC h4100 and h4300 series – Frequently asked questions [WLAN].” 18 Dec 2004. URL: http://h10010.www1.hp.com/wwpc/pscmisc/vac/us/en/sm/pocketpc/faq_h4300.html - wlan

9) Wikipedia – the free encyclopedia. “Secure Shell.” 15 Dec 2004. URL: http://en.wikipedia.org/wiki/Ssh

10) Wikipedia – the free encyclopedia. “ingress traffic.” 30 Nov 2004. URL: http://www.webopedia.com/TERM/I/ingress_traffic.html

11) Cisco. “Cisco Aironet 802.11a/b/g CardBus Wireless LAN Client Adapter data sheet.” 18 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a00801ebc29.html

12) Symantec Corporation. “Symantec Internet Security Threat Report Identifies More Attacks Now Targeting E-Commerce, Web Applications” Yahoo Financial News. 20 Sept 2004. 26 Nov 2004. URL: http://biz.yahoo.com/bw/040920/195026_1.html

13) Wikipedia – the free encyclopedia. “egress traffic.” 30 Nov 2004. URL: http://www.webopedia.com/TERM/E/egress_traffic.html

14) Cisco. “Cisco PIX 515E Security Appliance Data Sheet” 29 Nov 2004. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html

15)Cisco. “Cisco SMARTnet and SMARTnet Onsite Solutions Data Sheet. 5 Dec 2004. URL: http://www.cisco.com/en/US/products/svcs/ps3034/ps2827/ps2978/serv_datasheet09186a0080092491.html

16) Madden, Brian. “What is Citrix’s SSL VPN Strategy?,” 16 Jul 2004. 15 Dec 2004. URL: http://www.brianmadden.com/content/content.asp?id=214

17) Cisco. “Cisco Aironet 1200 Series Access Point Data Sheet.” 18 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html

18) Cisco. “Cisco Catalyst 6500 Series Switches Introduction.” 6 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/switches/ps708/index.html

19) Cisco. “Cisco Catalyst 6500 Series Firewall Services Module Introduction.” 6 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html

20) Cisco. “Cisco Catalyst 2950G 48 EI Switch Introduction.” 9 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/ps3821/index.html

21) Cisco. “Cisco Catalyst 2950 24 Switch Introduction.” 9 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/ps627/index.html

22) Cisco “Cisco 2611XM Multiservice Router Introduction.” 16 Dec 2004. URL: http://www.cisco.com/en/US/products/hw/routers/ps259/ps4830/index.html

23) Cisco “Cisco 3825 Integrated Services Router Introduction.” 16 Dec 2004. URL: http://www.cisco.com/en/US/products/ps5857/index.html

24) Cisco. “Cisco Reference Guide: Cisco Access Routers,” Spring 2003 V.1. 16 Dec 2004. URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps221/c1031/ccmigration_09186a008017f1d1.pdf

25) Cisco. “Security Technical Implementation Guide for SMBs.” 20 Nov 2004. URL: http://www.cisco.com/en/US/netsol/ns339/ns395/ns360/networking_solutions_design_guidance09186a008019b14e.html

26) Sourcefire, Inc. “SnortUsers Manual 2.2.0.” 2003. 14 Dec 2004. URL: http://www.snort.org/docs/snort_manual/