Global Information Assurance Certification Paper

David Ball
GCFW Practical Assignment
Version 4.0

SANS Monterey, CA. July 2004
Submitted: 14 March 2005

Table of Contents

Assignment 1
Future State of Security Technology:
"the Myth of Intrusion Prevention"

Note: Although not part of the requirements for this paper, in addition to detailing the individual network security components for GIAC Enterprises, and at the risk of making the paper appear lengthy, the GIAC Screening Router, PIX and Catalyst switch configuration have been included in the Appendices as a learning exercise for the author.

abstract

GIAC Enterprises, a supplier of Fortune Cooking sayings to the restaurant business in Europe, North America and Australia has hired an external security consultant to evaluate the possible future use of Intrusion Prevention technology as part of their overall security infrastructure solution.

There's an old folk saying that "An Ounce of Prevention is Worth a Pound of Cure". In the world of Network Perimeter Security the latest cure-all buzz word is the concept of Intrusion Prevention. Intrusion Prevention is the ability of a device to perform proactive, real-time network defense. The term Intrusion Prevention was first coined by Internet Security Systems (ISS) back in 1998. Over the intervening years Intrusion Prevention technology promised analysts the Holy Grail of security technologies, namely a self-defending network. Or at least the IPS vendors did. In this paper we examine how much of IPS is just marketing slant on old IDS technology and how much is actually new development in the field of Intrusion Detection. We attempt to define what constitutes IPS in an effort to clarify some misconceptions. We then look at the challenges facing security departments tasked with integrating IPS into their existing security architectures. We also provide information on current vendor offerings in the IPS space. Finally we look into our crystal ball and attempt to predict where IPS is headed in the near future.

history of ids

We can't talk about Intrusion Prevention without first discussing Intrusion Detection technology. The history of IDS stretches back to a 1980 research paper written by James P. Anderson entitled "Computer Security Threat Monitoring and Surveillance".[1] In his paper Anderson highlighted the importance of audit trails in a computer system but went on to suggest that audit data was at times incomplete and could be improved upon by increasing the relevance of the data to its intended recipient, i.e. the security personnel it was targeted at. Then in 1986 Dorothy Denning presented "An Intrusion Detection Model" at the IEEE Symposium on Security and Privacy in Oakland, California. IDES - the Intrusion Detection Expert System, a real-time IDS, grew out of this initial project. The model provided "a framework for a general-purpose intrusion-detection expert system" which detected security violations by monitoring changes in audit logs.

so what is ids?

IDS brings a visual aspect to network security monitoring which was previously lacking. IDS can shed light on the types of traffic traversing our network. An IDS can be configured to alert a security analyst when particular types of malicious traffic are identified. IDS is like the radar on a battleship. Radar doesn't directly protect the ship but it provides valuable information on incoming attacks. Radar is an indispensable tool in warfare. However, if you went to war with just radar you'd have a hard time winning any battles. If you included radar along with heavy guns, fighter and bomber aircraft and accurate intelligence then you are building a multi-tiered defense against the enemy. Similarly IDS alone doesn't protect you from attack but it is a great tool to use in conjunction with other security technologies in a defense in depth approach. To date the criticism leveled against IDS has been it's high administration overhead. IDS triggers alerts on a packet level so you may have many alerts all related to the same single attack. It is this multiple alert scenario and the difficulty of weeding out actual hostile traffic against a very noisy background of both normal and abnormal activity that constitutes IDS' biggest challenge.

network versus host ids

A network IDS is simply a server or appliance running software customized and fine-tuned to detecting hostile network traffic. A network IDS sits on a network segment and grabs packets off the wire, comparing them to a signature database or anomaly engine and alerting if a match or discrepancy is found. So at its very basic an IDS is simply a sniffer on steroids. A network IDS has a minimum of two network interface cards - one plugged into either the SPAN port on the segment's switch or inline to a TAP with the other interface plugging into the segment running the IDS Management console. The IDS engine uses either signature based or anomaly based detection intelligence to fire an alert to the console. A host IDS on the other hand lives on, for example, a Windows or Unix host and makes use of that systems audit logs, registry or file system to detect and alert on changes.

what then is ips?

Intrusion prevention is the evolution of a detection system into a prevention role. The evolution of IPS has taken two different directions. Some vendors have taken the IDS to Firewall route whereas others have taken the offline IDS to inline IDS route. Inline IDS is also referred to as active IDS whereas more traditional IDS is referred to as passive IDS.

ids versus ips

There is still confusion within the industry over what exactly defines an IPS. One of the reasons why there might exist so much confusion over IDS and IPS technologies is that vendors have typically interpreted IPS in their own unique way. IPS means different things to different people and sometimes conveniently so. There are as many definitions of IPS as there are security vendors providing the technology and invariably these definitions serve to achieve their own ends as business entities. So there is a gray area between IDS and IPS. A commonly agreed definition of IPS may help to debunk some of the lingering IPS myths.[2] Let's then attempt to formulate a definition of IPS and by doing so help to separate fact from fiction when discussing the two technologies.

characteristics of ips

There are a number of characteristics which identify IPS technology. However, note that none by itself qualifies a product as an IPS.

ips as an inline device

First off a true IPS sits inline rather like a Firewall. Data passes to an external interface, the IPS makes an informed decision based on its detection engine and either blocks or allows the traffic to pass to the inside interface.[3] This all happens in real time. In many cases IPS is just rehashed IDS technology modified to sit inline with IDS vendors tending to build their IDS detection engines into their inline IPS products.

proactive versus reactive monitoring

An IPS must be proactive in preventing attacks. An IDS is an alerting system but it alerts only after the fact. Returning to our radar analogy earlier, a radar system can detect an incoming missile but can do nothing by itself to stop that missile from hitting its target. Similarly, with an IDS the attack packets may have already made it the destination host despite the alert. An IPS on the other hand drops packets *before* they reach the intended target. In addition an IPS may continue to drop related traffic for a period of time after the initial attempted attack or drop traffic which is part of the same tcp stream. It's appropriate to mention here that a device with Active Response[4] or Reactive Defense mechanisms such as shunning and tcp resets is not sufficient to qualify a product as an IPS although some vendors will claim to the contrary. Although Active Response by itself doesn't qualify a product as IPS, some form of automated response is required. However this response should be independent of other security components.

contextual awareness

An IDS is unaware of its context within the network environment. It doesn't have a visual map of the hosts and network devices around it. It may alert on a UNIX exploit on the wire but if your machines are all Microsoft Windows then the criticality is reduced. You still need to know about these attacks however. You may hear a rumor around town that thieves are targeting BMW automobiles but you would still need to take notice even if you drove a Mercedes. Network awareness is seen as the next big challenge and evolution in network IDS/IPS. Companies like SourceFire are developing Real Time Network Awareness (RNA) into Snort using automated scanning and Vulnerability Assessment tools.

operates in real time or near real time

Here we have a further trait of an IPS. It must make real-time or, at the very least, near real-time decisions on denying of traffic. Hostile traffic must be blocked before it reaches its intended target. This requires making an immediate decision as to the nature of incoming streams and blocking them if found to be malicious.

packet scrubbing

Finally an IPS engine will normally provide for packet-scrubbing or clean-up before the packet is sent out the internal interface. Packet scrubbing removes protocol inconsistencies resulting from varying interpretations of the tcp/ip specification or from intentional packet manipulation.[5]

do we need ips?

So Intrusion Prevention is essentially an extension of existing IDS technology sitting inline rather than offline and taking action against attacks including active response mechanisms. However there is always the question whether you want to hand off that much control to an automated system. Marty Roesch the creator of the Snort Open Source IDS once commented that allowing IPS systems to make automated responses to intrusion attempts was like arming a security camera with a can of tear gas. Vendors have answered these concerns by providing two modes of operation with IPS: IDS mode and Inline mode. IDS mode allows you to plug the IPS into a span port or inline tap and tune the IPS to your environment. Once tuned the IPS can then switch over to inline mode. As you can see IPS does not do away with IDS completely. IDS and IPS should be seen as complimentary since their functions on the network are not entirely the same. The IDS performs the monitoring while the IPS performs access control. For example an IPS is not effective against a worm spreading on your internal network unless it's sitting inline. You still need IDS to detect the infection.

ips drowning in marketing collateral

As mentioned earlier IDS has suffered bad press due to its high administration overhead. This fact coupled with a now-famous summer 2003 announcement by Gartner Group that "*Intrusion Detection Is Dead, Long Live Intrusion Prevention*"[6] has added fuel to the IPS marketing frenzy. Marketing departments have been quick to jump on this opportunity and hail the benefits of Intrusion Prevention Systems when in a lot of cases they are just re-branding old IDS technology.

different vendor offerings

At the risk of making it sound like marketing material let's examine some of the current vendor offerings from the bigger players and the different ways they integrate IPS into their products.

Checkpoint InterSpect

The first move by Checkpoint into the appliance market. InterSpect provides Intrusion Prevention for "high value" internal network segments. It's not however designed to protect DMZ segments. InterSpect provides protection against malware, peer-to-peer and Instant Messaging applications, unauthorized MAC or IP addresses. InterSpect can also quarantine or block offending machines or segments.

Cisco Dynamic IPS

Joint leader in the IDS/IPS space together with ISS, Cisco inline technology has existed for some time in the form of the IDS functions of Cisco routers and PIX firewalls under the heading Cisco Secure Integrated Software. The PIX signature set is a subset of the signature set found on the Cisco Secure IDS product range with only about 60 signatures supported. Cisco also provides a router IDS card which slots into a 2600, 3600 or 3700 series Cisco routers to provide similar functionality to a network IDS sensor.[7] Cisco considers this router card part of its Cisco Intrusion Protection System. Cisco has also recently brought to market a series of Integrated Services routers with IPS capability namely the Cisco 3800 series Integrated Services router[8] with dynamic IPS.

Juniper/Netscreen IDP family

Juniper purchased Netscreen in 2003 and along with it came the Netscreen range of Firewalls and Intrusion Prevention Systems (IDP). Netscreen had earlier purchased OneSecure in 2002 and started building OneSecure's Deep Packet Inspection technology into its Netscreen firewall appliances starting with ScreenOS 5.0.

NAI/IntruVert

Network Associates purchased IntruVert and the IntruShield product line in 2003. The IntruShield products are appliance-based IPS. One of the oft-touted features of the IntruShield range is the ability to deploy multiple IPS sensors to protect multiple segments from a single IntruShield device through the use of what NAI call “Virtual IPS” technology. The IntruShield products are also considered some of the fastest IDS/IPS devices on the market.

RealSecure Proventia IPS appliance

ISS relies on an IPS technology called Virtual Patching on its Proventia range of appliances. Virtual Patching uses a vulnerability signature rather than an exploit signature as with traditional signature-based IDS/IPS. Signature based detection engines are easily evaded by making changes to the exploit itself. A well-defined vulnerability signature can protect against both known and unknown exploits.

Snort Inline

Snort Inline is a modified version of the popular Open Source Snort IDS product. Snort Inline uses a number of new rule types and works together with the Linux iptables firewall to determine which packets to drop or accept. Snort Inline uses the Snort IDS signature database to provide IPS functionality.[9]

Symantec 7100 series IPS appliance

Symantec recently launched to market a series of IPS appliances as part of their move into the IPS market. The 7100 series IPS is completely redesigned from the ground up rather than being based on their existing Manhunt IDS. The 7100 series introduces Symantec’s new Intrusion Mitigation Unified Network Engine (IMUNE) detection engine. IMUNE uses traditional signature based detection together with protocol anomaly detection, IDS evasion detection and rate limiting.[10] As with the ISS Proventia mentioned above the Symantec device also takes the approach of providing vulnerability signatures rather than exploit signatures to increase detection of zero-day attacks.

TopLayer Attack Mitigator IPS

The Attack Mitigator is a family of ASIC-based appliance IPS. The Attack Mitigator is an evolution of the Firewall rather than the IDS. By definition the TopLayer product is more of a rate-limiting IPS than a content-based IPS. Rate-limiting IPS detect changes in traffic flow allowing it to protect against syn-flooding and other DoS attacks. In contrast to traditional, signature based IPS, the Attack Mitigator product is best placed in front of the Firewall to protect from Denial of Service attacks. The Attack Mitigator will proxy incoming syn packets until it is sure the connection request is legitimate.[11]

TippingPoint Technologies' UnityOne

Like the TopLayer product, UnityOne is also a rate-limiting IPS providing protection against DoS attacks by using thresholds that define normal traffic and denying traffic crossing these thresholds and depending on the policy defined for the device. 3Com purchased TippingPoint at the end of 2004.

IPS placement in the enterprise

The following diagram shows placement of a traditional IPS based on Deep Packet Inspection and signature matching. The IPS sensor is placed directly behind the Firewall. The scenario below whereby the sensors and hosts report back to the Security Information Management console is a model that the industry is only just moving to. The idea is that information is relayed from the sensors to the SIM and the SIM looks after the task of event correlation, analysis and alerting.

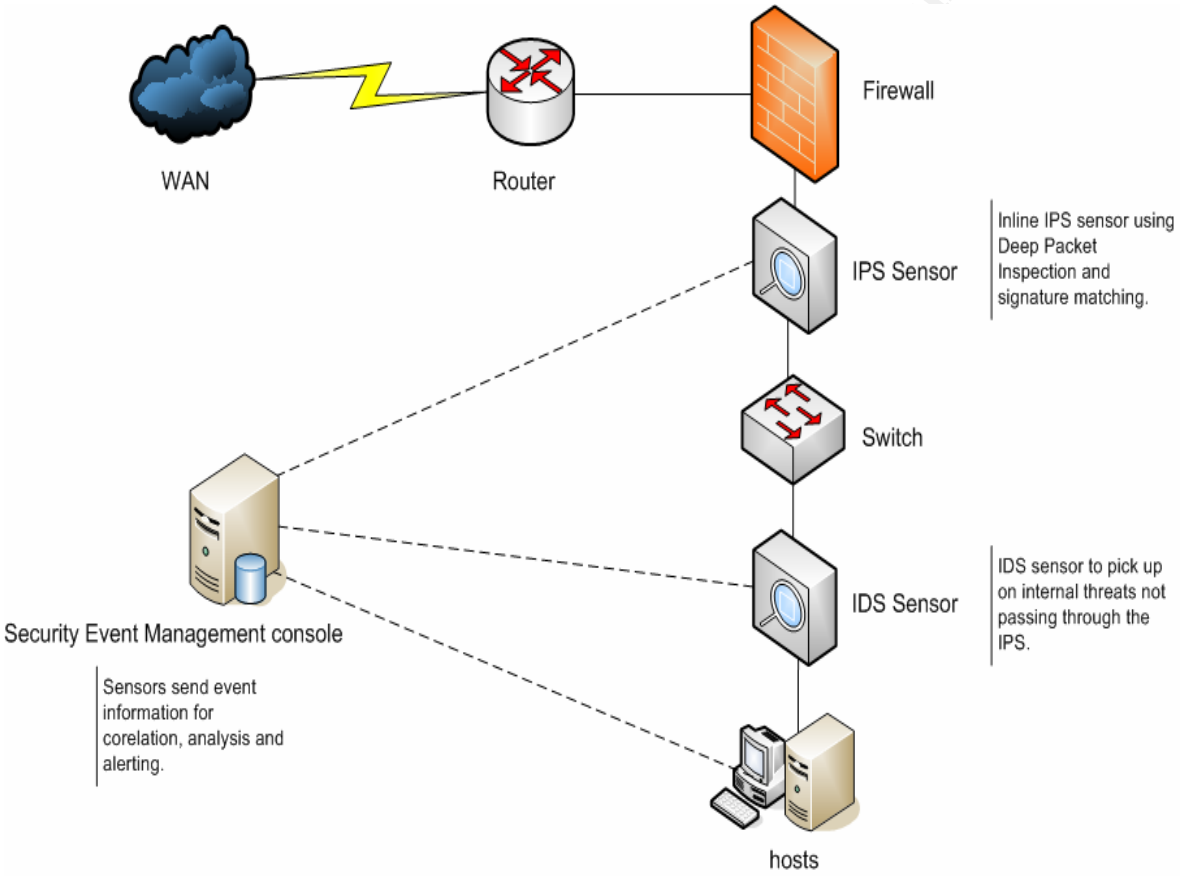

Figure 1: IPS Placement in the enterprise [12]

Current and Future Trends

Firewalls are still the single most effective security product sitting on corporate networks today. The trend however is moving toward the integration of IPS in the form of Deep Packet Inspection into current Firewalling devices. More and more vendors are collapsing IPS inline into the Firewall. We appear to be moving toward an all-in-one security device combining firewall and IDS technology. For sure there is a case for an all-in-one security device but for the moment these devices remain the domain of smaller enterprises with larger companies still preferring best-of-breed technology in separate devices.

Many companies are running IPS with a signature set pruned from the typical thousands of signatures to approximately 700-800 of the most common virus, worm and other attacks. A reduced signature set also helps to speed up performance of the IPS. If you do decide to run a cut down signature set then it's important to run an IDS with a full set of signatures behind the IPS to catch any exploits not alerted on by the IPS.

IPS clustering products are beginning to appear on the market. Many organizations use asymmetric routing with multiple routers to balance traffic and provide redundancy. This can confuse a non-clustered IPS. The clustered solutions also eliminate the single point of failure with one IPS. An example of such a clustered IPS solution is the new TopLayer Attack Mitigator IPS 5500 ProtectionCluster.

We are also now seeing IPS being offered as a Managed Service. The Sentinel Product by econet.com[13] is a managed IPS service where for a monthly subscription fee an IPS is installed outside the Firewall at the customer site and remotely managed by econet engineers. Many other MSSP's provide similar services with the vendor products mentioned earlier.

Although some years away there is a trend towards end-point security policy enforcement by building IPS functionality into the OS kernel at the host level. Firewall, IPS and anti-virus technology will move to the individual network devices such as hosts, and even LAN switches. Policy enforcement is then controlled by the Security Information Management console. By then we may see IDS being relegated to a mainly forensics and event analysis tool.[14]

On the subject of complexity, Intrusion Detection and Prevention has suffered from an inherent complexity in the way the technology is installed. Any new evolution in IDS and IPS technology must reduce complexity and allow for hundreds of appliances to be installed, updated, and managed with minimal subject matter expert interaction. We also need to simplify the tuning process incrementally. This may happen by way of pre-configured signature templates for different environments, i.e. ISP versus Financial organization or through the generation of pre-scanned profiles of the enterprise environment for the installation process. [15]

challenges for the enterprise

Although on the surface a panacea, IPS does bring its own unique set of challenges. For example, in the event of equipment malfunction do we fail open or fail closed? Fail open and you risk leaving through hostile traffic. Fail closed and we've just sent good and bad traffic to the proverbial bit bucket and performed a Denial of Service on our own network. There are also tuning challenges with IPS. False positives are more dangerous in IPS than IDS. As a result, and as mentioned earlier, most IPS vendors provide two modes of operation: IDS mode and Inline mode.

To create a healthier security ecosystem we need to start moving towards a more holistic approach to security where we start correlating real-time event data through Security Information Management from the myriad security devices and hosts on our network. It's unlikely that IPS will supercede IDS until we get the correlation variable nailed down. As depicted in Figure 1 above we are then heading towards a scenario whereby the IDS doesn't alert itself but reports to the SIM and the SIM takes care of event correlation and alerting. If we don't crack this correlation nut then false positives will continue to cripple the technology.

As with all security devices any IDS/IPS deployment must be based on a security policy. Without a security policy any deployment of IDS or IPS is doomed to failure.

Although Deep Packet Inspection technology provides the benefit of being able to look into the higher level OSI layers, the complexities inherent in Deep Packet Inspection software and some vendors' implementations have led to vulnerabilities in the DPI inspection engine.[16] Recent vulnerabilities have been found in Snort, Cisco, Checkpoint and Trend Micro products.

conclusion

There is no silver bullet or quick-fix solution when it comes to mitigating the risks of security breachs. A layered or multi-tiered defense is still considered the most effective approach. A layered defense with multi-vendor products takes the model a step further. IPS adds another level to the idea of defense in depth but shouldn't be held up as a cure-all for our security woes. With all the hype surrounding IPS and IDS technology it's easy to have unrealistic expectations of the value that both technologies bring to your network. While IPS might be a technology you need, there's still plenty of value that can be tapped from IDS by properly integrating it into your environment.[17] You might be better advised to make the effort to get more from an existing IDS implementation rather than implementing an IPS solution. If you already feel that you are using IDS to its maximum then go ahead and investigate IPS. Also the bad press that IDS gets should be seen as symptomatic of issues in the IT process rather than with the technology itself. However as vendors start to get their act together and the industry settles on an agreed definition, IPS technology will make its way firmly into corporate environments. However you're more likely to see IPS technology built into existing security devices rather than being able to point our your IPS "box" on the network. IPS should be seen more as a *technology* rather than a new and tangible security product. Despite the problems though the numbers do speak for themselves. Recent research indicates that the IDS/IPS market will hit US$1BN in yearly sales by 2007.[18] So the jury may still be out on the benefits of IPS and history may be the best judge whether the fuss over the technology was truly worth the effort.

references

[1] Anderson, James P. “Computer Security Threat Monitoring and Surveillance”. 26 February 1980.
http://csrc.nist.gov/publications/history/ande80.pdf

[2] Plano, Andrew M. What is an Intrusion Prevention System? ©2004.
http://www.anitian.com/corp/papers/ips_defined.pdf

[3] Intruvert Whitepaper: Intrusion Prevention: Myths, Challenges and Requirements. April 2003.
http://www.networkassociates.com/us/local_content/white_papers/public/wp_intrusionprevention.pdf

[4] Larsen, Jason and Haile, Jed. Understanding IDS Active Response Mechanisms. 29 January 2002.
http://www.securityfocus.com/infocus/1540

[5] G. Robert Malan and David Watson. University of Michigan. “Transport and Application Protocol Scrubbing”.
www.ieee-infocom.org/2000/papers/340.ps

[6] Gartner Group: IDS is dead. Long live Intrusion Prevention. June 2003.
http://www.esecurityplanet.com/views/article.php/2228631

[7] Cisco IDS Network Module for Cisco 2600, 3600, and 3700 Routers.
http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_data_sheet09186a008017dc22.html

[8] Cisco 3800 series Integrated Services Routers
http://www.cisco.com/en/US/products/ps5855/products_data_sheet0900aecd8016a8e8.html

[9] The official Snort Inline website.
http://snort-inline.sourceforge.net

[10] Braunberg, Andrew, CSO Online. Symantec's New Intrusion Prevention Devices Welcome in Market.
http://www.csoonline.com/analyst/report2757.html

[11] TopLayer Attack Mitigator IPS.
http://www.toplayer.com/content/products/intrusion_detection/attack_mitigator.jsp

[12] Radcliff, Deborah. Next Generation IDS. 8 November 2004.
http://www.nwfusion.com/research/2004/110804ids.html?page=2

[13] Sentinel IPS.
http://sentinel.econet.com/

[14] Radcliff, Deborah. Network World. The Evolution of IDS. 8 November 2004
http://www.nwfusion.com/research/2004/110804ids.html

[15] Yee, Andre. NFR Security. The intelligent IDS: next generation network intrusion management revealed.
http://www.eubfn.com/arts/887_nfr.htm

[16] Porter, Thomas. The Perils of Deep Packet Inspection. SecurityFocus. 11 January 2005
http://www.securityfocus.com/infocus/1817

[17] Van Wyk, Kenneth. Trouble Lies with IT and not IDS. 5 October 2004.
http://www.esecurityplanet.com/views/article.php/3417561

[18] Wilson, Jeff. Worldwide IDS/IPS Product Revenues. 9 June 2004.
http://www.infonetics.com/resources/purple.shtml?ms04.id.1q04.nr.shtml

Assignment 2
Security Architecture:
“Preventing the cookie from crumbling”

Abstract

GIAC Enterprises is a small but well known operation supplying fortune cookie sayings to the U.S., European and Australia/New Zealand markets from its distribution base in Hong Kong. We have been tasked with providing consulting services to GIAC Enterprises to assist with secure network connectivity between the GIAC Hong Kong office and its Branch offices, Customers, Suppliers, Partners and GIAC remote workers. We have also been asked to design the network perimeter security architecture for the Hong Kong head office and branch offices.

GIAC Enterprises Geographic Structure and headcount

The GIAC Head Office is located in Hong Kong with approximately twenty eight staff. The company has a further four satellite offices located in Dublin Ireland; San Francisco,California; Guangzhou, China and Brisbane, Australia supporting their respective geographic regions and bringing the total headcount to fifty staff.

Support staff skills and distribution

There are only two FTE's or Full Time Employees providing IT Support and Administration to the GIAC network. Both are based at the Hong Kong office. One is a Network Administrator with responsibility for basic Router and Firewall administration and the other is an MCSE certified SysAdmin who provides support for the Windows and UNIX hosts including the .NET development environment and back end MS SQL database. GIAC has part time staff at the branch offices who are GIAC employees but for whom IT support is only a portion of their work responsibilities. Budgets do not allow for full time staff at the Remote Offices. We have also hired the services of a Security Solutions Provider to make more complex configuration changes to our environment when required. This provider was chosen for its ability to provide on-the-ground support at all our offices as they have a local presence in each country.

Access Requirements

the GIAC Enterprise

GIAC Enterprises is a small operation and likewise technology budgets are small both for hardware and support staff. We have provided an up-front business plan and budget to management for the network security architecture across GIAC's five offices and the business plan and required purchases have been signed off on. Although the benefits of VPN Concentrators, Redundant Links and Routers, Commercial integrity checking tools and Enterprise Security Event Management applications are obvious these options are not available to *GIAC Enterprises* due to budgetary pressure and the frugal nature of the network architecture reflects this real-world reality. Hong Kong is the network hub for the enterprise and all core network hardware is located here.

the GIAC Telecommuter

Approximately 10% of the staff at each office are sales staff who are frequently on the road working out of hotels or at client premises. There is also a need to support a small group of telecommuters who work from home occasionally. We must provide secure remote access to email and the corporate Intranet for these staff. Access to the online sales databases for traveling sales staff is through a specially designed module of the Fortunes application and is accessed through the corporate web site.

the GIAC internal employee

We provide all internal GIAC employees with access to the Internet. Right now we don't provide for Content Filtering but in the future the company plans to evaluate the SurfControl product. All internal access to the corporate website is directly to the Public Services Segment from the internal network.

the GIAC Customer

Customers include fortune cookie resellers who supply to restaurants primarily in North America, Europe and the Australia market. Sayings are also sold to makers of Christmas crackers. Ironically the idea of fortune cookies after a meal is not common in Asia so only a minority of business is local to the region. Sayings are available under a number of different headings including traditional, romantic, funny and friendship. All orders are filled online through the fortune cookie sayings website at www.cookiemonster.com. Through the GIAC online presence customers also have the ability to track their own open orders.

the GIAC Supplier

GIAC has a supplier in Guangzhou Southern China who produces the fortune cookie sayings and a distribution centre in Hong Kong. Guangzhou was chosen due to its proximity to Hong Kong and the low labor costs and high quality when compared to other Asian countries. Our supplier requires secure access to the GIAC network to upload sayings to the database for sign off by management. We recommend suppliers and partners use the PuTTY client and SCP for secure copy of Fortune Sayings to our public SSH server.

the GIAC partner

The sayings are primarily meant for an English speaking market but GIAC does provide a translation service at no additional cost. The company can provide cookie sayings in four languages; English, Spanish, French and German. Our partner is responsible for the translation of GIAC fortune cookie sayings into these four languages. All sayings are uploaded in Chinese from the supplier and the fortunes are printed in Chinese with the translated sayings on the reverse. Customers may choose language requirements from the above list when ordering. Secure Partner access to the database is required to view sayings uploaded by the Guangzhou supplier and provide for translation of sayings signed off on by management. We also provide partner employees with mailboxes on the GIAC email server with IPSec VPN access to email.

the GIAC branch office

Branch office connectivity is provided via IPSec VPN over the public internet back to the head office. The VPN peer device on the head office side is the PIX Firewall and the VPN peer on the branch office side of the connection is the IOS Firewall providing CBAC and VPN services. Branch office employees connect to the head office over VPN tunnel to pick up email. All messaging is centralized at the Hong Kong office due to location of support staff. Remote offices connect to their Exchange 2000 mailboxes via the Outlook 2003 client over IPSec VPN tunnel. All traffic bound for the Internet from the internal branch network is sent unencrypted and all traffic bound for the Hong Kong head office is sent encrypted. There isn't a requirement for a fully meshed topology so there is no need for branch offices to directly connect to each other.

Application and Database architecture

The GIAC online presence has employed a typical three-tired architecture with IIS 6.0 serving up Microsoft Active Server Pages (ASP), with Microsoft .NET development environment and back-end MS SQL server database. The web server is housed on our Public Services Segment* and communicates with the Application server on the Application segment which in turn communicates with the back-end Database server on a database segment architected in a dual firewall setup.[1] The application is designed with separate supplier and partner modules to provide for the different levels of functionality required by both parties. Secure login is provided for each module through a username/password combination entered via a HTTPS encrypted session using SSL. GIAC has purchased a Verisign server SSL cert and installed the cert on its corporate web server. Secure uploading of data by suppliers and partners is provided through use of SSH.

**Note: Throughout this paper I will refer to the segment on which our publicly accessible services (DNS, SMTP, HTTP) are housed as the Public Services Segment and abbreviated to PSS. This is a typical Screened Subnet architecture. This is in contrast to DMZ which by strict definition is the area between the screening router and the Firewall.*

Management Guidelines

Management have communicated that wherever possible security solutions must be provided which leverage existing skills. If new skills are required then there is minimal training budget available. Remote Access and Branch office connectivity will be consolidated over a single T1 WAN connection to the Internet from the Hong Kong head office using IPSec VPN. This includes Internet browsing for internal staff. Three options for the Network Security Architecture with varying financial commitments have been provided to management at their request with a middle-ground approach selected.

the GIAC Security policy

Network security should be seen as a dynamic process centered on the GIAC security policy. It's important not to under-estimate the importance of having a security policy. As the saying goes, you need to figure out where you are going before you set out. The GIAC security policy is formally owned by and has been signed off on by GIAC management. Extracts from the GIAC management approved security policy relative to secure network access, identification and authentication is summarized below. This is a cut down list of policy related specifically to security architecture and does not include items such as acceptable use polices and incident handling procedures. The following sections can be cross-referenced directly with the Router Security, Server Security, VPN Security and Remote Access policy documents in use by GIAC Enterprises. In addition security policy related to all connectivity between GIAC and third party networks is defined in the Third Party Network Connection Agreement. [2]

GIAC Network Access policy

- We must allow the public to browse our corporate web server
- We must allow the public to query our DNS server and our DNS should be implemented in a split DNS architecture
- We must allow the public to send email to internal GIAC employees and all email should be relayed to/from an external SMTP server
- We consolidate all connectivity by provide a single T1 Internet Access point from the Hong Kong Head office and from each of our branch offices
- All communication between the GIAC branch and head office must be over IPSec VPN tunnel over the afore-mentioned T1 lines.
- All Remote Access to the corporate network by GIAC telecommuters and traveling sales staff must be via Remote Access IPSec VPN using the Cisco VPN software client.
- All uploads of fortune sayings from GIAC partner/suppliers must be encrypted.
- Web, Application and Database servers for the online fortune cookie sayings must be housed on separate secure segments off either the primary or secondary firewalls.
- Each network segment must have a Network IDS sensor.
- We must provide for a secure management segment for our Network and IDS management software.
- All management access to the firewall and other network hosts must be encrypted
- Network Perimeter devices must be hardened according to company guidelines. In the absence of such guidelines hardening must be according to industry standards.
- We must allow syslog messages from all Public Services Segment hosts and network perimeter security devices to the management console on the management segment.
- We must also allow SNMP messages to be sent from our network devices to our management console and we should block SNMP access to all but the logging host.
- We should provide for time-stamped logging of network events
- An NTP server must provide for accurate time stamps for logging purposes and should synchronize with an external time clock.
- All employees should be provided access to browse the Internet
- All employees must attend security awareness training as part of the new hire orientation process. They must also sign a statement that they have undertaken training and understand their responsibilities. Limited network access is provided until such time as awareness training has been completed and signed off on.
- The only mail allowed into our network is through our internal messaging environment. We block access to Hotmail and Yahoo Mail and all POP3 outbound access on port 110.

The following network diagram shows a high level view of GIAC Enterprises connectivity.

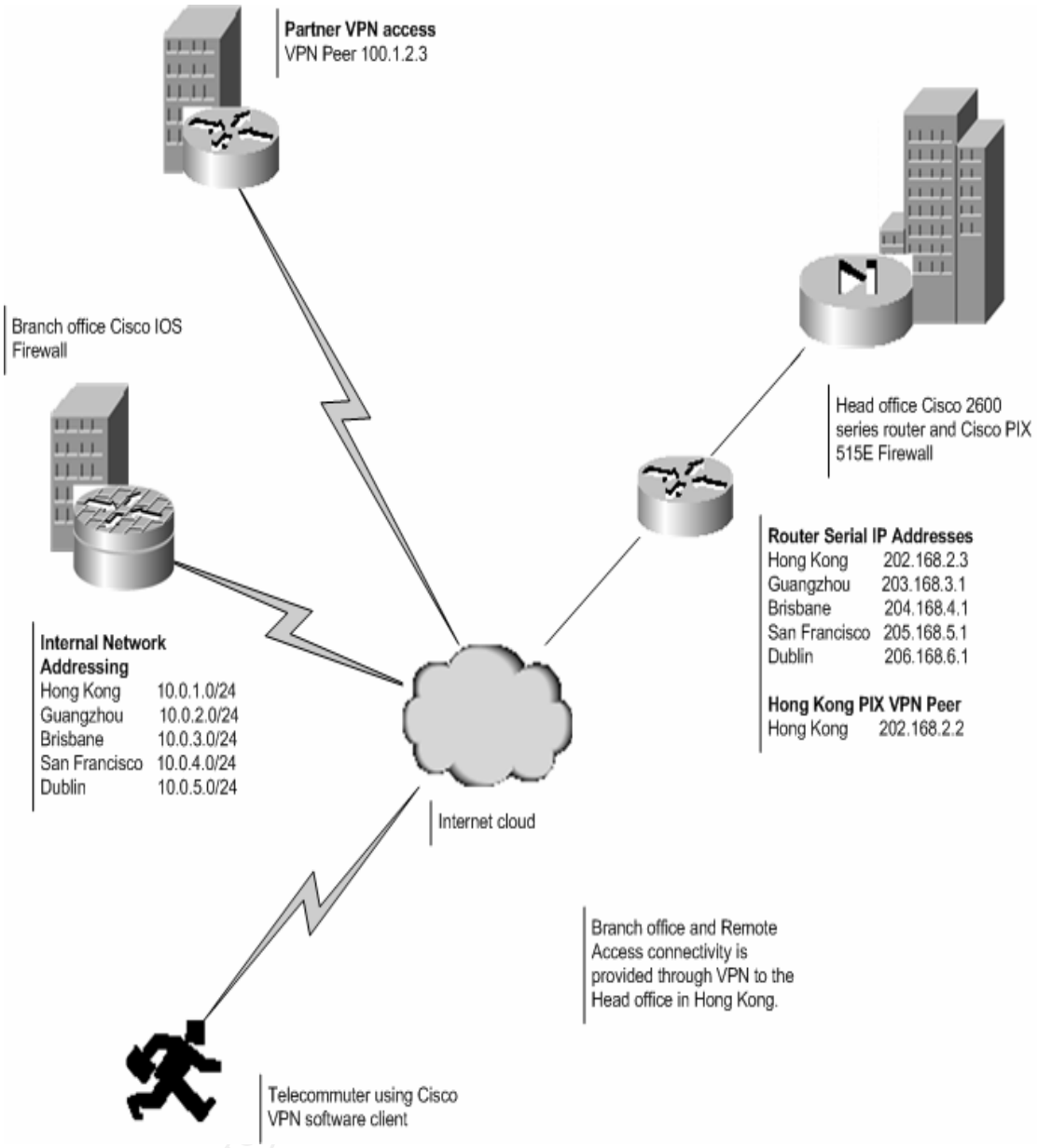

Figure 2 : GIAC Enterprise connectivity

GIAC Enterprises IP Addressing scheme

Subnetting

Each host on the GIAC network requires an IP address for every network it's connected to. An IP address consists of a network and host portion. A subnet mask is used to determine how many bits are used for each of the network and host portions of the IP. Subnetting allows a large network to be split up into smaller, more manageable units aiding network management and reducing network traffic. A host will determine if a destination machine is on its local subnet by bitwise "anding" the subnet mask with the source IP and the destination IP. The result is XOR'd and if the result is non-zero then the destination is not on the same subnet as the source. This packet is then sent to the default gateway which can be the router ethernet interface or the Firewall internal interface. Calculating a proper IP address range and subnet range is extremely important to both adequately satisfy existing GIAC IP addressing requirements and allow for possible future growth of the network.

the GIAC network IP addressing scheme

Segment	*Operating System/Application*	*Subnet Address/IP*
Hong Kong DMZ		
DMZ network address		202.168.2.0/24
Screening Router Ethernet interface	Cisco IOS v12.3	202.168.2.1
PIX Firewall outside interface	Cisco PIX OS v6.3	202.168.2.2
Screening Router Serial interface		202.168.2.3
Public Services Segment		
Public Services Segment network address		172.16.1.0/24
PIX Firewall interface		172.16.1.1
Corporate Web server *(Static NAT address)*	Microsoft IIS v6.0	172.16.1.2 *(202.18.2.5)*
External DNS	ISC BIND v9.2.5	172.16.1.3 *(202.168.2.6)*
Network Time Server (NTP)	RHE Linux NTPD v4.2	172.16.1.4 *(202.168.2.8)*
SMTP Relay	Exim Mail MTA v4.5	172.16.1.5 *(202.168.2.7)*
SSH server	OpenSSH v4.0	172.16.1.6 *(202.168.2.9)*
Snort IDS sensor	Snort 2.3	172.16.1.7
Application Segment		
Application Segment network address		172.16.2.0/24
PIX Firewall interface		172.16.2.1
Application server	Windows 2000 SP3 ASP .NET	172.16.2.2
Snort IDS sensor	Snort v2.3	172.16.2.3
Database Segment		
Database Segment network address		172.16.4.0/24
PIX Firewall interface		172.16.4.1
Database server	MS SQL 2000	172.16.4.2
Management Segment		
Checkpoint interface		172.16.3.1
Ciscoworks console	Ciscoworks 2000	172.16.3.2
IDS Console	SQUIL v0.5.3	172.16.3.3
Internal Networks		
Hong Kong		*10.0.1.0/24*
Guangzhou		*10.0.2.0/24*

Brisbane		*10.0.3.0/24*
San Francisco		*10.0.4.0/24*
Dublin Branch		*10.0.5.0/24*
Hong Kong office internal hosts		
PIX Firewall inside interface		10.0.1.1
WINS	Windows 2000 SP3	10.0.1.2
Internal DNS	Windows 2000 SP3	10.0.1.3
DHCP	Windows 2000 SP3	10.0.1.4
SMTP	MS Exchange 2000	10.0.1.5
CSACS	Cisco Secure ACS	10.0.1.6
Snort IDS sensor	Snort v2.3	10.0.1.7
Branch office Screening Routers		
Guangzhou Router Ethernet Interface		10.0.2.1
Brisbane Router Ethernet Interface		10.0.3.1
San Francisco Router Ethernet Interface		10.0.4.1
Dublin Router Ethernet Interface		10.0.5.1
Guangzhou Router Serial Interface		203.168.3.1
Brisbane Router Serial Interface		204.168.4.1
San Francisco Router Serial Interface		205.168.5.1
Dublin Router Serial Interface		206.168.6.1
Miscellaneous		
DHCP pool for Remote VPN users		10.0.10.1- 10.0.10.254
Hong Kong office NAT pool		202.168.2.200- 202.168.2.253
Hong Kong office PAT address		202.168.2.254

The following diagram shows the architecture of the Hong Kong office perimeter network and connectivity to branch offices and remote workers.

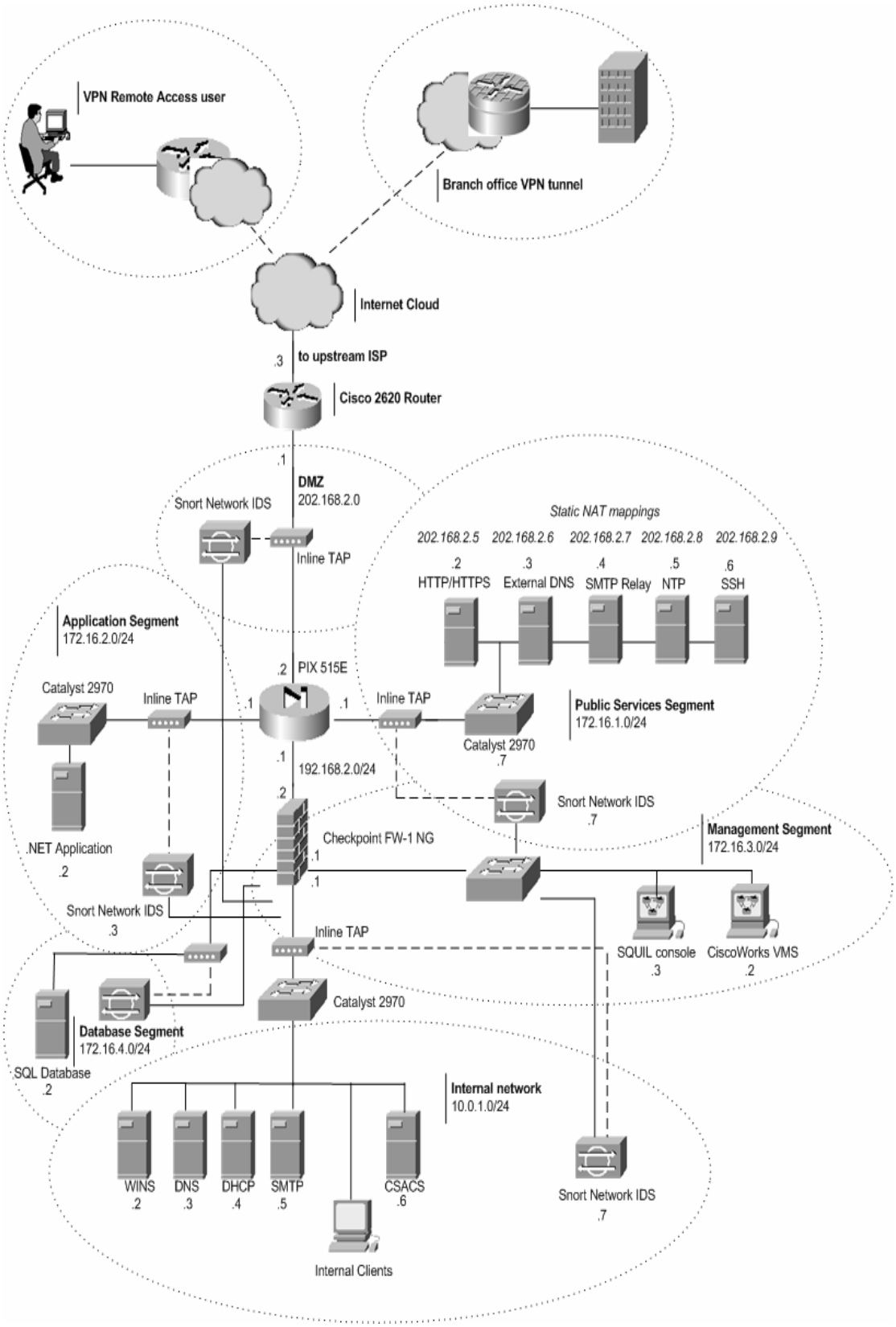

Figure 3: Hong Kong head office network diagram

Threat Mitigation for GIAC Network security components

Security of the individual network components will be addressed in the following sections and steps:

- Securing the perimeter router
- Securing the Public Services Segment switch
- Securing the branch office through use of IOS Firewall and CBAC
- Providing for Primary and Secondary Firewalls at the head office
- Implementing an Intrusion Detection architecture
- Configuring Site-to-site VPNs for branch office connectivity
- Configuring a Remote Access VPN for remote worker access
- Hardening the Public Services Segment host Operating Systems
- Hardening SMTP/BIND/NTP/IIS applications
- Securing the GIAC internal network
- Auditing the network through the use of External Assessment and Vulnerability Analysis.

securing the perimeter router

Routers are packet switching hardware or software based devices running customized software that sit at the Network layer of the OSI model and forward (route) or accept/deny (filter) packets based on criteria defined in the routing tables and packet filtering rules configured on the device. Routers are needed to route data packets between source and destination hosts on different layer 2 networks. Routers also provide for a LAN/WAN or broadcast domain boundary. By their nature routers need to advertise networks and securing our perimeter router is critical to the overall security of the GIAC network. Our GIAC router is our first line of defense as a filtering device and should be suitably hardened. A well configured router will add greatly to the security of the GIAC network it services. Due to its placement at the edge of the GIAC corporate network the perimeter router is open to the full wrath of the Internet and should be hardened accordingly.

GIAC Perimeter Router Threat Mitigation

The software component of any hardware device is typically referred to as an Operating System. As with a server or desktop Operating System like Linux or Windows for example, a router OS needs constant maintenance through OS version upgrades and upfront hardening even before the device is placed at the edge of our network. GIAC Enterprises has chosen a Cisco 2620 router as its border filtering device at the head office and running IOS version 12.3. A number of excellent resources are available to assist us in hardening our Internet Attached Router. A few of these resources now follow.

Cisco Router Security Resources

- Cisco AutoSecure utility [3]
- Router hardening documents provided by the Center for Internet Security [4]
- The NSA provides a very comprehensive hardening document specifically related to Cisco Router Security configuration [5]
- SANS publishes a step-by-step guide to securing Cisco Routers [6]

Steps to secure the GIAC Perimeter router

At its highest level GIAC router threat mitigation steps will follow the following steps:

1. Ensure most up to date and stable IOS version loaded
2. Disable unused global and per interface router local services
3. Harden router interfaces
4. Provide for secure administrative access to the router
5. Use access lists to filter traffic on IP address and port number and apply anti-spoofing ACL's
6. Provide for logging
7. Take a backup of the router configuration file

The following table details the different IOS commands required to achieve the steps above under the different headings mentioned.

Security Recommendation	Cisco IOS Command
Router Password Security	
Encrypt passwords in router config file	service password encryption
Implement a minimum password length of eight characters.	security passwords min-length 8
sets the number of allowable unsuccessful login attempts to five and log violations	security authentication failure rate 5 log
Set an enable secret password	enable secret
Secure Management Access	
enable ssh for secure router access	transport input ssh
time out console & vty connections after 5 minutes	exec-timeout 5 0
apply an access list to control vty connections	access-class MANAGEMENT-IN in
Specify a password on a line	password
enable password checking at login against CSACS server	login authentication auth-hosts
Disable select ICMP messages	
disable ICMP host unreachables	no ip unreachables
disable ICMP mask reply	no ip mask-reply
Network Time Protocol	
Enable use of NTP for time synchronization	ntp server 172.16.1.5
disable use of router as ntp server	ntp disable
DNS lookup	
disable DNS domain lookup	no ip domain-lookup
Address Resolution Protocol	
disable gratuitous arps	no ip gratuitous-arps
disable proxy arp	no ip proxy-arp
Disabling router services	
disable router HTTP server	no ip http server no ip http server-secure
disable use of router as bootp server	no ip bootp server
disable the X.25 Packet Assembler/Disassembler service.	no service pad
Disable the finger service	no ip finger
disable DEC Maintenance Operation Protocol	no mop enabled
disable ident of user requesting services	no ip identd
disable tcp small servers	no service tcp-small-servers
disable udp small servers	no service udp-small-servers
disable cisco discovery protocol	no cdp run
disable use of router as ftp server	no ftp-server write-enable
Path Integrity	
disable source routing of IP packets	no ip source-route
disable ICMP redirects	no ip redirects

Securing the router configuration	
Prevent loading of router config from the network	no service config
Provide for backup of router config	copy run tftp
Secure the backup directory where the config is stored	By default tftp directory is world-writeable which is a security concern
Logging	
enable logging	logging on
set logging server	logging 172.16.3.2
log critical messages to console	logging console critical
log all level 0-6 messages to our syslog server	logging trap informational
log all level 0-6 messages to internal buffer	logging buffered informational
timestamp logging messages	service timestamps log datetime show-timezone msec
timestamp debug messages	service timestamps debug datetime show-timezone msec
Guard against DoS attacks	
only wait 15 seconds while attempting to complete the three way TCP handshake.	ip tcp synwait-time 15
test whether the other end of an open TCP connection is still open and has not crashed or otherwise terminated.	service tcp-keepalives-in service tcp-keepalives-out
protect against smurf amplification attacks.	no ip directed-broadcast ip verify unicast reverse-path
IOS version upgrades	
Ensure latest stable IOS release loaded	copy tftp flash
Legal	
set warning banner against unauthorized access	banner motd
Secure routing updates	
provide for authentication of routing updates from neighbor routers	ip authentication mode eigrp 100 md5 ip authentication key-chain eigrp 100 eigrp-key-chain
Interface shutdown	
disable unused interfaces	shutdown

Note: See Appendix I for the Guangzhou perimeter router configuration including the above hardening steps.

configuring Cisco IOS Access Control Lists

Up until now we have spoken about securing the GIAC router itself. We now turn our attention to configuring the router to secure the network behind it through Access Lists. Router Access Lists allow our administrator to implement the GIAC security policy by controlling access to traffic moving through the router to and from the GIAC network. On a Cisco router there are a number of different categories of Access List with increasing levels of functionality. These are Standard, Extended, Named and Reflexive. Standard Access Lists only allow filtering on source IP address. Extended Access Lists allow filtering on source IP, destination IP, protocol fields and port numbers. A named access list gives a meaningful name to an ACL and has the added benefit of allowing us to edit the ACL line by line. With standard and extended ACLs we must copy the ACL to a text editor, making changes offline and pasting the amended ACL back to the router. Reflexive ACLs add stateful features to a Cisco router by tracking incoming and outgoing sessions. Reflexive ACLs fall under the category of enhanced ACLs which also include time based and dynamic ACLs.

An access list can be implemented either inbound or outbound on an interface and compares a packet sequentially through each line of the ACL until a match is made. Once a match is found all processing of the ACL stops. An implicit default deny policy at the end of a Cisco ACL dictates that any traffic not matching an ACL entry is dropped. An explicit deny rule should be configured to provide for logging of traffic attempting to violate our policy. You can only apply a maximum of two access lists per protocol per interface. For example inbound IP, outbound IP, inbound and outbound IPX, etc. Inbound ACLs are processed before routing takes place and Outbound ACLs are processed after the routing process. Note that access lists don't filter traffic that originates from the router itself.

The following categories of traffic can be denied or permitted with ACLs.

- Protect against spoofing by applying ingress filtering[7] at your external interfaces and dropping traffic with a source IP in the IANA Reserved range, the Loopback address, multicast traffic and Private RFC1918 address space.
- Apply egress filtering to control outbound traffic from the GIAC network
- Block inbound and outbound protocol traffic which may lead to network compromise or leakage of network information.
- Provide granular control over both good and malicious ICMP traffic.
- Allow for inbound and outbound traffic as detailed in the security policy. For example outbound HTTP and inbound DNS queries and SMTP traffic.

A filter applied inbound is know as an Ingress filter while a filter applied outbound to an interface is know as an Egress filter. Let's look at both.

Ingress Filters

Ingress filtering refers to the filtering of traffic inbound to an interface. Filtering of inbound traffic to the interface connecting the GIAC network to its ISP is extremely important. Malicious individuals wishing to spoof their source IP address often use unallocated, reserved or private address space (also called bogon ranges). IP address spoofing is used to mask the source of attack packets. It is important that a network neither accept nor announce such ranges and contribute to the instability of the Internet or an attack against an Internet-connected device or network. As with disallowing IP Directed Broadcasts, filtering of the bogon IP space is considered part and parcel of being a conscientious net citizen. On our perimeter router we include ACL's to null route the offending bogon packets and send them to the proverbial bit-bucket. The term *bogon* has its roots in the hacker community and derives from the word bogus meaning something which is fake or not genuine.

Why ingress filtering? "Many ISPs and end user firewalls filter such traffic because they have no legitimate use, and are therefore the result of accidental or malicious misconfiguration at the sender".[8] The bogon lists change frequently and you are invited to keep an eye on Rob Thomas' Secure IOS Templates web page[9] or sign up for the bogon-announce mailing list[10]

You can also use routing instead of filtering to route packets to the null interface (null0) and give null routing priority over processing of ACLs which are more CPU intensive. You can take advantage of null routing by sending non-routable traffic to the null interface first and reducing the amount of traffic hitting the processor intensive ACLs. Having both black holing and ACL's also gives you a safeguard in case any traffic were to slip through the null routing commands although as mentioned you still require ACLs for logging and statistical purposes. Please reference the ACL section of the GIAC screening router for the running configuration in Appendix I with comprehensive comments for full details of the filtering syntax for the above address space.

Egress filters

Egress filtering is just as important as ingress filtering and entails only allowing outbound traffic with a source IP of our internal network. This prevents malicious users from spoofing their source IP if an internal machine is compromised. We apply egress filters outbound on the ISP facing interface. If a machine internal to the GIAC network is compromised it may be used as a launch pad for attacks against other networks or to send Spam.

securing the Public Services Segment Catalyst switch

The network architecture of a layer 2 switched environment is flat, meaning that anyone can potentially plug themselves into the nearest hub or switch and have access to the local network. All hubs and switches on a LAN are members of a single broadcast domain. Previously all the security was provided at the router. However we now have more granular control at layer 2 through the use of VLANs, Private VLANs and Port Security. VLANs create separate broadcast domains forcing security checks at the upper OSI layers. Our GIAC Protected DMZ switch is a Catalyst 2970E switch running Cisco IOS Software Release 12.1(14)EA1. With Cisco IOS release 12.1(14)EA1, the Catalyst 2970 now supports several new features previously only available on the higher end Catalyst 3550. GIAC is currently looking at wireless technologies and as external consultants we have suggested that some of the new features including Port ACLs, 802.1x Guest VLANs and 802.1x port security would be worth considering in the future.

configuring private VLANs

In our scenario Private VLANs are configured on the Public Services Segment switch. We will configure Private VLANs for our GIAC PSS switch to provide a method of isolating particular ports on our PVLAN compatible switch in an attempt to provide additional security to hosts on that switch. For example our PSS hosts: Web Server, DNS and SMTP servers are configured in a PVLAN configuration whereby the individual switch ports are isolated in an attempt to contain the possible compromise of one of the DMZ hosts. If a malicious attacker were to compromise the DNS server a PVLAN configuration would prevent the attacker from attacking the other hosts on that segment. The only communications path from the DNS server to any other host would be back through the primary Firewall. PVLANs are appropriate in this scenario as the HTTP, DNS and SMTP servers do not need to communicate with each other. PVLAN's are also called PVLAN Edge. Edge connections refer to ethernet connections to end-user devices, in this case our PSS servers. Due to the possibility of VLAN hopping it's recommended that a single switch not contain VLANs from different networks with different security levels. One caveat here before we continue: For companies using SPAN for IDS or Network Management and also using protected ports, SPAN only works if either the monitor port or the port being monitored is not a protected port.[11] The monitor port must not configured as a protected port.

configuring Port Security

Another method of securing switch ports is called Port security which entails setting one MAC address in the MAC address table of each port. Port security helps guard against MAC overflow attacks against the switch. Tools such as *dsniff* by Dug Sung and specifically the *macof* utility attempt to overflow the switch MAC/CAM table and fail the switch open allowing sniffing of switch ports.[12] Appendix III details the commands required to enable port security on a particular switch port[13] and the resulting switch configuration.

securing GIAC Branch Office connectivity

To effectively secure a remote office you would typically need to provide for a Router, Firewall, Intrusion Detection System and VPN device at the remote site.[14] The monetary expense and added complexity would quickly overwhelm GIAC Enterprises' technology budget and existing support staff. GIAC Enterprises has determined that purchasing a single routing device which integrates the above functionality would be the most appropriate approach. The Cisco IOS Firewall and VPN Feature set was chosen to provide Routing, VPN, IDS and Firewalling capabilities for GIAC's remote offices. An IOS Firewall Router was chosen over a PIX Firewall due to the small office size, no requirement for DMZs, low budget and only a requirement for hide NAT.

CBAC or Context Based Access Control enables our branch office routers to act like a PIX Firewall by providing stateful inspection of network, transport and application layer protocols. This is achieved by running the IOS Firewall Feature Set on the router. In addition the Firewall feature set provides the ability to log to a remote Syslog server, Java Applet blocking, DoS and Intrusion detection and prevention and real-time alerting and auditing. The IOS Firewall also has the ability to look at application layer protocols. CBAC doesn't provide access control for all protocols as would a PIX firewall but only for protocols you define when you configure CBAC on your router. CBAC works together with router ACLs and inspects traffic not denied by the ACL. Since the GIAC branch office router will also be one end of a VPN tunnel to the Head office we add a VPN Accelerator card (VAC+) to offload heavy duty encryption/decryption from the normal routing/packet filtering role of the router. The VAC+ handles the tasks related to IPSec including encryption/decryption, one-way hash computation, key exchange and SA storage. We consider terminating the VPN tunnel on the 2600 router an acceptable performance hit due to the small number of users in the remote offices. The head office end of the VPN tunnel peer is terminated at the PIX Firewall.

configuring the Cisco IOS Firewall

Let's look at an overview of the steps required to configure CBAC for Stateful Inspection and filtering. See Appendix I for full details of the CBAC config.

1. Determine interfaces to monitor with CBAC
2. Configure access list for that interface
3. Configure CBAC timers and threshold levels
4. Define IP traffic to be monitored using Inspection Rule
5. Apply Inspection Rule to interfaces determined in point 1 above
6. Finally configure logging and audit trails

Since we terminate our VPN connection on this router we can use CBAC to inspect traffic both before entering the VPN tunnel and after leaving the tunnel. We cannot however use CBAC to inspect IPSec encrypted packets between the GIAC head office and our branch offices. Cisco now refers to the IOS Firewall under the heading *Cisco Secure Integrated Software*.

Providing for Primary and Secondary Firewalls at the head office

A Firewall creates our security boundary between the Internet and the GIAC corporate network. A security boundary may be defined as "the line of intersection between two areas, subnets or environments that have different security requirements or needs".[15] The corporate Firewall acts as a choke point for traffic traveling between these two intersecting networks. It also provides a focus for implementation of our security policy. Having identified a security boundary we need to deploy controls and mechanisms to control the flow of information across these boundaries. Firewalls may be categorized as Packet Filters i.e. a Cisco router, Firewalls implementing Stateful Inspection (a term coined by Checkpoint in 1993[16]), Application Proxies and newer SI Firewalling technology with built in Application Protocol awareness as with the newest Checkpoint Firewall-1 NG-AI product. Some newer firewalling technologies include Deep Packet Inspection which migrates some features of IDS technology to the Firewall, namely the ability to inspect the data portion of packets passing its interfaces. Our Cisco PIX is a Stateful Inspection Firewall. When a firewall is said to "keep state" it stores information about the relationship between packets currently passing its interfaces and packets previously passing the same interface. It does this through the use of a state table. Let's now look at the dual Firewall architecture which GIAC Enterprises will implement.

primary Firewall

The primary Firewall is the Firewall directly behind the perimeter router. The Cisco PIX 515E Firewall was chosen as the primary firewall for GIAC. The PIX 501 and 506E do not allow configuration of DMZ segments so based on the size of GIAC Enterprises and the architecture requirements the PIX 515E was deemed the most suitable model. The 515E was purchased with an additional 4 port interface card which was added to slot 1. The 515E has two card slots and additional cards and interfaces are numbered from top to bottom and from left to right on the same card.

secondary Firewall

A secondary firewall is not mandatory in any Network Perimeter architecture design but it does add an added level of security for more sensitive environments. Choosing a different product adds to the support load on the security staff and added complexity to the environment but this is the tradeoff for the additional security of dissimilar Firewall architectures for the primary and secondary Firewalls. For the purposes of our GIAC network security architecture we will implement a secondary firewall in the form of Checkpoint Firewall-1 NG. This secondary Firewall will provide additional protection for the internal network while also providing Management and Database segments to protect our CiscoWorks management station and the fortune's database respectively. This means that an attacker now has two levels of Firewalls to penetrate before reaching client data on our database server.

implementing an Intrusion Detection architecture

There are two categories of IDS – the Network IDS and the Host IDS. On the GIAC network we have chosen the open source Snort IDS product for use as our Network Intrusion Detection sensor to be placed in strategic positions across our network; namely on our Public Services Segment, our Database and Application segments and on the internal network. Each Snort sensor is installed with two NICs. One (sniffing) is plugged into our NetOptics inline TAP and the other (Command and Control) to the switch on which the IDS console is connected. The sniffing interface is not given an IP address and is configured in so-called *stealth mode*, the premise being if you can't see the device you can't attack it. We will use SGUIL[17] as our IDS console. The SGUIL console will live on our Management segment. A Host IDS in comparison is installed directly to a host machine and interacts primarily with that system's logs and alerts on registry or file system changes. GIAC has evaluated the Cisco Security Agent but as yet have not implemented a host IDS solution on the network. Our nIDS sensors are tuned with a specific set of signatures relevant to the segment they are monitoring. We also enable Snort active response by compiling Snort with the *flexresp* switch as below.

```
foo#./Configure -enable-flexresp
```

This allows resetting of TCP and UDP packets through use of TCP resets and ICMP unreachables respectively.[18] We won't be implementing any mechanism to auto modify our router or PIX ACLs in response to malicious traffic due to the danger of blocking normal traffic. A random source MAC address is generated when TCP resets are sent to further disguise the presence of the IDS. As with any signature based system we need to allow for the regular update of our IDS signatures. We will use the Oinkmaster[19] Perl script to update our Snort Rules.

Inline TAP versus SPAN port

A TAP sits inline between a router, switch or firewall and provides an access port into which a monitoring device like our IDS is plugged. GIAC chose to use an inline TAP instead of a switch SPAN port for IDS monitoring due to accepted issues with using a SPAN port. These issues with SPAN include missing packets thru aggregation of ports on switches with heavy traffic loads. It's also possible that the switch will filter over/undersized or corrupt packets. The IDS can only monitor packets sent to the SPAN port so it is possible for a malicious packet to reach an end host but not make it to the SPAN port. TAPs also eliminate the delay inherent in mirroring traffic to a SPAN port. In addition port mirroring through use of SPAN presents additional problems because it does not receive VLAN information and only presents one side of a full-duplex connection.[20] A final soft benefit of a tap over SPAN is the avoidance of problems where security owns the IDS infrastructure and the networking group owns the switch fabric and may not take kindly to handing over valuable switch ports to the security group. Both groups have different goals i.e. availability versus security.[21]

configuring Site-to-Site and Remote access VPNs for branch office and remote worker connectivity

We must allow users at our branch offices and remote users to access email and our corporate Intranet both located at our head office. We configure the head office PIX Firewall and the branch office Cisco router as VPN peers to create a secure VPN gateway between each of these two networks. IPSec tunnel mode is used between both peers. We will terminate all four branch offices VPN tunnels and our Remote Access VPN tunnel on the outside interface of our Hong Kong PIX. Appendix II of this document details the full head office PIX Firewall configuration.

To enable creation of the initial secure channel between our IPSec peers we must allow for UDP port 500 IKE traffic to the PIX and once the IKE Security Association has been established we must allow for port 50 ESP Protocol to create the IPSec tunnel. Encapsulating Security Payload or ESP provides for the confidentiality of GIAC data between VPN peers by encrypting the payload of IP packets between the head office and branch offices or Remote Workers. Our Security Policy requires use of 3DES (168bit) encryption, MD5 hash algorithm (HMAC variant), pre-shared keys for authentication, Diffie-Helman Group 5 for secure key exchange and a Security Association Lifetime of 86,400 seconds or 1 day.

Since many of our sales staff tend to spend the majority of their time on the road it makes sense to have a remote access facility available to them to access their email and the corporate Intranet. The Cisco VPN software client is loaded on each road warrior laptop allowing the user to connect back to the head office over a secure VPN connection. Our PIX Firewall is configured as the other side of the VPN connection between these remote clients. Information regarding internal WINS and DNS servers is pushed to the VPN client on establishing a connection with the PIX.

hardening the Public Services Segment host Operating System

UNIX hosts

It is also necessary to harden each PSS host, also called a Bastion host. For Linux systems Jay Beale provides a set of hardening scripts known as the "Bastille Linux Project". You also have the option of referencing and using free of charge the hardening guidelines provided by the Centre for Internet Security as referenced earlier in the section on Cisco IOS hardening. The latter site provides both a list of benchmarks for hardening a Linux host (among others) and a non-intrusive scanning tool scoring the security of the Linux box against the former Benchmarks. For this exercise we have chosen to use the Bastille Linux script. GIAC uses Linux for it's Bind external DNS server, for the Network Time Protocol (NTP) server and for its Snort nIDS sensor. Any publicly accessible host should be hardening before being placed on the network. In addition to hardening the OS we must also harden the underlying application. For example our external DNS server requires locking down the UNIX OS and also hardening the BIND application itself.

Microsoft Windows hosts

In the past shipping an Operating System in a default open configuration has had the advantage of cutting down on support calls and providing a default configuration with all services running which covers pretty much all user's needs. As time passed the disadvantages of shipping such an open config became obvious and vendors started to ship services turned off by default. To assist in hardening a Microsoft Windows system there are many sources of information on the Internet both from Microsoft and third party organizations. Microsoft provides a lot of useful security information on their website.[22]
The full set of steps required to harden a Windows 2000 host can be found at the following site.[23] As an overview the hardening steps are as follows:

- Apply all of the most recent OS support packs and any additional roll-up security patches released since the latest support pack
- Shut down unneeded Windows services.
- Change default passwords and disable unneeded or unused accounts
- Implement (and enforce) a password policy
- Enable Auditing/Logging
- Enable Access Control through File/Directory permissions and adhere to the concept of least privilege
- Keep OS patches up to date by implementing a patch management solution using products such as Shavlik HFNetChck or St. Bernard Update Expert.

A host must be hardening before it is connected to the network. The time taken to compromise an unhardened system connected to the internet is often less than the time taken to download the necessary patches from the relevant update sites. Either download the patches to another pre-hardened admin workstation or install a software firewall on the host to be hardened before connecting to the internet. Let's look very briefly at how we would harden the different server applications on the PSS.

hardening the SMTP Relay application

Our GIAC external SMTP Relay runs the Exim MTA. Briefly some of the steps we might take to secure the SMTP application would be to ensure we only relay mail for our own domains, ensure we are not configured as an open mail relay, disable version banners and SMTP Help, implement DNS reverse lookup to combat SPAM and of course install anti-virus software on all mail servers.

hardening the BIND DNS application

There are also a number of steps we can take to secure the DNS BIND application. We implement a split DNS architecture (explained below) and use different DNS applications for internal and external servers; ISC Bind for external DNS and Microsoft DNS for internal. We configure the internal DNS to forward all unresolved queries to the external DNS. From there any unresolved queries are forwarded to the root DNS. We disable DNS recursive queries on the external DNS server. We provide for a Secondary DNS at the ISP site and only allow zone transfers to authorized hosts. We also have the option of using Transaction Signatures (TSIG) to authenticate servers for DNS zone transfers. We prevent external hosts from querying the Bind version (through /etc/named.conf file) and finally we take a regular backup of our DNS configuration files from the server.

hardening the NTP Application

Time is a critical element of any network design. Time allows us to correlate events across different network hosts and devices for purposes of Network Management, Incident Response and other time sensitive applications. We run the Linux NTP daemon on our Public Services Segment. The NTP server synchronizes with an external NTP source and in turn our internal hosts and network devices poll the internal NTP server for the correct time and adjust their clocks accordingly. We have already hardened the underlying Linux OS by downloading and running the Bastille Linux scripts. We then download and install the latest Linux NTP server RPM from rpmfind.net The latest version for RHL 9 at the time of writing is *ntp-4.1.2-0.rc1.2.i386.rpm*. We will use the NTP server maintained by the Chinese University of Hong Kong at 137.189.8.137: ntp.cuhk.edu.hk. This clock services Hong Kong, China, and South East Asia. To secure our NTP server we restrict the clients that can use our NTP server to sync time. We also restrict the type of access that the cuhk server has to our NTP server by editing the */etc/ntp.conf* file on the server.

hardening the Microsoft IIS Web Server

Make sure we apply the latest patches from Microsoft and keep up-to-date on new IIS vulnerabilities. We disable unneeded ISAPI filters and extensions and consider running the *IISLockdown* tool. We also try to run services with non-admin or least privilege accounts to contain damage if compromised.

Implementing a Split DNS architecture

As mentioned above GIAC implements a split DNS architecture. The GIAC external DNS server only contains records for the publicly accessible hosts namely our SMTP, WWW and DNS servers. Using the same server for both external and internal DNS requests is a security risk as it could expose the structure of the internal network to outsiders. Also it means an internal user must loop back in through the firewall to hit the external DNS to query the IP of the GIAC web server. With a split DNS architecture we create two zones for the same domain. Both internal and external zones must be located on different physical servers. GIAC external DNS /etc/named.conf file contains configuration settings for the BIND DNS server.

auditing the GIAC Network

External Assessment

GIAC engages a third-party professional consulting firm to perform an external assessment of the network on a yearly basis to test the effectiveness of its safeguards. Having a penetration test performed is akin to going to the doctor for a medical checkup. The aim is to determine whether you/your network is as healthy/secure as you think. A consulting firm may use a combination of automated and manual testing methods to perform external assessment work. An open source framework for external assessment is available through the OSSTMM or Open Source Security Testers Methodology Manual.[24] GIAC includes its Fortune's application and database environment in its external assessment scope. After securing the GIAC environment it's important to keep it healthy with continued self-assessments. Quarterly internal vulnerability assessments are stipulated at GIAC and are similar to exercising and good diet between medical checkups. We try not to focus on the technical findings of a pen test as a measure of the security or lack of in our security posture rather flaws discovered during a pen test should be considered symptomatic of procedural shortcomings in the systems management process and investigated from this standpoint.[25]

Vulnerability Assessment

Applications have services, services have vulnerabilities and vulnerabilities may be exploited by malicious individuals. Services run on port numbers and most services can be identified by a particular port number. In programming terms a port is a memory address space. Since there are 65,535 UDP ports and a similar number of TCP ports both protocols have separate address spaces. The term given to finding vulnerabilities in your network is Vulnerability Assessment or VA. GIAC uses a combination of Open Source and commercial VA tools including Nessus and ISS Internet Scanner and the Router Auditing Tool (RAT) for PIX and Cisco router auditing. It is generally advised that more than one tool be used so that results can be cross-correlated. Vulnerability Assessment is a dynamic exercise and is carried out by GIAC on a quarterly basis or sooner if following changes to the network or host configuration. The GIAC Vulnerability assessment policy dictates procedures for informing asset owners of the tools, timing and frequency of assessments including internal asset owners and external clients. Included in the policy are steps to take in case of outages caused by the VA process

securing the GIAC Internal Network

Defense in depth is a term coined by the DoD in late 1990 and provides for multiple layers of security rather than depending on a single security solution. How many times have you heard "It's ok we're secure. We have a Firewall!". A misconfigured Firewall however is sometimes worse than no Firewall at all as it gives a false sense of security. People also say there's no bad security product only a badly implemented one. In an architecture implemented using defense in depth we also need to provide for the security of the internal network including desktop virus protection, patch management, personal firewalls and server backups. Our GIAC product of choice for desktop antivirus is Mcafee Viruscan. We also load Mcafee Netshield on all File and Messaging servers and we use the Sybari Antigen[26] product to scan mailboxes and incoming/outgoing email on the Hong Kong Exchange 2000 Message Store. Automatic Antigen signature updates are triggered each night at 3am. We back up all critical servers using the Backup Exec product. Finally to complete our defense in depth architecture we configure a personal firewall on each client desktop. We have chosen the BlackIce product from ISS. It is important to keep internal systems up to date with new OS and application patches as they are released. This can prove to be a daunting task for System Administrators especially in large organizations. All patches are first tested on non-production machines before being rolled out in the GIAC environment. GIAC uses the St. Bernard Update Expert product for patch management. GIAC has gathered a CIRT to enhance the effectiveness of the existing GIAC security policy by implementing a basic incident response policy and creating an Incident Response team.

providing awareness training to GIAC staff

There's a popular belief that with enough security awareness training security professionals can train their users to be security-aware citizens. This is only true to a certain extent and we still need to rely on security controls for example to prevent users from double clicking email attachments. "Given the choice between dancing pigs and security, the user will choose dancing pigs every time"[27] We need to remove the human variable from computer security as much as possible. Security Awareness training is provided to all GIAC staff.

implementing physical and environmental controls

Finally although securing network devices through software configuration is a necessity it is really game over if you don't also provide for the physical security of the network infrastructure devices and a malicious individual gains access to your machine room. GIAC networking equipment and servers are secured in a machine-room accessible only to authorized staff and only through the use of a swipe card and key pad. A log book is provided for all visitor access which should also be escorted. This is laid down in the GIAC Enterprises security policy document. GIAC also implements environmental controls in the form of CRAC Aircon and FM200 Fire suppression systems in its computer room facility.

references

[1] Zeltser, Lenny. Firewall Deployment for Multitier Applications.
http://www.zeltser.com/multi-firewall/

[2] SANS Security Policy Project.
http://www.sans.org/resources/policies/

[3] Cisco AutoSecure.
http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/cas11_ds.pdf

[4] Centre for Internet Security. Cisco Benchmarks.
http://www.cisecurity.com/bench_cisco.html

[5] NSA Security Recommendation Guides.
http://nsa2.www.conxion.com/cisco/download.htm

[6] SANS Press. Securing Cisco Routers: Step-by-Step.
https://store.sans.org/store_item.php?item=70

[7] RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.
http://www.faqs.org/rfcs/rfc2827.html

[8] Thomas, Rob. Bogon Reference Page.
http://www.cymru.com/Bogons

[9] Thomas, Rob. Secure IOS Template.
http://www.cymru.com/Documents/secure-ios-template.html

[10] Bogon Announcement List.
http://puck.nether.net/mailman/listinfo/bogon-announce

[11] Catalyst 2900 XL and Catalyst 3500 XL Software Configuration Guide.
http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007e83c.html#1028477

[12] Sung, Dug. Dsniff suite.
http://www.monkey.org/~dugsong/dsniff/

[13] Configuring Port Security on the Cisco Catalyst 2900XL.
http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007e838.html#xtocid18

[14] Cisco Systems. Securing the Branch office Network.
http://www.cisco.com/en/US/netsol/ns477/networking_solutions_white_paper0900aecd80162f0e.shtml

[15] Harris, Shon. CISSP Study Guide
http://books.mcgraw-hill.com/getbook.php?isbn=0072257121&template=&PHPSESSID=d3e2eeb0a1854d99df6e3675aded6ef5

[16] Checkpoint Press Release. Checkpoint awarded patent for Stateful Inspection technology.
http://www.checkpoint.com/press/1997/patent2.html

[17] SGUIL. Snort GUI for Lamerz.
http://sguil.sourceforge.net/

[18] SANS Institute. IDS FAQ. What is Active Response?
http://www.sans.org/resources/idfaq/active.php

[19] Oinkmaster.
http://oinkmaster.sourceforge.net/

[20] Cisco Systems. Incident Handling.
http://www.ciscopress.com/content/downloads/cisco/1587051176ch08.pdf

[21] NetOptics whitepaper. “Technology Overview: Tap and Span port comparison”.
http://www.netoptics.com/support/white_paper.asp?Section=support

[22] Microsoft Windows Security website.
http://www.microsoft.com/security

[23] Windows 2000 Security Hardening Guide
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

[24] Herzog, Pete. The Open Source Security Testers Methodology Manual.
http://www.isecom.org/osstmm/

[25] Van Wyk, Kenneth. Finding the Elusive Value in Penetration Testing.
http://www.esecurityplanet.com/views/article.php/3392151

[26] MSNBC News. Microsoft Purchases Sybari.
http://www.msnbc.msn.com/id/6935137/

[27] Felton, Edward Prof. Princeton University.*
www.ruxcon.org.au/files/2004/14-daniel_lewkovitz.pdf

** Referenced in the paper “Social Engineering (or the gentle art of having others hurt themselves for your amusement)” by Daniel M. Lewkovitz. (Page 6).*

Assignment 3
the GIAC Firewall policy

implementing policy through the use of Firewall rules

Our Firewall rules implement the GIAC Enterprises security policy. The PIX Firewall implements policy through the use of Access Control Lists (ACLs) or conduits depending on the version of PIX software used. Before a PIX is configured it has a default deny-all policy both for inbound and outbound connections. By configuring dynamic NAT we allow inside hosts to make outbound connections. However, all inbound connections from the Outside are still denied until an ACL is applied to the external interface to allow inbound connections.

One point to note about an Acess Control List on a PIX is that any return traffic does not require an ACL if it is part of an already established connection. The PIX keeps track of established connections through its connection table. This is commonly referred to as keeping state. There is also a common misconception that egress or outbound filtering prevents return traffic from an already established connection but this is a misnomer. GIAC employs a default deny-all access policy common for commercial organizations whereby we default to the tightest configuration available initially, then gradually open things up when our security issues and defenses are better understood.[1]

On the PIX Firewall each interface is assigned a security level represented by a number between 0 and 100. The inside interface is typically assigned security level 100 while the outside interface is assigned a security level of 0 with all other interfaces given a security level between these numbers. An interface is either a higher or lower security level relative to any other interface with the higher numbered interface considered the more trusted. For example a *Security50* level is considered more trusted than a *Security0* level. Also an interface is considered “inside” in relation to any other interface with a lower security level and an interface is considered “outside” to another interface with a higher security level.

The general rule of thumb states that an interface with a higher security level can access an interface with a lower security level and likewise an interface with a lower security level *cannot* access an interface with a higher level (unless we explicitly configure it to allow such access). Interfaces with the same security level cannot communicate with each other. As mentioned earlier our GIAC PIX outside and inside interfaces are configured with their default security levels of 0 and 100 respectively. Our Public Services Segment security level is set at 50 and the Application segment set at 40.

Network Address Translation (NAT)

It's worth briefly mentioning the role of NAT in conjunction with PIX ACLs. Network Address Translation is the process of readdressing packets so that they appear to originate from a different host IP address. Since only publicly routable IP addresses are allowed on the Internet and the number of such IPs is limited NAT allows us to use a small pool of routable addresses for all outgoing sessions. It also provides some limited security by hiding the company's internal addressing scheme. The PIX *nat* and *global* commands work together to provide NAT and PAT. The *nat* and *global* commands are paired using a corresponding Nat ID. The *nat (inside)* command details the inside GIAC network range eligible for translation. In brief the nat and global commands allow a higher security interface to speak to a lower security interface and the *static* command with a corresponding access list allows the lower security level interface to talk back. Finally, although a nat/global combination doesn't require an ACL to function it is recommended practice that you do apply an ACL to inbound traffic. We commented earlier in this paper that on a PIX all ACLs are inbound. The PIX doesn't support outbound ACLs as does a Cisco IOS-based router.

the GIAC Enterprises Firewall Ruleset

Our GIAC Cisco PIX Firewall has four interfaces so we are looking at four inbound traffic flows which must be accounted for in the Firewall rules configuration. These four information flows are as follows:

FROM-OUTSIDE
inbound to the outside interface from the Internet

We must allow outside access from the Internet to services on our public services segment, namely the ability to browse our corporate web server, send email to our external mail server and query our external DNS server. We also must provide a way for our external NTP server to communicate with a public time source. We must allow inbound Syslog and SNMP trap messages from our screening router bound for the Ciscoworks console.

FROM-PSS
inbound to the Public Services Segment interface from the PSS itself

The corporate web server must be able to communicate with the ASP.NET application server on our application segment and in turn the application server must be able to query the backend SQL database on the Database segment.[2] We must configure the PIX to allow DCOM and RPC traffic between the Web server and the Application server. We also need to allow Netbios port 139 for Windows authentication. Finally we must also allow our public services segment hosts to send syslog messages to our management console on the management segment. The Management segment is also off the secondary Checkpoint Firewall.

FROM-INSIDE
inbound to the inside interface from the GIAC Internal network

All internal employees must be able to browse the internet and must be able to browse the corporate web server on our public services segment. We must also allow for SSH administration from our Management segment to our public services segment hosts and to our Firewall and screening router.

FROM-APP
inbound to the Application interface from the Application segment

The application server on our application segment must be able to query the back end SQL database on the database segment behind the secondary firewall. We need to open Distributed Transaction Coordinator (DTC) and RPC ports to allow communiction between the Application server and the SQL Database server.

characteristics of a firewall ruleset

There are a number of characteristics of a PIX Firewall ruleset which are worth remembering. Many of these traits equally apply to other vendor Firewalls.

1. Firstly rules are parsed sequentially from top to bottom. Once a match is made processing of a ruleset or ACL stops. Rule order is important for this reason. More explicit rules should be placed near the top with more general rules towards the bottom. This prevents a more general rule overriding an explicit rule further than the ACL.
2. ACL's are processor intensive. To ease processing time for ACL's, try to place rules with most hits near the top if possible. The show access-list command on the PIX shows a hit counter for each ACL entry. The Cisco PIX uses the concept of turbo ACLs to speed up processing of large ACLs.
3. A Cisco ACL has a default implicit deny rule at its end. It is recommended to add an "explicit" deny rule and log traffic attempting to violate the Firewall policy.
4. If you are not comfortable with the PIX command line interface the PIX Device Manager (PDM) can be used to provide a graphical interface when building Access Lists, Network Address Translation and VPNs.
5. An interface with an ACL applied to it where the ACL does not exist has a default allow policy.
6. When updating an ACL always do a *no access-list* command first to remove the ACL from the interface.

The tables on the following pages detail each of the inbound Access Control Lists on the GIAC Firewall. Each table includes three sections:

Source and destination interfaces followed by source and destination IP addresses or networks, protocol and port numbers and whether the rule is a permit or deny.

Rule No.	Source	Destination Interface	Source IP/Network	Destination IP/Network	Application Protocol	Network Protocol	Dest Port	Action
1.	Internet	Outside	Any	172.16.1.2	HTTP	TCP	80	Permit

Followed by an english language description of the purpose of the rule.

Rule No.	Rule Description
1.	Allow any outside host to access the corporate web server over http on tcp port 80

and finally the PIX syntax for the access list command as it would look in the PIX configuration.

Rule No.	PIX Access List configuration
1.	access-list FROM-OUTSIDE permit tcp any host 172.16.1.2 eq 80

GIAC PIX Access Control Lists

FROM-OUTSIDE (Inbound to the Outside interface from the Internet)

Rule No.	Source	Destination Interface	Source IP/Network	Destination IP/Network	Application Protocol	Network Protocol	Dest Port	Action
1.	Internet	Outside	Any	172.16.1.2	HTTP	TCP	80	Permit
2.	Internet	Outside	Any	172.16.1.2	HTTPS	TCP	443	Permit
3.	Internet	Outside	Any	172.16.1.3	DNS	TCP	53	Permit
4.	Internet	Outside	Any	172.16.1.3	DNS	UDP	53	Permit
5.	Internet	Outside	Any	172.16.1.4	SMTP	TCP	25	Permit
6.	Internet	Outside	209.99.1.1	172.16.1.9	SSH	TCP	22	Permit
	Internet	Outside	210.22.34.1	172.16.1.9	SSH	TCP	22	Permit
7.	Router	Outside	202.168.2.1	172.16.3.2	SNMP	UDP	161 162	Permit
8.	Router	Outside	202.168.2.1	172.16.3.2	Syslog	UDP	514	Permit
9.	Internet	Outside	203.168.3.1	202.168.2.2	IKE	UDP	500	Permit
10.	Internet	Outside	204.168.4.1	202.168.2.2	IKE	UDP	500	Permit
11.	Internet	Outside	205.168.5.1	202.168.2.2	IKE	UDP	500	Permit
12.	Internet	Outside	206.168.6.1	202.168.2.2	IKE	UDP	500	Permit
13.	Internet	Outside	100.1.2.3	202.168.2.2	IKE	UDP	500	Permit
14.	Internet	Outside	203.168.3.1	202.168.2.2	ESP	TCP	50	Permit
15.	Internet	Outside	204.168.4.1	202.168.2.2	ESP	TCP	50	Permit
16.	Internet	Outside	205.168.5.1	202.168.2.2	ESP	TCP	50	Permit
17.	Internet	Outside	206.168.6.1	202.168.2.2	ESP	TCP	50	Permit
18.	Internet	Outside	100.1.2.3	202.168.2.2	ESP	TCP	50	Permit
19.	Any	Any	Any	Any	Any	Any	Any	Deny

Rule No.	Rule Description
1.	Allow any outside host to access the corporate web server over http on tcp port 80
2.	Allow any outside host to access the corporate web server over https on tcp port 443
3.	Allow any outside host to make a DNS query to the GIAC external DNS on udp port 53
4.	Allow any outside host to make a DNS query to the GIAC external DNS on tcp port 53 *
5.	Allow any outside SMTP server to send mail to the GIAC external mail server on tcp port 25
6.	Allow partner/supplier to access SSH server to upload Fortune Sayings/Translations.
7.	Allow SNMP from Perimeter router to Management console
8.	Allow Syslog from Perimeter router to Management console
9.	Internet Key Exchange (IKE) inbound from Guangzhou branch office (create IKE SA)
10.	Internet Key Exchange (IKE) inbound from Brisbane branch office (create IKE SA)
11.	Internet Key Exchange (IKE) inbound from San Francisco branch office (create IKE SA)
12.	Internet Key Exchange (IKE) inbound from Dublin branch office (create IKE SA)
13.	Internet Key Exchange (IKE) inbound from Partner (create IKE SA)
14.	Encapsulating Security Payload (ESP) from Guangzhou branch office (create IPSec SA)
15.	Encapsulating Security Payload (ESP) from Brisbane branch office (create IPSec SA)
16.	Encapsulating Security Payload (ESP) from San Francisco branch office (create IPSec SA)
17.	Encapsulating Security Payload (ESP) from Dublin branch office (create IPSec SA)
18.	Encapsulating Security Payload (ESP) from Partner (create IPSec SA)
19.	Default Deny All Rule

Rule No.	PIX Access List configuration
1.	access-list FROM-OUTSIDE permit tcp any host 172.16.1.2 eq 80
2.	access-list FROM-OUTSIDE permit tcp any host 172.16.1.2 eq 443
3.	access-list FROM-OUTSIDE permit tcp any host 172.16.1.3 eq 53
4.	access-list FROM-OUTSIDE permit udp any host 172.16.1.3 eq 53
5.	access-list FROM-OUTSIDE permit tcp any host 172.16.1.4 eq 25
6.	access-list FROM-OUTSIDE permit tcp host 209.99.1.1 host 172.16.1.9 eq ssh access-list FROM-OUTSIDE permit tcp host 210.22.34.1 host 172.16.1.9 eq ssh

```
7.    access-list FROM-OUTSIDE permit udp host 202.168.2.1 host 172.16.3.2 range snmp snmptrap
8.    access-list FROM-OUTSIDE permit udp host 202.168.2.1 host 172.16.3.2 eq syslog
9.    access-list FROM-OUTSIDE permit udp host 203.168.3.1 host 202.168.2.2 eq 500
10.   access-list FROM-OUTSIDE permit udp host 204.168.4.1 host 202.168.2.2 eq 500
11.   access-list FROM-OUTSIDE permit udp host 205.168.5.1 host 202.168.2.2 eq 500
12    access-list FROM-OUTSIDE permit udp host 206.168.6.1 host 202.168.2.2 eq 500
13    access-list FROM-OUTSIDE permit udp host 100.1.2.3 host 202.168.2.2 eq 500
14    access-list FROM-OUTSIDE permit esp host 203.168.3.1 host 202.168.2.2
15    access-list FROM-OUTSIDE permit esp host 204.168.3.1 host 202.168.2.2
16    access-list FROM-OUTSIDE permit esp host 205.168.3.1 host 202.168.2.2
17    access-list FROM-OUTSIDE permit esp host 206.168.6.1 host 202.168.2.2
18    access-list FROM-OUTSIDE permit esp host 100.1.2.3 host 202.168.2.2
19    access-list FROM-OUTSIDE deny ip any any log
      access-group FROM-OUTSIDE in interface outside
```

* tcp used for zone transfers or reissue of original UDP DNS query where query results greater than 512K.

FROM-PSS (Inbound to Public Services Segment interface from the PSS itself)

Rule No.	Source Interface	Destination Interface	Source IP/Network	Destination IP/Network	Application Protocol	Network Protocol	Dest Port	Action
1.	PSS	Inside	172.16.1.4	10.0.1.5	SMTP	TCP	25	Permit
2.	PSS	Outside	172.16.1.5	137.189.6.18	NTP	UDP	123	Permit
3.	PSS	Outside	172.16.1.3	Any	DNS DNS	*UDP* *TCP*	53 53	Permit Permit
4.	PSS	Outside	172.16.1.3	202.100.1.2	DNS	TCP	53	Permit
5.	PSS	Application	172.16.1.2	172.16.2.2	RPC DCOM	TCP	135 5000 to 5020	Permit
6.	PSS	Application	172.16.1.2	172.16.2.2	Netbios	TCP	139	Permit
7.	PSS	Inside	172.16.1.2	172.16.3.2	Syslog	UDP	514	Permit
8.	PSS	Inside	172.16.1.3	172.16.3.2	Syslog	UDP	514	Permit
9.	PSS	Inside	172.16.1.4	172.16.3.2	Syslog	UDP	514	Permit
10.	PSS	Inside	172.16.1.5	172.16.3.2	Syslog	UDP	514	Permit
11.	PSS	Inside	172.16.1.7	172.16.3.2	Syslog	UDP	514	Permit
12.	Any	Any	Any	Any	Any	Any	Any	Deny

Rule No.	Rule Description
1.	Allow PSS SMTP server to access Internal SMTP server for mail relay
2.	Allow PSS NTP server to synchronize with external time source at Chinese Uni Hong Kong
3.	Allow PSS External DNS to forward unresolved DNS queries from internal DNS to Root DNS
4.	Allow DNS zone transfers with secondary DNS server hosted by ISP
5.	Allow RPC and DCOM traffic between the Web server and the Application server
6.	Allow port 139 for Windows authentication between Web server and App server (non-AD environments).
7.	Allow syslog messages from Corporate Web server to Management console
8.	Allow syslog messages from External DNS to Management console
9.	Allow syslog messages from SMTP Relay to Management console
10.	Allow syslog messages from NTP server to Management console
11.	Allow syslog messages from DMZ switch to Management console
12.	Default deny all

Rule No.	PIX Access List configuration
1.	access-list FROM-PSS permit tcp host 172.16.1.4 host 10.0.1.5 eq 25
2.	access-list FROM-PSS permit udp host 172.16.1.5 host 137.189.6.18 eq 123
3.	access-list FROM-PSS permit udp host 172.16.1.3 any eq 53 access-list FROM-PSS permit tcp host 172.16.1.3 any eq 53
4	access-list FROM-PSS permit tcp host 172.16.1.3 host 202.100.1.2 eq 53
5.	access-list FROM-PSS permit tcp host 172.16.1.2 host 172.16.2.2 eq 135 access-list FROM-PSS permit tcp host 172.16.1.2 host 172.16.2.2 range 5000 5020
6.	access-list FROM-PSS permit tcp host 172.16.1.2 host 172.16.2.2 eq 139
7.	access-list FROM-PSS permit udp host 172.16.1.2 host 172.16.3.2 eq 514
8.	access-list FROM-PSS permit udp host 172.16.1.3 host 172.16.3.2 eq 514
9.	access-list FROM-PSS permit udp host 172.16.1.4 host 172.16.3.2 eq 514
10.	access-list FROM-PSS permit udp host 172.16.1.5 host 172.16.3.2 eq 514
11.	access-list FROM-PSS permit udp host 172.16.1.7 host 172.16.3.2 eq 514
12.	access-list FROM-PSS deny ip any any log access-group FROM-PSS in interface PSS

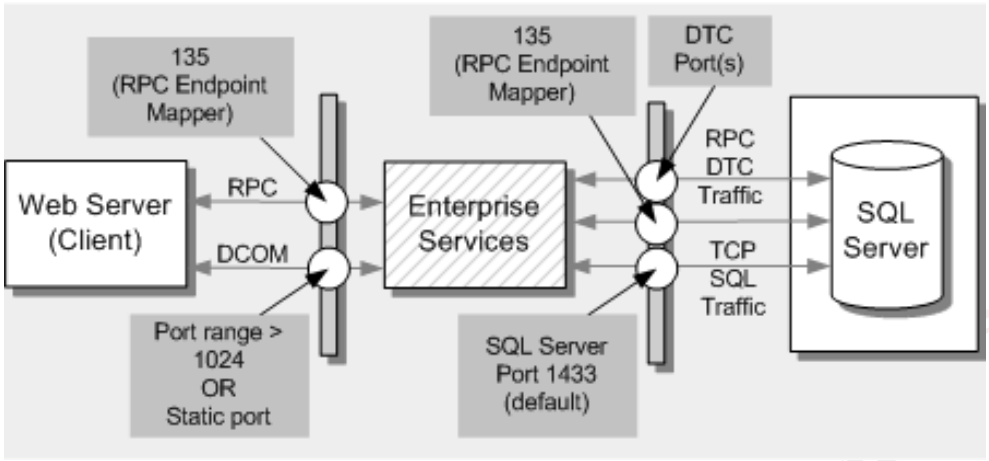

Figure 4. Typical Enterprise Services firewall port configuration

(graphic taken from Microsoft MSDN website ref No.2 in endnotes)

The above diagram shows communication flow in a Firewalled multitiered application architecture and the ports required to allow traffic flow between web, application and database servers in the GIAC environment. For traffic flow between the GIAC Web server and Application server we need to open RPC and DCOM ports. By default, DCOM uses RPC dynamic port allocation, which randomly selects port numbers above 1024. In addition, port 135 is used by the RPC endpoint mapping service. We want to avoid opening all ports >1024 on our GIAC Firewall if possible for obvious reasons. Luckily we do have the ability to reconfigure the ports we need to open for DCOM and restrict RPC port allocation to a defined range.[3] We can also use a static endpoint mapping and restrict the ports required to only two i.e. port 135 for RPC and a single static configured port for DCOM. Note that static port configuration is only available in Win2000 SP3 or Win2003.

To allow communications between the .NET application server and the backend SQL Database we need to enable RPC *and* DTC communications. "Distributed Transaction Coordinator or DTC also uses Remote Procedure Call (RPC) dynamic port allocation. By default RPC dynamic port allocation randomly selects port numbers above 1024. By modifying the registry, we can control which ports RPC dynamically allocates for incoming communication. You can then configure your firewall to confine incoming external communication to only those ports and port 135 (the RPC Endpoint Mapper port)".[4] Microsoft recommends that you open up ports from 5000 and up, and that you open a minimum of 15 to 20 ports. For the purposes of the GIAC architecture we open ports 5000-5020 as seen in the previous page.

FROM-INSIDE (inbound to the inside interface from the Internal network)

Rule No.	Source Interface	Destination Interface	Source IP/Network	Destination IP/Network	Application Protocol	Network Protocol	Dest Port	Action
1.	Inside	Outside	10.0.1.0	Any	MSN	TCP	1863	Deny
2.	Inside	Outside	10.0.1.0	207.46.104.20	HTTP	TCP	80	Deny
3.	Inside	Outside	10.0.1.0	207.46.110.252	HTTP	TCP	80	Deny
4.	Inside	Outside	10.0.1.0	210.158.219.57	HTTP	TCP	80	Deny
5.	Inside	Outside	10.0.1.0	66.218.75.184	HTTP	TCP	80	Deny
6.	Inside	Outside	10.0.1.0	Any	POP3	TCP	110	Deny
7.	Inside	DMZ	10.0.1.0	172.16.1.2	HTTP	TCP	80	Permit
8.	Inside	DMZ	10.0.1.0	172.16.1.2	HTTPS	TCP	443	Permit
9.	Inside	DMZ	10.0.1.3	172.16.1.3	DNS	UDP	53	Permit
					DNS	TCP	53	Permit
10.	Inside	Outside	10.0.1.0	Any	HTTP	TCP	80	Permit
11.	Inside	DMZ	172.16.3.2	172.16.1.2	SSH	TCP	22	Permit
12.	Inside	DMZ	172.16.3.2	172.16.1.3	SSH	TCP	22	Permit
13.	Inside	DMZ	172.16.3.2	172.16.1.4	SSH	TCP	22	Permit
14.	Inside	DMZ	172.16.3.2	172.16.1.5	SSH	TCP	22	Permit
15.	Inside	DMZ	172.16.3.2	172.16.1.7	SSH	TCP	22	Permit
16.	Inside	DMZ	10.0.1.0	172.16.1.9	SSH	TCP	22	Permit
17.	Inside	Outside	172.16.3.2	202.168.2.1	SSH	TCP	22	Permit
18.	Any	Any	Any	Any	Any	Any	Any	Deny

Rule No.	Rule Description
1.	Deny outgoing MSN messenger access from internal network
2.	Deny http access to messenger.hotmail.com
3.	Deny http access to Web Messenger
4.	Block outbound access to Hotmail.com
5.	Block outbound access to Yahoo Mail.
6.	Block all outbound POP3 on TCP port 110 .
7.	Allow any inside host to access the corporate web server over http on tcp port 80
8.	Allow any inside host to access the corporate web server over https on tcp port 443
9.	Allow unresolved internal DNS queries to forward to external DNS over TCP or UDP 53
10.	Allow any inside host to access the Internet for web browsing on TCP port 80
11.	Allow SSH from Management Segment to PSS web server over TCP port 22
12.	Allow SSH from Management Segment to External DNS
13.	Allow SSH from Management Segment to SMTP Relay server on PSS
14.	Allow SSH from Management Segment to NTP server on PSS
15.	Allow SSH from Management Segment to PSS Catalyst switch
16	Allow SSH from inside network to SSH server to pick up Fortunes uploaded by partner/supplier
17.	Allow SSH from Management Segment to Screening router ethernet interface
18.	Default deny-all Rule

Rule No.	PIX Access List configuration
1.	access-list FROM-INSIDE deny tcp any any eq 1863
2.	access-list FROM-INSIDE deny tcp any 207.46.104.20 eq http
3.	access-list FROM-INSIDE deny tcp any 207.46.110.252 eq http
4.	access-list FROM-INSIDE deny tcp any 210.158.219.57 eq http
5.	access-list FROM-INSIDE deny tcp any 66.218.75.184 eq http
6.	access-list FROM-INSIDE deny tcp any any eq pop3
7.	access-list FROM-INSIDE permit tcp any host 172.16.1.2 eq 80
8.	access-list FROM-INSIDE permit tcp any host 172.16.1.2 eq 443
9.	access-list FROM-INSIDE permit tcp host 10.0.1.3 host 172.16.1.2 eq 53
10.	access-list FROM-INSIDE permit tcp any any eq 80

```
11.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 172.16.1.2 eq 22
12.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 172.16.1.3 eq 22
13.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 172.16.1.4 eq 22
14.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 172.16.1.5 eq 22
15.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 172.16.1.7 eq 22
16      Access-list FROM-INSIDE permit tcp host 10.0.1.0 0.0.0.255 host 172.16.1.9 eq 22
17.     access-list FROM-INSIDE permit tcp host 172.16.3.2 host 202.168.2.1 eq 22
18.     access-list FROM-INSIDE deny ip any any log
        access-group FROM-INSIDE in interface inside
```

FROM-APP (inbound to the Application interface from the Application segment)

Rule No.	Source Interface	Destination Interface	Source IP/Network	Destination IP/Network	Application Protocol	Network Protocol	Dest Port	Action
1.	Application	Inside	172.16.2.2	172.16.4.2	MS-SQL	TCP	1433	Permit
2.	Application	Inside	172.16.2.2	172.16.4.2	MS-SQL	UDP	1434	Permit
3.	Application	Inside	172.16.2.2	172.16.4.2	RPC	TCP	135	Permit
4.	Application	Inside	172.16.2.2	172.16.4.2	DTC	TCP	5000 to 5020	Permit
5.	Any	Any	Any	Any	Any	Any	Any	Deny

Rule No.	Rule Description
1.	Allow .NET application server to access back end SQL database on Database segment over tcp port 1433 (default listener port)
2.	Allow .NET application server to access back end SQL database on Database segment over udp port 1434 (used for negotiation)
3.	Allow RPC communications over port 135 between .NET Application and SQL Database
4.	Allow DTC communications over port range 5000 to 5020 between .NET and SQL
5.	Default Deny All

Rule No.	PIX Access List configuration
1.	access-list FROM-APP permit tcp host 172.16.2.2 host 172.16.4.2 eq 1433
2.	access-list FROM-APP permit udp host 172.16.2.2 host 172.16.4.2 eq 1434
3.	access-list FROM-APP permit tcp host 172.16.2.2 host 172.16.4.2 eq 135
4.	access-list FROM-APP permit tcp host 172.16.2.2 host 172.16.4.2 range 5000 5020
5.	access-list FROM-OUTSIDE deny ip any any log access-group FROM-OUTSIDE in interface outside

references

[1] Ranum, Marcus. Infosecurity Magazine. October 2004. http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss486_art995,00.html

[2] Microsoft MSDN. “Securing Your Application Server: Firewall Considerations”. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secmod/html/secmod90.asp

[3] Microsoft MSDN. Article ID:300083. July 2, 2004 How To: Restrict TCP/IP Ports on Windows 2000 and Windows XP

[4] Microsoft MSDN. “Configuring Microsoft Distributed Transaction Coordinator (DTC) to Work Through a Firewall”. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q250367

Appendix I

Appendix I shows the router configuration for GIAC's Guangzhou branch office detailing CBAC, VPN, IOS hardening and Filtering as discussed and referenced in the earlier sections above. The following config shouldn't be considered a complete configuration for the environment described above. It simply shows how a working router configuration might look after the hardening steps detailed above. With respect to ACLs the configuration is quite basic as we are not hosting any publicly accessible services at our branch offices.

```
version 12.3
! Disable the X.25 Packet Assembler/Disassembler service.
no service pad
!
! TCP keepalives to enable the router to send periodic
! messages to ensure that a TCP connection is still open.
service tcp-keepalives-in
service tcp-keepalives-out
!
! Logging and debug messages to include timestamps. Timestamps allow
! for accurate event correlation in the event of system or network
! compromise.
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
!
! Ensure that passwords are displayed in their encrypted form when
! the router config is viewed
service password-encryption
!
! implement a minimum password length of eight characters
security passwords min-length 8
!
! set the number of allowable unsuccessful login attempts to five
security authentication failure rate 5 log
!
! The TCP and UDP small servers refer to the echo, chargen and
! discard servers running on ports 7, 19, and 9 respectively. They
! are disabled by default on IOS 11.3 and later. The echo port may be
! leveraged with the Fraggle exploit to cause a Denial of Service.
no service tcp-small-servers
no service udp-small-servers
!
! set a descriptive host name to provide contextual information of
! the device location and function for administration purposes.
hostname GZH-ROUTER
!
! log critical messages to the console
logging console critical
!
! configure AAA login authentication for vty lines. It is generally
! recommended that AAA Authentication through RADIUS or TACACS+ be
! used for any administrative access to the router. AAA allows us to
! centralize all management of administrative access.
aaa new-model
aaa authentication login auth-hosts tacacs+
tacacs-server host 10.0.1.6
```

```
tacacs-server key tacacskey123
!
! set enable and enable secret passwords
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
enable password 7 140E4758161C2C3222
!
! In the absence of a AAA infrastructure a username and password
! combination can be used to prompt before allowing administrative
! access. Local authentication is also a useful form of backup if for
! some reason the AAA server is unavailable.
username giac-user password 7 13021E130841142B38373F3C2726
!
! set router timezone
clock timezone UTC 8
!
! allow use of subnet zero for addressing.
ip subnet-zero
!
! disable source routing of packets. Source routing of packets can be
! used to manipulate trust relationships in a network.
no ip source-route
!
! Disable gratuitous ARP to prevent ARP table poisoning,
! ARP spoofing and Man-in-the-Middle attacks.
no ip gratuitous-arps
!
! Reduce default syn wait time to 15 seconds. The synwait-time IOS
! parameter is the amount of time that the IOS waits while attempting
! to complete the three way TCP handshake with a destination host.
! The default is 30 seconds. An unusually large number of half-open
! TCP connections could be indicative of a denial of service attack.
! By reducing the timeout value to 15 the IOS closes TCP connections
! within 15 seconds if the connection has not been established.
ip tcp synwait-time 15
!
! Disable DNS name lookups. If DNS name lookup is enabled on a Cisco
! router, DNS name queries are sent to the broadcast address
no ip domain-lookup
!
! Disable use of router as a name server
no ip name-server
!
! Disable use of router as a bootp server. A bootp server was a
! precursor to present day DHCP. A bootp server would hold a table of
! MAC to IP address mappings and would provide an IP address to
! diskless hosts similar to the way DHCP works today.
no ip bootp server
!
! enable Cisco Express Forwarding. Cisco Express Forwarding (CEF)
! must be enabled on the router for Unicast RPF to work.
ip cef
!
! Disable CDP globally. CDP is the Cisco Discovery Protocol. CDP is
! used to provide details on neighbor Cisco devices such as device ID,
! hostname and platform capabilities. This information may be
! leveraged to provide network information and can be used to garner
! layer 3 IP addressing information of neighboring devices which an
! attacker could then telnet to.
no cdp run
!
! In addition to command line router configuration a Cisco router
```

```
! provides the ability to perform web based administration through
! the HTTP protocol. HTTP access is risky however as it provides for
! clear text authentication. It is recommended to either disable the
! HTTP server or use the ip http access-class command to restrict
! access to a management IP.
no ip http server
no ip http secure-server
!
! The finger service can be used to determine which users are logged
! into the network device and enumerate user names. It is recommended
! to disable the finger service.
no ip finger
!
! Certain protocols like POP, SMTP and Telnet use IDENT to identify
! the user requesting services. This may be considered a security
! concern as network information may be disclosed.
no ip identd
!
! enable IP routing
ip routing
!
! Configure Context-Based Access Control (CBAC) Timers and Thresholds.
! TCP/IP relies on a number of different timers during the life of a
! TCP/IP session to maintain state. These timers include synwait and
! finwait timers, keep-alive timers and connection establishment
! timers. These timers are very important in ensuring the correct
! sending and receiving of data during a TCP/IP session. Timers can
! be exploited by hackers to their benefit. For example hackers can
! exploit the lack of a synwait time to create many half-open TCP
! connections and create a possible denial of service condition. CBAC
! provides us the ability to modify default timers and thresholds as
! described in the following example. Note that many of the
! parameters passed in the following examples are already default
! values but are shown by way of example. It's better to stick with
! the defaults and tuning as you gain more experience of how changes
! will affect your IOS Firewall operation.
ip inspect tcp synwait-time 15
ip inspect tcp finwait-time 1
ip inspect tcp idle-time 2400
ip inspect udp idle-time 20
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! define CBAC audit trails
ip inspect audit-trail
ip audit notify log
ip audit po max-events 100
!
! define IP traffic to be monitored by CBAC. We need to tell CBAC
! which protocols we want monitored or that protocol will not be
! looked at.
no ip inspect name GZH-CBAC
ip inspect name GZH-CBAC tcp audit-trail on
ip inspect name GZH-CBAC udp audit-trail on
ip inspect name GZH-CBAC smtp audit-trail on
ip inspect name GZH-CBAC http audit-trail on
!
```

```
! Configure IPSec Internet Key Exchange (IKE) policy. 3des/md5/pre-
! shared key, Diffie Hellman Group 2, SA lifetime 86400 seconds.
crypto isakmp enable
crypto isakmp identity address
!
crypto isakmp policy 1
 encryption 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 86400
!
! set VPN peer pre-shared key and IP address
crypto isakmp key giackey123 address 202.168.2.2
!
! IPSec crypto map configuration
crypto ipsec transform-set giac-transformset ah-md5-hmac esp-des esp-
md5-hmac
crypto map giac-cryptomap local-address Serial0/0
!
crypto map giac-cryptomap 1 ipsec-isakmp
 match address IPSEC-IN
 set peer 202.168.2.2
 set transform-set giac-transformset
 set security-association lifetime seconds 86400
 set security-association lifetime kilobytes 4608000
!
! Configure PIX inside interface
interface FastEthernet0/0
 description connected to intranet
 ip address 10.0.2.1 255.255.255.0
 ip access-group e0-outbound in
!
! Disabling ICMP Type 3, 5 and 18 messages namely ICMP Host
! Unreachable, ICMP Redirects and ICMP Netmask Reply prevents the
! router from sending back information that may help an attacker to
! map the network. Tools such as NMAP and SING can solicit ICMP
! replies from a host or router which may help in mapping a network.
 no ip redirects
 no ip unreachables
 no ip mask-reply
!
! IP Proxy ARP allows a router to act as an intermediary for ARP
! broadcasts to another network. The advantage with proxy ARP is that
! it can assist a host to reach hosts on a remote subnet without the
! need to configure routing or a default gateway. There are however
! security considerations if IP Proxy ARP is enabled, namely a host
! can spoof another host in an attempt to intercept packets meant for
! the real host. It is recommended that IP Proxy ARP be disabled.
 no ip proxy-arp
!
! enable network address translation on inside interface
 ip nat inside
!
! Turn off IP Directed Broadcast for all interfaces and sub-
! interfaces to help prevent your network from being used in a
! Distributed Denial of Service attack. In a Smurf DDoS a malicious
! hacker sends an ICMP ping to the network broadcast address spoofing
! the IP of the victim as the source of the echo request packet. A
! network configured to forward directed broadcasts will send the
! ping packet to all hosts on the network who in turn respond with an
```

```
! echo reply to the spoofed host causing a denial of service. The
! larger the number of replying hosts the greater the effect of the
! DDoS attack. Smurf is the name given to the exploit code written to
! exploit this feature. A list of the most active Smurf amplifiers
! sorted by Autonomous System (AS) number is available on netscan.org.
! To help prevent spoofing used in the DDoS attack the ip verify
! unicast reverse-path command on Cisco routers checks that the
! source IP address and interface of a packet appears in its routing
! table and the return interface is the same as the interface on
! which the packet was received.
 no ip directed-broadcast
!
! MOP is a DEC protocol used for communication between remote hosts
! and network devices. MOP may be used as an attack vector to
! compromise a Cisco router. It is recommended to disable MOP if not
! in use.
 no mop enabled
!
! set keepalive interval to 10 seconds
 keepalive 10
!
! shut down unused router interfaces
interface FastEthernet0/1
 shutdown
!
! configure outside interface.
interface Serial0/0
 description connected to Internet
 crypto map giac-cryptomap
 ip address 203.168.3.1 255.255.255.0
 ip access-group S0-INBOUND-FROM-INTERNET in
 distribute-list <access-list-no> in|out <interface>
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip mask-reply
 no ip proxy-arp
 ip nat outside
 encapsulation ppp
 no ip route-cache
 no ip mroute-cache
 no ip directed-broadcast
 no mop enabled
!
! The command ntp disable keeps a router interface from acting as an
! NTP server. The interface can still take time from an NTP server in
! client mode. It is recommended to disable NTP for all external
! interfaces.
 ntp disable
!
! Apply Context based Access Control monitoring to outbound traffic
 ip inspect GZH-CBAC out
!
! configure null interface for null routing
interface null0
no ip unreachables
!
! Implement turbo access lists for faster processing of ACLs.
ip access-list compiled
!
! Access Control List IPSEC-IN - allow IPSec from Hong Kong head
```

```
! office
no access-list IPSEC-IN
access-list IPSEC-IN permit udp host 202.168.2.2 host 203.168.3.1 eq
500
access-list IPSEC-IN permit esp host 202.168.2.2 host 203.168.3.1
!
! Dynamic NAT/PAT configuration for internal hosts.
ip nat translation timeout 86400
ip nat translation tcp-timeout 86400
ip nat translation udp-timeout 300
ip nat translation dns-timeout 60
ip nat translation finrst-timeout 60
ip nat inside source list 1 interface Serial0/0 overload
!
! configure routing protocols
router eigrp 100
 network 10.0.1.0
 network 10.0.2.0
 network 10.0.3.0
 network 10.0.4.0
 network 10.0.5.0
 no auto-summary
!
! Enable classless routing. Enables IOS to forward packets
! destined for an unrecognized subnet to the best supernet route.
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Serial0/0
ip route 172.16.1.0 0.0.0.255 FastEthernet0/0
!
! configure SNMP
snmp-server community <complex-community-string> RO MANAGEMENT-IN
no snmp-server location
no snmp-server contact
!
! Black hole routes. Route to null interface. Less processor
! intensive than ACL's. Inspired by Rob Thomas' Secure IOS Template.
ip route 1.0.0.0 255.0.0.0 null0
ip route 2.0.0.0 255.0.0.0 null0
ip route 5.0.0.0 255.0.0.0 null0
ip route 7.0.0.0 255.0.0.0 null0
ip route 10.0.0.0 255.0.0.0 null0
ip route 23.0.0.0 255.0.0.0 null0
ip route 27.0.0.0 255.0.0.0 null0
ip route 31.0.0.0 255.0.0.0 null0
ip route 36.0.0.0 255.0.0.0 null0
ip route 37.0.0.0 255.0.0.0 null0
ip route 39.0.0.0 255.0.0.0 null0
ip route 41.0.0.0 255.0.0.0 null0
ip route 42.0.0.0 255.0.0.0 null0
ip route 49.0.0.0 255.0.0.0 null0
ip route 50.0.0.0 255.0.0.0 null0
ip route 73.0.0.0 255.0.0.0 null0
ip route 74.0.0.0 255.0.0.0 null0
ip route 75.0.0.0 255.0.0.0 null0
ip route 76.0.0.0 255.0.0.0 null0
ip route 77.0.0.0 255.0.0.0 null0
ip route 78.0.0.0 255.0.0.0 null0
ip route 79.0.0.0 255.0.0.0 null0
ip route 89.0.0.0 255.0.0.0 null0
```

```
ip route 90.0.0.0 255.0.0.0 null0
ip route 91.0.0.0 255.0.0.0 null0
ip route 92.0.0.0 255.0.0.0 null0
ip route 93.0.0.0 255.0.0.0 null0
ip route 94.0.0.0 255.0.0.0 null0
ip route 95.0.0.0 255.0.0.0 null0
ip route 96.0.0.0 255.0.0.0 null0
ip route 97.0.0.0 255.0.0.0 null0
ip route 98.0.0.0 255.0.0.0 null0
ip route 99.0.0.0 255.0.0.0 null0
ip route 100.0.0.0 255.0.0.0 null0
ip route 101.0.0.0 255.0.0.0 null0
ip route 102.0.0.0 255.0.0.0 null0
ip route 103.0.0.0 255.0.0.0 null0
ip route 104.0.0.0 255.0.0.0 null0
ip route 105.0.0.0 255.0.0.0 null0
ip route 106.0.0.0 255.0.0.0 null0
ip route 107.0.0.0 255.0.0.0 null0
ip route 108.0.0.0 255.0.0.0 null0
ip route 109.0.0.0 255.0.0.0 null0
ip route 110.0.0.0 255.0.0.0 null0
ip route 111.0.0.0 255.0.0.0 null0
ip route 112.0.0.0 255.0.0.0 null0
ip route 113.0.0.0 255.0.0.0 null0
ip route 114.0.0.0 255.0.0.0 null0
ip route 115.0.0.0 255.0.0.0 null0
ip route 116.0.0.0 255.0.0.0 null0
ip route 117.0.0.0 255.0.0.0 null0
ip route 118.0.0.0 255.0.0.0 null0
ip route 119.0.0.0 255.0.0.0 null0
ip route 120.0.0.0 255.0.0.0 null0
ip route 121.0.0.0 255.0.0.0 null0
ip route 122.0.0.0 255.0.0.0 null0
ip route 123.0.0.0 255.0.0.0 null0
ip route 124.0.0.0 255.0.0.0 null0
ip route 125.0.0.0 255.0.0.0 null0
ip route 126.0.0.0 255.0.0.0 null0
ip route 127.0.0.0 255.0.0.0 null0
ip route 169.254.0.0 255.255.0.0 null0
ip route 172.16.0.0 255.240.0.0 null0
ip route 173.0.0.0 255.0.0.0 null0
ip route 174.0.0.0 255.0.0.0 null0
ip route 175.0.0.0 255.0.0.0 null0
ip route 176.0.0.0 255.0.0.0 null0
ip route 177.0.0.0 255.0.0.0 null0
ip route 178.0.0.0 255.0.0.0 null0
ip route 179.0.0.0 255.0.0.0 null0
ip route 180.0.0.0 255.0.0.0 null0
ip route 181.0.0.0 255.0.0.0 null0
ip route 182.0.0.0 255.0.0.0 null0
ip route 183.0.0.0 255.0.0.0 null0
ip route 184.0.0.0 255.0.0.0 null0
ip route 185.0.0.0 255.0.0.0 null0
ip route 186.0.0.0 255.0.0.0 null0
ip route 187.0.0.0 255.0.0.0 null0
ip route 189.0.0.0 255.0.0.0 null0
ip route 190.0.0.0 255.0.0.0 null0
ip route 192.0.2.0 255.255.255.0 null0
ip route 192.168.0.0 255.255.0.0 null0
ip route 197.0.0.0 255.0.0.0 null0
```

```
ip route 223.0.0.0 255.0.0.0 null0
!
! Drop Reserved/Unallocated/Private IP address space. Catch traffic
! not dropped by null routing.
ip access-list extended S0-INBOUND-FROM-INTERNET
 no access-list S0-INBOUND-FROM-INTERNET
 deny ip 0.0.0.0 0.255.255.255 any log
 deny ip 1.0.0.0 0.255.255.255 any log
 deny ip 2.0.0.0 0.255.255.255 any log
 deny ip 5.0.0.0 0.255.255.255 any log
 deny ip 7.0.0.0 0.255.255.255 any log
 deny ip 10.0.0.0 0.255.255.255 any log
 deny ip 23.0.0.0 0.255.255.255 any log
 deny ip 27.0.0.0 0.255.255.255 any log
 deny ip 31.0.0.0 0.255.255.255 any log
 deny ip 36.0.0.0 0.255.255.255 any log
 deny ip 37.0.0.0 0.255.255.255 any log
 deny ip 39.0.0.0 0.255.255.255 any log
 deny ip 41.0.0.0 0.255.255.255 any log
 deny ip 42.0.0.0 0.255.255.255 any log
 deny ip 49.0.0.0 0.255.255.255 any log
 deny ip 50.0.0.0 0.255.255.255 any log
 deny ip 73.0.0.0 0.255.255.255 any log
 deny ip 74.0.0.0 0.255.255.255 any log
 deny ip 75.0.0.0 0.255.255.255 any log
 deny ip 76.0.0.0 0.255.255.255 any log
 deny ip 77.0.0.0 0.255.255.255 any log
 deny ip 78.0.0.0 0.255.255.255 any log
 deny ip 79.0.0.0 0.255.255.255 any log
 deny ip 89.0.0.0 0.255.255.255 any log
 deny ip 90.0.0.0 0.255.255.255 any log
 deny ip 91.0.0.0 0.255.255.255 any log
 deny ip 92.0.0.0 0.255.255.255 any log
 deny ip 93.0.0.0 0.255.255.255 any log
 deny ip 94.0.0.0 0.255.255.255 any log
 deny ip 95.0.0.0 0.255.255.255 any log
 deny ip 96.0.0.0 0.255.255.255 any log
 deny ip 97.0.0.0 0.255.255.255 any log
 deny ip 98.0.0.0 0.255.255.255 any log
 deny ip 99.0.0.0 0.255.255.255 any log
 deny ip 100.0.0.0 0.255.255.255 any log
 deny ip 101.0.0.0 0.255.255.255 any log
 deny ip 102.0.0.0 0.255.255.255 any log
 deny ip 103.0.0.0 0.255.255.255 any log
 deny ip 104.0.0.0 0.255.255.255 any log
 deny ip 105.0.0.0 0.255.255.255 any log
 deny ip 106.0.0.0 0.255.255.255 any log
 deny ip 107.0.0.0 0.255.255.255 any log
 deny ip 108.0.0.0 0.255.255.255 any log
 deny ip 109.0.0.0 0.255.255.255 any log
 deny ip 110.0.0.0 0.255.255.255 any log
 deny ip 111.0.0.0 0.255.255.255 any log
 deny ip 112.0.0.0 0.255.255.255 any log
 deny ip 113.0.0.0 0.255.255.255 any log
 deny ip 114.0.0.0 0.255.255.255 any log
 deny ip 115.0.0.0 0.255.255.255 any log
 deny ip 116.0.0.0 0.255.255.255 any log
 deny ip 117.0.0.0 0.255.255.255 any log
 deny ip 118.0.0.0 0.255.255.255 any log
 deny ip 119.0.0.0 0.255.255.255 any log
 deny ip 120.0.0.0 0.255.255.255 any log
```

```
 deny ip 121.0.0.0 0.255.255.255 any log
 deny ip 122.0.0.0 0.255.255.255 any log
 deny ip 123.0.0.0 0.255.255.255 any log
 deny ip 124.0.0.0 0.255.255.255 any log
 deny ip 125.0.0.0 0.255.255.255 any log
 deny ip 126.0.0.0 0.255.255.255 any log
 deny ip 127.0.0.0 0.255.255.255 any log
 deny ip 169.254.0.0 0.0.255.255 any log
 deny ip 172.16.0.0 0.15.255.255 any log
 deny ip 173.0.0.0 0.255.255.255 any log
 deny ip 174.0.0.0 0.255.255.255 any log
 deny ip 175.0.0.0 0.255.255.255 any log
 deny ip 176.0.0.0 0.255.255.255 any log
 deny ip 177.0.0.0 0.255.255.255 any log
 deny ip 178.0.0.0 0.255.255.255 any log
 deny ip 179.0.0.0 0.255.255.255 any log
 deny ip 180.0.0.0 0.255.255.255 any log
 deny ip 181.0.0.0 0.255.255.255 any log
 deny ip 182.0.0.0 0.255.255.255 any log
 deny ip 183.0.0.0 0.255.255.255 any log
 deny ip 184.0.0.0 0.255.255.255 any log
 deny ip 185.0.0.0 0.255.255.255 any log
 deny ip 186.0.0.0 0.255.255.255 any log
 deny ip 187.0.0.0 0.255.255.255 any log
 deny ip 189.0.0.0 0.255.255.255 any log
 deny ip 190.0.0.0 0.255.255.255 any log
 deny ip 192.0.2.0 0.0.0.255 any log
 deny ip 192.168.0.0 0.0.255.255 any log
 deny ip 197.0.0.0 0.255.255.255 any log
 deny ip 223.0.0.0 0.255.255.255 any log
 deny ip 224.0.0.0 31.255.255.255 any log
!
! Drop inbound packets that claim to originate from our internal
! network.
 deny ip 203.168.3.0 0.0.0.255 any log
!
! Permit packets returning as part of an already established
! connection.
 permit tcp any any established
!
! Implement Access Control for routing updates
 permit eigrp 100, etc.
!
! Drop all non-initial ICMP fragments. ICMP messages are small and
! unlikely to ever require fragmentation.
 deny icmp any any fragments log
!
! Deny ICMP redirect and mask request traffic.
 deny icmp any any redirect log
 deny icmp any any mask-request log
!
! Permit ping for troubleshooting
 permit icmp any any echo
 permit icmp any any echo-reply
!
! permit "fragmentation needed but DF bit set" message.
 permit icmp any any packet-too-big
!
! Allow source quench for flow control and time-exceeded messages for
! traceroute.
 permit icmp any any source-quench
```

```
 permit icmp any any time-exceeded
!
! Allow admin prohibited, icmp traceroute and host/port unreachables
 permit icmp any any administratively-prohibited
 permit icmp any any traceroute
 permit icmp any any unreachable
!
! Deny all other icmp traffic
 deny icmp any any log
!
! Deny "iffy" protocol traffic. Should be blocked both inbound and
! outbound. The log-input keyword records the source MAC address
! which may be required for trace-back. MAC addresses are more
! relevant when identifying attack sources since IP addresses can be
! spoofed.
 deny tcp any any eq 23 log-input
 deny tcp any any range 67 69 log-input
 deny udp any any range 67 69 log-input
 deny tcp any any eq 111 log-input
 deny udp any any eq 111 log-input
 deny tcp any any range 135 139 log-input
 deny udp any any range 135 139 log-input
 deny udp any any range 161 162 log-input
 deny tcp any any eq 445 log-input
 deny udp any any eq 445 log-input
 deny udp any any eq 514 log-input
 deny tcp any any range 1025 1039 log-input
 deny udp any any range 1025 1039 log-input
 deny tcp any any eq 2049 log-input
 deny udp any any eq 2049 log-input
 deny tcp any any range 6000 6255 log-input
 deny udp any any range 6000 6255 log-input
 deny tcp any any range 6666 6667 log-input
 !
! Default deny all rule
 deny ip any any log
!
! Access Control List E0-INBOUND-FROM-INTRANET
ip access-list extended E0-INBOUND-FROM-INTRANET
 no access-list E0-INBOUND-FROM-INTRANET
!
! Egress Filtering. Only permit outbound traffic with our network
! address.
 permit ip 203.168.3.0 0.0.0.255
!
! ICMP inbound
 deny icmp any any fragments
 permit icmp 172.16.3.0 0.0.0.255 any echo
 permit icmp any any packet-too-big
 permit icmp any any time-exceeded
 deny icmp any any
!
! Define ACL for telnet, vty and AUX access to router for management.
! Allow management from Ciscoworks management server.
ip access-list standard MANAGEMENT-IN
 no access-list MANAGEMENT-IN
 permit 172.16.3.2
!
! Once again block critical services, this time outbound from the
! internal network.
 deny tcp any any eq 23 log-input
```

```
 deny tcp any any range 67 69 log-input
 deny udp any any range 67 69 log-input
 deny tcp any any eq 111 log-input
 deny udp any any eq 111 log-input
 deny tcp any any range 135 139 log-input
 deny udp any any range 135 139 log-input
 deny udp any any range 161 162 log-input
 deny tcp any any eq 445 log-input
 deny udp any any eq 445 log-input
 deny udp any any eq 514 log-input
 deny tcp any any range 1025 1039 log-input
 deny udp any any range 1025 1039 log-input
 deny tcp any any eq 2049 log-input
 deny udp any any eq 2049 log-input
 deny tcp any any range 6000 6255 log-input
 deny udp any any range 6000 6255 log-input
 deny tcp any any range 6666 6667 log-input
!
! configure banner warning against unauthorized access
banner motd ^C
Unlawful Access will be prosecuted to the fullest extent of the law.
^C
! Configure console, telnet/ssh and out-of-band settings with
! timeouts and apply an access-list allowing only the management
! interface to make connections. Use crypto generate rsa general-keys
! modulus 1024 command to generate ssh keys.
!
! console port configuration
line con 0
 access-class MANAGEMENT-IN in
 exec-timeout 5 0
 password 7 061F5A7256560F0003
 logging synchronous
 login authentication auth-hosts
!
! vty access via SSH as per GIAC access policy
line vty 0 4
 access-class MANAGEMENT-IN in
 exec-timeout 5 0
 transport input ssh
 password 7 01AFE1589CDA0679F2
 login authentication auth-hosts
!
! disable AUX port out-of-band access
line aux
  exec-timeout 0 0
!
! Set NTP server. Accurate and synchronized time is important on a
! network as it provides a frame of reference for all devices on the
! network and allows us to carry out post-incident forensics and
! intrusion response. Without accurate time it is virtually
! impossible to cross-correlate log information on different host and
! network devices. GIAC synchronizes time on its internal network
! with an external time source through use of an internal NTP server.
ntp server 172.16.1.5
end
```

Appendix II

Appendix II shows the fully commented GIAC Enterprises Primary PIX 515E Firewall configuration.

```
PIX Version 6.3(1)
! Configure type and capability of each interface
! 10baset = 10Mbps Half Duplex
! 100Full = 100mbps Full Duplex
interface ethernet0 10baset
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
!
! Assign names to interfaces and set interface security
! levels
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 pss security50
nameif ethernet3 application security40
!
! Set hostname to giac
hostname giac-fw
!
! set DNS domain name to giac.org
domain-name giag.org
!
! fixup command enables use of services on the firewall
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol ip udp 5060
fixup protocol skinny 2000
! mailguard messes with MS Exchange server behind a PIX Firewall
! disable SMTP fixup
no fixup protocol smtp 25
fixup protocol sqlnet 1521
!
! enable use of name command for name-to-IP-address
! mappings.
Names
!
! create name-to-IP-address mappings for easier reading
name 100.1.2.3 partner-vpn-peer
name 202.168.2.2 hongkong-vpn-peer
name 203.168.3.1 guangzhou-vpn-peer
name 204.168.4.1 brisbane-vpn-peer
name 205.168.5.1 sanfran-vpn-peer
name 206.168.6.1 dublin-vpn-peer
name 172.16.1.2 webserver
name 172.16.1.3 ext-dns
name 172.16.1.4 ext-email
name 172.16.1.5 ntp-server
name 172.16.1.7 pss-switch
```

```
name 172.16.1.9 ssh-server
name 172.16.2.2 appserver
name 172.16.3.2 database-server
name 10.0.1.3 int-dns
name 10.0.1.2 int-wins
name 10.0.1.5 int-email
name 172.16.3.2 ciscoworks
name 137.189.6.18 ext-ntp-cuhk
!
! ACL to select outbound traffic to branch offices for IPSec
! for branch offices and partner access
access-list IPSEC-GUANGZHOU permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.25.255.0
access-list IPSEC-BRISBANE permit ip 10.0.1.0 255.255.255.0 10.0.3.0
255.25.255.0
access-list IPSEC-SANFRAN permit ip 10.0.1.0 255.255.255.0 10.0.4.0
255.25.255.0
access-list IPSEC-DUBLIN permit ip 10.0.1.0 255.255.255.0 10.0.5.0
255.25.255.0
access-list IPSEC-PARTNER permit ip 10.0.1.0 255.255.255.0 10.0.6.0
255.25.255.0
!
! … for remote VPN users
access-list IPSEC-REMOTE-VPN permit ip any 10.0.10.0 255.255.255.0
!
! ACL for traffic inbound to outside interface from the Internet
access-list FROM-OUTSIDE permit tcp any host webserver eq www
access-list FROM-OUTSIDE permit tcp any host webserver eq https
access-list FROM-OUTSIDE permit tcp any host ext-dns eq domain
access-list FROM-OUTSIDE permit udp any host ext-dns eq domain
access-list FROM-OUTSIDE permit tcp any host ext-email eq smtp
access-list FROM-OUTSIDE prmit tcp host 209.99.1.0 ssh-server eq ssh
access-list FROM-OUTSIDE prmit tcp host 210.99.1.0 ssh-server eq ssh
access-list FROM-OUTSIDE permit udp host 202.168.2.1 host ciscoworks
snmp snmptrap
access-list FROM-OUTSIDE permit udp host 202.168.2.1 host ciscoworks
eq syslog
access-list FROM-OUTSIDE permit udp host guangzhou-vpn-peer host
hongkong-vpn-peer eq isakmp
access-list FROM-OUTSIDE permit udp host brisbane-vpn-peer host
hongkong-vpn-peer eq isakmp
access-list FROM-OUTSIDE permit udp host sanfran-vpn-peer host
hongkong-vpn-peer eq isakmp
access-list FROM-OUTSIDE permit udp host dublin-vpn-peer host
hongkong-vpn-peer eq isakmp
access-list FROM-OUTSIDE permit udp host partner-vpn-peer host
hongkong-vpn-peer eq isakmp
access-list FROM-OUTSIDE permit esp host guangzhou-vpn-peer host
hongkong-vpn-peer
access-list FROM-OUTSIDE permit esp host brisbane-vpn-peer host
hongkong-vpn-peer
access-list FROM-OUTSIDE permit esp host sanfran-vpn-peer host
hongkong-vpn-peer
access-list FROM-OUTSIDE permit esp host dublin-vpn-peer host
hongkong-vpn-peer
access-list FROM-OUTSIDE permit esp host partner-vpn-peer host
hongkong-vpn-peer
access-list FROM-OUTSIDE deny ip any any log
!
! ACL for traffic inbound to inside interface from the Intranet
access-list FROM-INSIDE deny tcp any any eq 1863
```

```
access-list FROM-INSIDE deny tcp any 207.46.104.20 eq http
access-list FROM-INSIDE deny tcp any 207.46.110.252 eq http
access-list FROM-INSIDE deny tcp any 210.158.219.57 eq http
access-list FROM-INSIDE deny tcp any 66.218.75.184 eq http
access-list FROM-INSIDE deny tcp any any eq pop3
access-list FROM-INSIDE permit tcp any host webserver eq www
access-list FROM-INSIDE permit tcp any host webserver eq https
access-list FROM-INSIDE permit udp host int-dns host ext-dns eq
domain
access-list FROM-INSIDE permit tcp host int-dns host ext-dns eq
domain
access-list FROM-INSIDE permit tcp any any eq www
access-list FROM-INSIDE permit tcp host ciscoworks host webserver eq
ssh
access-list FROM-INSIDE permit tcp host ciscoworks host ext-dns eq
ssh
access-list FROM-INSIDE permit tcp host ciscoworks host ext-email eq
ssh
access-list FROM-INSIDE permit tcp host ciscoworks host ntp-server eq
ssh
access-list FROM-INSIDE permit tcp host ciscoworks host pss-switch eq
ssh
access-list FROM-INSIDE deny ip any any log
!
! ACL for traffic inbound to DMZ interface from the Public Services
! Segment
access-list FROM-PSS permit tcp host ext-email host int-email eq smtp
access-list FROM-PSS permit tcp host ext-dns host int-dns eq domain
access-list FROM-PSS permit udp host ntp-server host ext-ntp-cuhk eq
123
access-list FROM-PSS permit udp host ext-dns any eq domain
access-list FROM-PSS permit tcp host ext-dns any eq domain
access-list FROM-PSS permit tcp host webserver host appserver eq 135
access-list FROM-PSS permit tcp host webserver host appserver range
5000 5020
access-list FROM-PSS permit udp host webserver host ciscoworks eq
syslog
access-list FROM-PSS permit udp host ext-dns host ciscoworks eq
syslog
access-list FROM-PSS permit udp host ext-email host ciscoworks eq
syslog
access-list FROM-PSS permit udp host ntp-server host ciscoworks eq
syslog
access-list FROM-PSS permit udp host pss-switch host ciscoworks eq
syslog
access-list FROM-PSS deny ip any any log
!
! ACL for traffic inbound to APP interface from the Application
! Segment
access-list FROM-APP permit tcp host app-server host database-server
eq 1433
access-list FROM-APP permit udp host app-server host database-server
eq 1434
access-list FROM-APP permit tcp host app-server host database-server
eq 135
access-list FROM-APP permit tcp host app-server host database-server
range 5000 5020
access-list FROM-APP deny ip any any log
!
! ACL IPSEC-NO-NAT for use with Nat 0 to prevent NAT'ing of IPSec
! traffic. NAT breaks IPSec.
```

```
! NO-NAT for outbound IPSec traffic to branch offices and partner
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.2.0
255.255.255.0
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.3.0
255.255.255.0
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.4.0
255.255.255.0
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.5.0
255.255.255.0
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.6.0
255.255.255.0
!
! NO-NAT for outbound IPSec traffic for remote VPN users. ACL defines
! traffic between inside and ip local pool for NO-NAT.
access-list IPSEC-NO-NAT permit ip 10.0.1.0 255.255.255.0 10.0.20.0
255.255.255.0
!
! number of lines the console can display without the need for paging.
pager lines 24
!
! Syslog configuration. Log to Ciscoworks management server.
logging on
logging timestamp
logging trap debugging
logging host inside 172.16.3.2
!
! Allow ICMP Unreachable messages (type 3) at the outside interface
! and deny ICMP echo replies. Denying Type 3 ICMP messages disables
! MTU path discovery which causes problems for IPSec traffic.
icmp deny any echo-reply outside
icmp permit any unreachable outside
!
! set Message Transfer Unit for all interfaces to 1500 bytes
mtu outside 1500
mtu inside 1500
mtu pss 1500
mtu application 1500
!
! Set IP addresses of PIX interfaces.
ip address outside hongkong-vpn-peer 255.255.255.0
ip address inside 10.0.1.1 255.255.255.0
ip address pss 172.16.1.1 255.255.255.0
ip address application 172.16.2.1 255.255.255.0
!
! Configure IDS features of PIX
ip audit name ATTACK-RULE attack action alarm drop reset
ip audit name INFO-RULE info action alarm
!
! Apply IDS attack and info rules to all PIX interfaces
ip audit interface outside info-rule
ip audit interface outside attack-rule
ip audit interface inside info-rule
ip audit interface inside attack-rule
ip audit interface pss info-rule
ip audit interface pss attack-rule
ip audit interface application info-rule
ip audit interface application attack-rule
!
ip audit info action alarm
ip audit attack action alarm
!
```

```
!
! Configure anti-spoofing on firewall interfaces
ip verify reverse-path interface outside
ip verify reverse-path interface pss
ip verify reverse-path interface application
!
! Define dhcp pool for Remote VPN users
ip local pool VPNPOOL 10.0.10.1-10.0.10.254
!
! Store history data used to display statistics used in PDM
! Monitoring tab
pdm history enable
!
! set arp cache timeout to 14400 seconds
arp timeout 14400
!
! Use global command together with nat command (below) to
! assign a public IP to a connection initiated from an
! internal host. NAT pool followed by PAT address.
global (outside) 1 202.168.2.200-202.168.2.253 255.255.255.0
global (outside) 1 202.168.2.254
!
! Define NAT for inside hosts accessing PSS web server
global (pss) 1 172.16.0.200-172.16.0.254 netmask 255.255.255.0
!
! Access list to avoid NAT'ing IPSec traffic as defined in ACL IPSEC-
! NO-NAT above. NAT Traversal is available in newer versions of PIX
! software.
nat (inside) 0 access-list IPSEC-NO-NAT
!
! Enable Network Address Translation for hosts on the internal
! network 10.0.1.0 initiating an outbound connection to the Internet
! or to the corporate web server. The 1 is the NAT ID defined in the
! corresponding global commands above. The command indicates the
! hosts eligible for NAT.
nat (inside) 1 10.0.1.0 255.255.255.0
!
! Define static translations for outside hosts accessing DMZ Web
server
static (pss,outside) 202.168.2.5 webserver
!
! Define static translations for outside hosts accessing External DNS
! server
static (pss,outside) 202.168.2.6 ext-dns
!
! Define static translations for external mail to SMTP relay
static (pss,outside) 202.168.2.7 ext-email
!
! Define static translations for NTP to GIAC NTP server
static (pss,outside) 202.168.2.8 ntp-server
!
! Define static translation for DMZ SMTP relay to internal SMTP
static (inside, pss) ext-email int-email
!
! Define static translations for external DNS to internal DNS
static (inside, DMZ) ext-dns int-dns
!
! Apply ACLs to interfaces
access-group FROM-OUTSIDE in interface outside
access-group FROM-INSIDE in interface inside
access-group FROM-PSS in interface pss
```

```
access-group FROM-APP in interface app
!
! set static routes for networks not directly connected to the PIX
route outside 0.0.0.0 0.0.0.0 202.168.2.1
route inside 10.0.1.0 255.255.255.0 192.168.2.1 1
route inside 172.16.3.0 255.255.255.0 192.168.2.1 1
route inside 172.16.4.0 255.255.255.0 192.168.2.1 1
!
! Set default Translation slot timeout of 3 hours
timeout xlate 3:00:00
!
! Set default connection timeout for various connection
! types
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
!
! Triple-A protocol setup
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
!
! Internal AAA server configured as part of MYTACACS server group and
! all inbound connections require CSACS authentication
aaa-server MYTACACS protocol tacacs+
aaa-server MYTACACS (inside) host 10.0.1.6 tacacskey123 timeout 5
aaa authentication include tcp/0 outside 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 MYTACACS
!
! Enable inside interface for PDM access via browser
http server enable
http 10.0.1.0 255.255.255.0 inside
!
! Define SNMP setup
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
!
! Enable SYN flood protection
floodguard enable
!
! GIAC VPN configuration for Telecommuter Remote VPN Access
! and Site-to-site VPN connectivity to branch offices follows.
! Permit IPSec packets to bypass our PIX ACL's
sysopt connection permit-ipsec
!
! Define IPSec transform sets
crypto ipsec transform-set HONGKONG esp-3des esp-md5-hmac
!
! define dynamic crypto map for remote VPN clients
crypto dynamic-map DYNAMIC-MAP 10 match address outside IPSEC-REMOTE-
VPN
crypto dymanic-map DYNAMIC-MAP 10 set transform-set HONGKONG
!
! define static crypto maps for partner and branch office VPNs.
crypto map VPNMAP 10 ipsec-isakmp
crypto map VPNMAP 10 match address IPSEC-PARTNER
crypto map VPNMAP 10 set peer partner-vpn-peer
crypto map VPNMAP 10 set transform-set HONGKONG
```

```
!
crypto map VPNMAP 20 ipsec-isakmp
crypto map VPNMAP 20 match address IPSEC-GUANGZHOU
crypto map VPNMAP 20 set peer guangzhou-vpn-peer
crypto map VPNMAP 20 set transform-set HONGKONG
!
crypto map VPNMAP 30 ipsec-isakmp
crypto map VPNMAP 30 match address IPSEC-BRISBANE
crypto map VPNMAP 30 set peer brisbane-vpn-peer
crypto map VPNMAP 30 set transform-set HONGKONG
!
!
crypto map VPNMAP 40 ipsec-isakmp
crypto map VPNMAP 40 match address IPSEC-SANFRAN
crypto map VPNMAP 40 set peer sanfran-vpn-peer
crypto map VPNMAP 40 set transform-set HONGKONG
!
crypto map VPNMAP 50 ipsec-isakmp
crypto map VPNMAP 50 match address IPSEC-DUBLIN
crypto map VPNMAP 50 set peer dublin-vpn-peer
crypto map VPNMAP 50 set transform-set HONGKONG
!
! Using a higher index for dynamic crypto map is more efficient
! vis-à-vis processing since we would expect the remote VPN to see
! less activity
crypto map VPNMAP 65530 ipsec-isakmp dynamic DYNAMIC-MAP
crypto map VPNMAP client authentication MYTACACS
crypto map VPNMAP interface outside
!
! ISAKMP configuration for GIAC branch offices and partner. Use
! different keys for different peers for better security.
isakmp enable outside
isakmp key ******** address guangzhou-vpn-peer netmask
255.255.255.255
isakmp key ******** address brisbane-vpn-peer netmask 255.255.255.255
isakmp key ******** address sanfran-vpn-peer netmask 255.255.255.255
isakmp key ******** address dublin-vpn-peer netmask 255.255.255.255
isakmp key ******** address partner-vpn-peer netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
!
! Client VPN Remote Access for GIAC telecommuters. Configure VPN
! Group to push configuration to remote Cisco VPN client software.
vpngroup REMOTEVPN address-pool VPNPOOL
vpngroup REMOTEVPN dns-server int-dns
vpngroup REMOTEVPN wins-server int-wins
vpngroup REMOTEVPN default-domain giac.org
vpngroup REMOTEVPN idle-time 1800
vpngroup REMOTEVPN password ********
!
! Set timeouts for inactive telnet sessions
telnet timeout 5
!
! Only Allow ssh to PIX inside interface. Clear-text telnet is not
! permitted based on the GIAC security policy.
ssh 10.0.1.0 255.255.255.0 inside
!
```

```
! Set timeouts for inactive ssh sessions
ssh timeout 5
!
! Set timeouts for inactive console sessions
console timeout 0
!
! Set the display terminal width to 80 characters
terminal width 80
!
! cryptographic checksum of PIX configuration
Cryptochecksum:b545dc7361dd9c9eaa13c0e22af0577d
```

Appendix III

Appendix III shows the Public Services Segment Catalyst switch Port Security configuration commands and switch configuration file extract.

Enter Interface configuration mode and configure the port as an access port.

```
2970switch(config)#int fa0/1
2970switch(config-if)#switchport mode access
```

Then enable port security with the following command.

```
2970switch(config-if)#switchport port-security
```

Instruct the switch to set a maximum MAC address of 1 for the port. The sticky keyword in the following configuration tells the switch to learn the first MAC address from the attached device and add this MAC as a secure MAC address to the switch configuration.

```
2970switch(config-if)#switchport port-security max-
address sticky
```

This is followed by the command to shut down the port if it is compromised.

```
2970switch(config-if)#switchport port-security violation
shutdown
```

The following Catalyst IOS based switch configuration shows configuration of port security on a single interface of the Public Services Segment switch.

```
hostname hkg-pss-switch
!
ip address 172.16.1.7 255.255.255.0
ip default-gateway 172.16.1.1
!
enable password level 15 <enablepassword>
!
interface FastEthernet0/2
 no cdp enable
 switchport mode access
 switchport port-security
 switchport port-security maximum 6
 switchport port-security aging time 5
 switchport port-security aging static
 switchport port-security mac-address sticky
 no ip address
!
line console
```

Bibliography

Following in alphabetical order is a list of reference books which assisted in the writing of this paper.

CCSP Study Guide: Cisco Secure PIX Firewall Advanced – CiscoPress
Author: Behzad Behtash
http://www.ciscopress.com/title/1587051494

CCSP Study Guide: Securing Cisco IOS Networks – CiscoPress
Author: John F. Roland
http://www.ciscopress.com/title/1587051516

CISCO IOS Access Lists – O'Reilly
Author: Jeff Sedayao
http://www.oreilly.com/catalog/cisrtlist/

Cisco Router Firewall Security – CiscoPress
Author: Richard A. Deal
http://www.ciscopress.com/title/1587051753

Hardening Cisco Routers – O'Reilly
Author: Thomas Akin
http://www.oreilly.com/catalog/hardcisco/

Hardening Network Infrastructure
Author: Wes Noonan
http://books.mcgraw-hill.com/getbook.php?isbn=0072255021

Inside Network Perimeter Security (1st Edition)
Authors: Northcutt, Zeltser, Winters, Frederick, Ritchey
http://www.amazon.com/exec/obidos/ASIN/0735712328/103-1198569-0788622

Network Security Fundamentals – Cisco Press
Authors: Gert De Laet & Gert Schauwers
http://www.ciscopress.com/title/1587051672

Tao of Network Security Monitoring, The: Beyond Intrusion Detection
Author: Richard Bjetlich
SQUIL Chapter
http://www.awprofessional.com/title/0321246772

Best damn CISCO Internetworking book period, The
Author: Callisma
http://www.syngress.com/catalog/?pid=2530