Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

GCFW Practical Assignment v2.0

Security Architecture for GIAC Enterprises

Prepared by Jim Hietala

Submitted March 4, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

This paper describes a network security architecture for GIAC Enterprises, a fictitious company that is in the fortune cookie business. The paper describes the business operations of GIAC Enterprises, defines the access requirements for employees, customers, and partners of GIAC, and it presents a new secure network architecture. In addition, a security policy and tutorial is provided for the eSoft InstaGate firewall unit. A plan for technical validation of the firewall policy is provided, including actual validation results. Finally, the paper describes and analyzes a series of attacks on a previous secure network design for GIAC Enterprises.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.0 Security Architecture for GIAC Enterprises

The management of GIAC Enterprises, having grown IT in a somewhat "helter-skelter" fashion since the company's inception, has determined that securing access to corporate IT systems is now a key business objective. Accordingly, they have asked us to develop a new, secure e-business infrastructure. Our charter is to analyze, recommend, implement, and test a new network infrastructure.

Management is also concerned about employee misuse of the Internet resource, and about the growing security and productivity problems associated with e-mail borne viruses, SPAM, and peer-to-peer application use by employees. Consequently, GIAC's management have given us a charter to not only develop an overall architecture that will secure GIAC's Internet access, but one which will specifically address the following issues relating to internet access as well:

- Controlling/monitoring employee Internet access
- Protecting against viruses
- Providing a mechanism to limit SPAM
- Providing a control mechanism for peer-to-peer traffic (including popular file sharing networks), and instant messaging

Economic constraints

GIAC's management is highly cost-conscious, and has tasked us with providing solid network security, and solving the internet use and abuse problems noted above, while doing so on a very tight budget. Like many small-medium sized businesses, GIAC does not have a wealth of in-house technical expertise in the area of information security, and as a result they have directed us to seek out solutions that are easily managed. Taken together, these two objectives have caused GIAC's management to direct us to target appliance-type solutions, in the belief that they will be both cost-effective and simple to manage on an ongoing basis. GIAC management's desire to keep costs to a minimum has also caused us to forgo some options that we would otherwise recommend, including having dual internet connections, multiple routers, and multiple firewalls for redundancy and failover. In addition, while we would recommend the use of a VPN device that is separate from the firewall for optimal security, economic constraints have limited us to seeking an integrated solution.

Scope of assignment

GIAC's management has given us the following instructions regarding what is in scope and out of scope for this engagement:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In scope:

Define a new secure network architecture for GIAC, create security policy for the firewall, VPN, and border router, and validate the firewall policy. Make recommendations regarding other security practices that can enhance the security of GIAC's network and IT resources.

Out of scope:

Describing how to harden hosts, servers, workstations, and other IT systems except for those that comprise the perimeter security for GIAC.

And, while we have recommended that GIAC mandate and/or implement remote firewalls and anti-virus products, for customers, suppliers, and mobile GIAC employees, implementation of these is not a part of this project.

1.1 Business Operations

As a fast-growing e-business company, GIAC Enterprises derives all of it's revenues from the sales of fortune cookie sayings through its commercial website. The company has grown rapidly in the last few years, and as it has done so, it has sought to keep costs down by leveraging the Internet for communications, for marketing purposes, and as a mechanism to enable sales wherever possible.

The various IT stakeholders in GIAC's operations include employees, suppliers, sales partners, customers, and the general public.

Employees- GIAC's employee base consists of three broad categories of users, fixed-location office-based, fixed-location home-based teleworkers, and mobile users (salespeople and executives).

Suppliers- GIAC subcontracts the development of clever fortune cookie sayings to numerous firms specializing in the creation of unique, meaningful messages. These firms are located all over the world, and are very competitive with each other.

Sales partners- GIAC uses a mixed sales channel for the fortune cookie sayings, including not only internal salespeople who call on large accounts directly, but also 3rd party sales agents who sell GIAC's fortune cookie sayings to smaller fortune cookie manufacturers in different parts of the world. The 3rd party sales agents generally have Internet access, however the access speeds available vary considerably from partner to partner.

© SANS Institute 2004, Author retains full rights.

GIAC's critical IT assets that support its business operations include the following:

SQL Server- GIAC uses an SQL database server, running 2 key applications. The first is a fortune cookie database, and the second is a sales database containing records of all customers and prospects, and their purchasing activity.

Payroll- GIAC outsources payroll processing to a 3rd party firm.

E-Mail- GIAC has implemented a Microsoft Exchange server on the local LAN.

Web server- GIAC has implemented a Microsoft IIS Internet Server, running on Windows 2000. The IIS webserver is presently hosted in the corporate data center, and is on the corporate LAN. One of our recommendations is that the web server be moved, along with other systems requiring Internet access, to a new screened-subnet zone, protected by a firewall.

Internal LAN- GIAC has had in place for some time a flat (non-switched) 10/100 ethernet LAN that connects internal employees to the IT resources, and to the Internet. GIAC presently uses single class C subnet, with public Internet addresses, for its IP addressing scheme.

Internet connection- GIAC has a T-1 connection to the Internet. The access router is currently provided by the service provider, is managed by the service provider, and is included in the monthly service. Because the access router is a key component of a defense-in-depth strategy, we are recommending that GIAC purchase an access router, and manage the security of the router.

Security- GIAC has until now asked the service provider to implement filtering on the access router, to disallow any non-essential protocols, services, and access.

1.2 Security policy

In developing our security architecture, we are utilizing several guiding principles, which are a part of GIAC's overall security policy:

- Our standard policy will be to restrict access by all user groups to only those systems, applications, protocols, and services which

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

management has decided are appropriate, and to deny access to all others.

- We will also seek to utilize a defense in depth approach by providing layers of security controls at multiple points in the network design. The network design will segment various workstations, systems, and servers into zones, such that appropriate access controls can be established on inbound and outbound traffic.

- We will require the use of SSL by suppliers and customers who will be accessing the GIAC secure web server. We will use Verisign[1] certificates to provide customers and suppliers with assurance as to the authenticity of the GIAC web server.

- We will pay particular attention to exposures that could result from opening up access to GIAC's network from systems that are outside of GIAC's direct control (including customer systems and networks, supplier systems and networks, and remote employee systems), and will attempt to mitigate these exposures through making educated design choices, and through recommending additional security products to lock down these remote systems and networks.

- Although outside of the scope of this project, we recognize that active patch management is key to ensuring a secure network environment. We have recommended that GIAC consider automated tools to perform patch management on both servers and workstations.

- Similarly, we are recommending that GIAC consider using a product such as Tripwire[2], which will establish baselines for all files used in key systems, both to enhance security, and to add some discipline to the change management process.

1.2 Access Requirements

	Outbound access requirements	Outbound to Internet services, protocols, ports	Inbound access requirements	Inbound to LAN, services, protocols / ports
General public	Not applicable/none	Not applicable/none	To general GIAC web server,	HTTP, HTTPS

[1] http://www.verisign.com
[2] http://www.tripwire.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

			inbound mail to GIAC	
Customers	Not applicable/none	Not applicable/none	To secured web server, to purchase fortunes	HTTPS
Suppliers	Not applicable/none	Not applicable/none	To secured web server, to upload their fortunes	HTTPS
Partners	Not applicable/none	Not applicable/none	To secured web server, to purchase batches of fortunes, download, and perform translations	HTTPS
System administrators	Internet access, e-mail, and admin access to DMZ systems and router	DNS internal HTTP, HTTPS, SMTP, SSH		
Employees on internal GIAC LAN	Internet access, e-mail	DNS internal HTTP, HTTPS, SMTP	None to individual systems	
Mobile employees (salespeople & executives)	Internet access, e-mail	When on LAN: DNS internal HTTP SMTP	Inbound VPN access to the sales database, internet access, and e-mail	When mobile: DNS, HTTP, SMTP VPN- IPSEC, IKE

© SANS Institute 2004, Author retains full rights.

1.3 Architectural Overview

The network security design for GIAC Enterprises includes the following components, grouped according to their physical location on the network.

Border Router- We have decided to use a Cisco 3620 model router, running IOS version 12.3. The 3620 router has enough performance to adequately support GIAC's WAN requirements for the foreseeable future. It also can be used to perform a variety of access control functions via

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access control lists, and will serve as a key component of our defense-in-depth strategy.

Internet Firewall- The primary firewall is the eSoft InstaGate PRO unit, running OS version 3.1-20031001. This appliance-based firewall platform is based on a hardened LINUX OS, and performs stateful packet inspection of inbound and outbound traffic. It includes an integrated VPN concentrator capable of supporting site-to-site IPSEC connections, client-to-site IPSEC connections, and PPTP connections. It also includes an integrated proxy server (based on SQUID). However, in our network design, we have decided to place a proxy server behind the firewall, in a content security appliance. The system can be deployed in a high-availability configuration, with primary and secondary units for failover, however in order to keep costs in line with management expectations, we are not proposing this configuration. The InstaGate PRO unit was chosen for its high degree of integration, ease of deployment and ongoing management, and relatively modest cost. The InstaGate PRO is a true appliance solution, with updates and security patches to the operating system and firewall software being made to the unit remotely, and automatically, by the vendor. The PRO appliance will act as the DNS server for the LAN in the GIAC network. It will also act as the DHCP server for the GIAC LAN. While we would prefer to have both of these functions performed on separate servers from a security standpoint, the software to support these functions is included with the InstaGate, which will help us to keep the overall project within budget limitations. We are also configuring the PRO unit with an optional IDS/IPS software module, described below, and with the application filtering softpak to scan all Internet traffic for instant messaging and peer-to-peer protocols, and to block their use from the corporate LAN. The application filter is a key part of the overall solution that GIAC's management has asked for, in terms of controlling the use of the internet resource.

External web services zone- This screened subnet will be created using a DMZ interface on the Internet firewall, and will be used as a separate zone, with unique firewall rules, containing the public web server, and secure web server. For the most part, systems on this network zone will only communicate with the Internet, with 2 exceptions. The secure web server will need to communicate with the SQL server housing the sales and fortune cookie database applications on the Database and admin network zone, for updating the fortune cookie database, and sales inventory records. We have defined that this will happen via a mix of HTTPS (in from remote users), and SQL (from the Secure Web server to the SQL server on the admin network zone) protocols. Finally, administrative and operations personnel will need secure access to both systems on the external web services zone, from the admin workstations. The administrators will use HTTPS and SSH for this purpose.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Internal router- We will use a Cisco 3600 router as an internal router. This router will provide the connection from the internal Internet services network, employee workstations subnet, and database network to the Internet. And although we have not included a configuration for this device, we would strongly suggest that GIAC take advantage of the filtering and access control capabilities of this router, to segment groups of users and systems, and lock down internal access. For example, access control lists can be implemented in this router to limit access to the SQL server, and the logging server, to only those employees with a specific business reason to do so, and to block access from all other employee workstations.

Internal Internet service network- This network segment will house the internal mail server.

Database and admin zone- This network segment will house the logging server, and the SQL server containing the GIAC fortune cookie database, as well as two workstations used by IT operations personnel.

Employee workstation subnet- This network segment is where all of the GIAC employee workstations will be connected.

Personal Firewalls- We recommend that all remote employees approved for VPN access use a personal firewall and desktop anti-virus product at all times. This will help to mitigate the risk that remote workers will be exposed to a virus or worm while operating their computer on an insecure network, and then infect the rest of GIAC's operations when they connect to the corporate LAN (either remotely via VPN tunnel, or locally on the LAN). All GIAC suppliers and customers wishing to use the GIAC secure ordering website will be required to certify that they have implemented firewalls for all public access points into their networks. This will help to mitigate the risk that suppliers and customers will be exposed to a virus or worm, and then infect the rest of GIAC's operations when they connect to the corporate secure web server.

Secure Web server- We will implement a secure web server that will be the system that external suppliers use to provide the fortune cookie sayings, and that customers use to place orders. The server will be based on Apache (2.0.48), running on a Red Hat Linux system (Enterprise Linux ES3). We have recommended that GIAC harden this server by removing all unnecessary services, and that they configure the web server to make it harder to fingerprint. In addition, we are recommending that GIAC invest in a HIDS/HIPS type product for this server- either the Cisco/Okena[3]

[3] http://www.cisco.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

solution, or the Network Associates/Entercept[4] product. Either of these solutions will identify attempted intrusions, and block them at the web server. Because web servers are such attractive targets, putting HIDS/HIPS capabilities on them is an important addition to the layered network security we are seeking to achieve.

Public Web server- GIAC will continue to use their Microsoft IIS Internet Server (IIS ver 6.0), running on Windows 2000 (5.0SP4). We have recommended that GIAC harden this server by removing all unnecessary services. As above, we are recommending that GIAC invest in a HIDS/HIPS solution for this web server. Although a little less business-critical than the secure web server, the public web server could still be subject to defacement attacks, worms, viruses, and other malware, as well as attempts to gain root access, and we want to eliminate these possibilities.

IDS/IPS system- We will use the eSoft IDS/IPS SoftPak for the InstaGate PRO unit to detect and prevent against intrusions. This security software module was developed by Latis Networks[5], and is a commercial product based upon the SNORT software. As it is integrated into the firewall, it is able to detect and prevent intrusions on the external, internet-facing Ethernet interface, the screened subnet Ethernet interface, or the internal interface. The IDS/IPS module integrates well with the firewall, and allows automatic blocking of intrusion attempts through the use of dynamically implemented firewall rules.

ESoft InstaGate SCM Secure Content Management appliance- This appliance solution will be deployed between the firewall and the internal networks, and will be used to provide proxy services, and for anti-virus e-mail scanning, URL filtering of outbound web traffic, and anti-spam e-mail scanning. Utilizing the SCM appliance as a proxy server makes sense, because the appliance will also be filtering outbound web traffic based on destination URL. The SCM appliance will allow us to address the concerns of GIAC's management regarding viruses, inappropriate web site use by employees, and the growing problem of SPAM. The SCM appliance provides tools to reduce and eliminate SPAM, and to control what kinds of websites employees are allowed to access over the Internet. Access to inappropriate sites, as defined by GIAC management, will be blocked. The SCM appliance also provides reporting tools on web and e-mail use, and anti-virus tools that will ensure that viruses are blocked at the SCM device. Because many of today's most serious security threats against corporate networks are delivered via e-mail, the SCM appliance is a key component of our defense-in-depth strategy.

[4] http://www.nai.com
[5] http://www.stillsecure.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.4 IP Addressing Scheme

GIAC will use the following IP addressing scheme in defining the different segments of its network:

IP Address Range	Used For:
110.1.1.0/24	GIAC internet access
110.1.1.1	Border router wan
110.1.1.10	Border router lan
110.1.1.20	Firewall wan
110.1.1.30	Firewall secondary IP, NAT'ed to 192.168.3.2
110.1.1.40	Secondary IP, NAT'ed to 192.168.3.4
110.1.1.41	Secondary IP, NAT'ed to 192.168.3.5
110.1.2.0/24	Firewall DMZ, external web services zone
110.1.2.1	Firewall DMZ port
110.1.2.2	Public web server
110.1.2.3	Secure web server
192.168.1.0/24	Firewall to LAN router
192.168.1.1	Firewall lan port
192.168.1.2	Internal router wan
192.168.1.3	InstaGate SCM appliance
192.168.2.0/24	Internal internet services subnet
192.168.2.1	Internal router port
192.168.2.2	Mail server
192.168.3.0/24	Database and admin zone
192.168.3.1	Internal router port
192.168.3.2	Logging server
192.168.3.3	SQL database
192.168.3.4	Admin workstation
192.168.3.5	Admin workstation
192.168.4.0/24	Employee workstations subnet

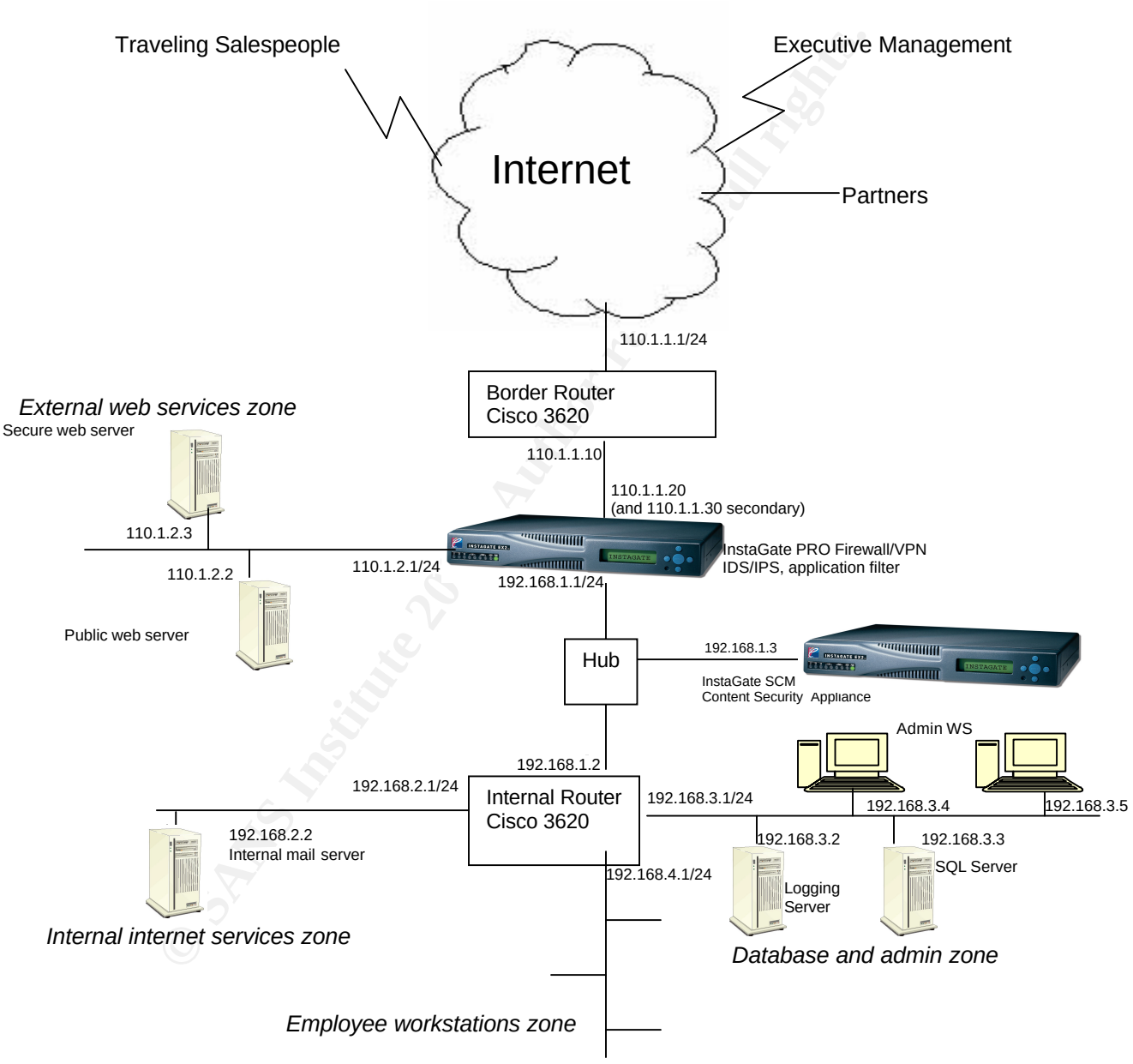
Note: We have used addresses above that are defined by IANA in RFC 1466[6] as reserved IP addresses for all external public IP addresses, in lieu

[6] http://www.apps.ietf.org/rfc/rfc1466.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

of using real IP addresses that belong to actual organizations. We will be using private, non-routable IP addresses, as defined in RFC 1918[7] for all internal network segments. We will also be using Network Address Translation on the internal network zones, to provide an added layer of security. In addition, we will be using a proxy server for Internet access.

1.5 Network Diagram of Proposed Architecture



[7] http://www.apps.ietf.org/rfc/rfc1918.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.0 Security Policy and Tutorial

In developing the security policy for the border router and the firewall, we have sought to address the most common and serious attacks, as identified in the SANS Top 20 Internet Security Vulnerabilities[8]. Many of the guidelines suggested for developing a secure perimeter in Inside Network Perimeter Security[9] have also been implemented.

2.1 Cisco 3620 Border Router Security Policy

Because the firewall that we will be using provides for stateful packet inspection, we will not be using reflexive access control lists on the router, only extended ACL's. The rules and CLI commands below harden the router, and implement the access control that we want to put in place in the border router, which is the first point of entry into GIAC's network. We are implementing extensive filtering in the border router, both to augment the capabilities of the firewall at the border of the GIAC network, but also to "lighten the load" on the firewall, by exposing it to less traffic. As the firewall is a multi-function security appliance that is being asked to perform some other security tasks, we want to enhance it's performance by filtering packets in the border router. The Cisco IOS manual for version 12.3[10] was invaluable in developing this security policy, and the resulting ACL's.

2.1.1 We will start by establishing secure administrative passwords to the router, putting restrictions on console and auxiliary port access, and adding an ACL that restricts where virtual terminal access can occur from:

Rule/Command	Purpose	Importance
enable secret <password>	Encrypts the administrative password using an MD5 hash	We don't want the administrative password stored in plaintext
service password-encryption	Encrypts any other passwords stored in the router, such as telnet passwords	We don't want other passwords stored in plaintext
username <username> password 7	Adds an additional username and password for accessing the router via the console, and specifies that the Cisco defined	

[8] http://www.sans.org/top20/
[9] Inside Network Perimeter Security Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey, © New Riders Publishing 2003
[10] http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	encryption algorithm will be used	
line aux 0 no exec transport input none	Restricts access to the auxiliary port	Locks down access
line con 0 exec-timeout 1 log in local	Requires authentication, and applies a more restrictive timeout of 1 minute	Locks down access
access-list 15 permit host 110.1.1.40 log access-list 15 permit host 110.1.1.41 log access-list 15 deny any any log	Allows virtual terminal access from these 2 administrative systems, and denies access from all other addresses	Locks down access to the router console so that it can only occur from 2 internal administrative systems
line vty 0 4 access-class 15 in password <password> login transport input ssh	Applies the previous ACL, and forces SSH to be used	SSH is more secure than simple Telnet

2.1.2 In order to maximize the security of the border router, we will disable all services and protocols that are not absolutely necessary on the device. To turn off these unnecessary services on the Cisco router, we will implement the following rules & commands:

Rule/Command	Purpose	Importance
no ip http server	Explicitly disables HTTP server from router	Not needed by GIAC, more secure to explicitly remove
no snmp-server	Explicitly disables SNMP server from router	Not needed by GIAC, more secure to explicitly remove
no cdp run	Explicitly disables Cisco Discovery Protocol from router	Not needed by GIAC, more secure to explicitly remove
Service tcp-keepalives-in	Eliminates a DOS attack possibility, using VTY's	DOS attacks are a prime concern on the border router
no service tcp-small-servers	Eliminates TCP small services	Not needed by GIAC, more secure to explicitly remove
no service udp-small-servers	Eliminates UDP small services	"
no ip bootp server	Eliminates Bootp	"
no service finger	Eliminates IP finger	"
no tftp server	Eliminates TFTP	"
no domain-lookup	Disables DNS name lookups from the router, which we don't need	"
no boot network no service config	Disallows the router from booting over the network, and loading it's configuration over the	"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	network	
no ip identd	Identd is a service that provides information about the system	We don't want to provide any extra information to attackers
ntp disable	Eliminates Network Time Protocol	Not needed by GIAC, more secure to explicitly remove

2.1.3 We will also add a warning banner to the border router, which will display upon console access login attempts:

Rule/Command	Purpose	Importance
banner login ^C WARNING: Only authorized users may access this system. Unauthorized access attempts are logged, and will be investigated and prosecuted to the fullest extent of the law. ^C	Displays warning banner	Puts attackers on notice that GIAC takes security and unauthorized access seriously

2.1.4 There are a number of IP routing configuration settings and commands that can strengthen the GIAC network from attack. In addition, we are enabling logging from the router to our logging device in the 192.168.3 subnet, using the secondary IP of 110.1.1.30 which is Nat'ed to this internal address.

Rule/Command	Purpose	Importance
no ip source-route (apply to each interface)	Disallows source routing	More secure to disable
no ip redirects (apply to each interface)	Disallows manipulation of IP return path	More secure to disable
no ip unreachables (apply to each interface)	Filters out unwanted host unreachables, ICMP type 3 messages	If unfiltered, these messages could be used by an attacked to map out our network
ip cef (applied globally)	Required for unicast reverse-path command	Strengthens security
ip verify unicast reverse-path (apply to each interface)		Strengthens security
no ip directed-broadcast	Prohibits directed broadcasts from coming through the GIAC router	More secure to disable
no ip proxy-arp	We don't need to support proxy ARP	More secure to disable
logging on	Enables logging	Logging enables us to recreate and examine unauthorized access attempts
no logging console	Disables logging to console	
logging 110.1.1.30	Directs logging to the server at this address (this is actually a	Allows us to centrally collects logs, and using NAT is the most secure

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	secondary IP address on the firewall, that is NAT'ed to the private address of 192.168.3.2)	way to achieve this
service timestamps log datetime msecs	Defines logging format	

Note: Some of the commands above (e.g. ip directed broadcasts) have been disabled by default in later versions of Cisco IOS, and do not absolutely have to be explicitly disabled. However, specifying that they be turned off upon configuring the border router is a fail-safe, in the event an older version of IOS somehow gets deployed, or Cisco changes the defaults.

2.1.5 Similarly, there are a number of class-maps that can be established to filter out potentially malicious HTTP URL's. This class map list includes both Apache and IIS attacks, which is important as GIAC operates both as web server platforms. We will enable Cisco Express Forwarding, and Network Based Application Recognition, to filter on the following. Note that this technology could also be used to rate limit the amount of bandwidth that can be consumed by various applications. We are choosing to instead just block certain types of traffic using the application filter in the InstaGate PRO firewall appliance further back in the network.

Rule/Command	Purpose	Importance
class-map match-any http-attacks match protocol http url "*default.ida*" match protocol http url "*x.ida*" match protocol http url "*.ida*" match protocol http url "*cmd.exe*" match protocol http url "*root.exe*" match protocol http url MIME "*readme.eml*" match protocol http url MIME "*readme.exe*" match protocol http url "*_mem_bin*" match protocol http url "*/c/*" match protocol http url "*/d/*" match protocol http url "*/ONERROR/*" match protocol http url "*/HTdigest/*" match protocol http url "*/nph-test-cgi/*" match protocol http url "*/_vti_bin/*"	Adds a layer of defense by removing any HTTP URL's containing these known Apache and IIS HTTP attacks	Strengthens security of traffic directed at our web server, and does so at the point of entry into the GIAC network
policy-map mark-inbound-http-attacks class http-attacks set ip dscp 1	Applies the class map	Strengthens security of traffic directed at our web server
interface serial 0 service policy input mark-inbound-http-attacks	Applies the class map	Strengthens security of traffic directed at our web server

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.1.6 Next we will establish the rules for the external interface, using an extended access list:

Rule/Command	Purpose	Importance
access-list 105 permit tcp any 110.1.1.20 eq 25	Allows mail to reach the wan interface of the InstaGate PRO firewall appliance- the PRO will be configured as a mail relay	Needed for email
access-list 105 permit udp any 110.1.1.20 eq 53	Allows DNS traffic from anywhere to reach the DNS server, which is being performed by the PRO appliance	Needed for DNS resolution
access-list 105 permit tcp any 110.1.1.3 eq 80	Allows HTTP traffic to reach the public web server	Needed for web inbound access to GIAC web site
access-list 105 permit tcp any 110.1.1.3 eq 443 log	Allows HTTPS secure traffic to reach the public web server	Needed for web inbound (HTTPS) access to GIAC web site
access-list 105 permit tcp any 110.1.1.4 eq 443	Allows HTTPS secure traffic from partners and customers to reach the secure web server	Needed for uploading of fortunes from suppliers to GIAC, and for ordering of fortunes by customers, via secure web server
access-list 105 permit udp any 110.1.1.20 eq 500 log access-list 105 permit esp any 110.1.1.20 log access-list 105 permit ah any 110.1.1.20 log	These three rules allow VPN traffic from anywhere to reach the VPN gateway in the InstaGate PRO, and logs all VPN access	Needed to provide VPN access to executives and traveling salespeople
access-list 105 permit icmp any any packet-too-long access-list 105 deny icmp any any log	Allows ICMP packet too long messages, and blocks all other ICMP message types, including redirects and	ICMP is a commonly exploited protocol for reconnaissance and DOS attacks, and blocking redirects and echo requests significantly

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	echo requests	strengthens our perimeter security
access-list 105 deny ip 127.0.0.0 0.255.255.255 any log access-list 105 deny ip 224.0.0.0 31.255.255.255 any log access-list 105 deny ip 192.168.0.0 0.0.255.255 any log access-list 105 deny ip 172.16.0.0 0.15.255.255 any log access-list 105 deny ip 10.0.0.0 0.255.255.255 any log	Block all traffic from spoofed internal addresses, and loopback and multicast addresses	No legitimate reason for these addresses to be allowed in via external interface, strengthens security
access-list 105 deny tcp any any range 135 139 log access-list 105 deny udp any any range 135 139 log access-list 105 deny tcp any any 445 log	Block Netbios traffic	No reason to enable Netbios protocols, as they are not used on the GIAC network
access-list 105 deny ip 0.0.0.0 0.255.255.255 any log access-list 105 deny ip 1.0.0.0 0.255.255.255 any log access-list 105 deny ip 2.0.0.0 0.255.255.255 any log access-list 105 deny ip 5.0.0.0 0.255.255.255 any log access-list 105 deny ip 7.0.0.0 0.255.255.255 any log access-list 105 deny ip 23.0.0.0 0.255.255.255 any log access-list 105 deny ip 31.0.0.0 0.255.255.255 any log access-list 105 deny ip 36.0.0.0 0.255.255.255 any log access-list 105 deny ip 37.0.0.0 0.255.255.255 any log access-list 105 deny ip 39.0.0.0 0.255.255.255 any log access-list 105 deny ip 41.0.0.0 0.255.255.255 any log access-list 105 deny ip 42.0.0.0 0.255.255.255 any log access-list 105 deny ip 58.0.0.0 0.255.255.255 any log access-list 105 deny ip 59.0.0.0 0.255.255.255 any log access-list 105 deny ip 71.0.0.0 0.255.255.255 any log ... access-list 105 deny ip 79.0.0.0 0.255.255.255 any log access-list 105 deny ip 85.0.0.0 0.255.255.255 any log ... access-list 105 deny ip 127.0.0.0 0.255.255.255 any log access-list 105 deny ip 173.0.0.0 0.255.255.255 any log ... access-list 105 deny ip 187.0.0.0 0.255.255.255 any log access-list 105 deny ip 189.0.0.0 0.255.255.255 any log access-list 105 deny ip 190.0.0.0 0.255.255.255 any log access-list 105 deny ip 197.0.0.0 0.255.255.255 any log access-list 105 deny ip 223.0.0.0 0.255.255.255 any log access-list 105 deny ip 240.0.0.0 0.255.255.255 any log ... access-list 105 deny ip 255.0.0.0 0.255.255.255 any log	Blocks all traffic from IANA reserved (unallocated IP address ranges[11]), and logs the access attempt	No legitimate reason for these addresses to be allowed in via external interface, strengthens security
access-list 105 deny tcp 110.1.1.0 0.0.0.255 any log access-list 105 deny udp 110.1.1.0 0.0.0.255 any log	Blocks any spoofed traffic coming from the Internet with an IP address in GIAC's assigned IP range, and logs attempts	No legitimate reason for these addresses to be coming from the Internet, strengthens security

[11] http://www.iana.org/assignments/ipv4-address-space

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access-list 105 deny tcp any any range 6000 6255 log	Blocks X-Windows protocol from entering GIAC's network	GIAC does not use this terminal protocol, strengthens security to filter it out
access-list 105 deny udp any any 69 log	Blocks TFTP traffic from entering GIAC's network	No legitimate reason for this protocol to be coming at us from the Internet, strengthens security
access-list 105 deny udp any any 514 log	Blocks syslog traffic from entering GIAC's network	No legitimate reason for this protocol to be coming at us from the Internet, strengthens security
access-list 105 deny udp any range 161 162 log	Blocks snmp traffic from entering GIAC's network	No legitimate reason for this protocol to be coming at us from the Internet, strengthens security
access-list 105 deny any any log	Denies and logs all other traffic	Probably the most important rule in the ACL, this denies all other traffic, and logs invalid access attempts
interface serial 0 access-group-105 in	Applies this access list to the border router wan interface	

In creating this access list, which governs what traffic is allowed in on the WAN interface, we have placed the most frequently used rules (which we believe will be the permit rules for allowed traffic) at the top of the ACL, followed by the specific deny rules, followed by a general deny rule that blocks all traffic not explicitly permitted.

2.1.7 We will also apply rules to the internal (LAN) interface of the border router, to process and filter the information that we allow to pass from the GIAC network to the Internet. We need to do this both for security reasons, and to be a "good network citizen" on the Internet. Following are the rules for an access list to be applied to the internal interface:

Rule/Command	Purpose	Importance
access-list 110 deny icmp any any host-unreachable log	Prohibits any host-unreachable icmp messages from going to the Internet from GIAC's	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from

© SANS Institute 2004, Author retains full rights.

	network	GIAC's network using icmp
access-list 110 deny icmp any any echo-reply log	Prohibits any echo-reply icmp messages from going to the Internet from GIAC's network	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from GIAC's network using icmp
access-list 110 deny icmp any any time exceeded log	Prohibits any time exceeded icmp messages from going to the Internet from GIAC's network	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from GIAC's network using icmp
access-list 110 deny udp any any 69 log	Prohibits any tftp messages from going to the Internet from GIAC's network	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from GIAC's network using tftp
access-list 110 deny udp any any 514 log	Prohibits any syslog messages from going to the Internet from GIAC's network	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from GIAC's network using syslog
access-list 110 deny udp any any range 161 162 log	Prohibits any snmp messages from going to the Internet from GIAC's network	No valid reason for any of these messages to be leaving GIAC's network, prevents any internal misuse or hacking from GIAC's network using snmp
access-list 110 deny tcp any any range 6000 6255 log	Blocks any X-Windows traffic from leaving GIAC's network for the Internet	
access-list 110 deny tcp any any 1433 log	Prohibits any SQL traffic from leaving the	Blocks any SQL-Slammer like attacks from propagating out

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	GIAC network	of the GIAC network, good general practice
access-list 110 deny udp any any 1434 log	Prohibits any SQL traffic from leaving the GIAC network	Blocks any SQL-Slammer like attacks from propagating out of the GIAC network, good general practice
access-list 110 deny tcp any any range 135 139 log access-list 110 deny tcp any any 445 log access-list 110 deny tcp any any 593 log	Prohibits Windows Netbios, RPC traffic from leaving GIAC's network, and logs any such access attempts	Keeps attacks like the Blaster worm from propagating out of the GIAC network, good general practice
access-list 110 deny UDP any any range 135 139 log access-list 110 deny UDP any any 445 log	Prohibits Windows Netbios, RPC traffic from leaving GIAC's network, and logs any such access attempts	Keeps attacks like the Blaster worm from propagating out of the GIAC network, good general practice
access-list 110 permit 110.1.1.0 0.0.0.255 any	Allows access out of GIAC's network to the Internet	
access-list 110 deny any any log-input	Denies all other outbound access, and logs invalid access attempts, including layer 2 info	Would prevent spoofed IP addresses from leaving GIAC's network, prevents network misuse
interface eth0 access-group 110 in	Assigns the access control list to the internal ethernet interface on the border router	

2.1.8 Regarding logging, we have chosen to log most anomolous behavior (those things that we view as potentially representing attacks). This includes logging all administrative access to the router from our two allowed admin workstations, and logging all access attempts that we have created deny rules for, including from invalid addresses, internal addresses, etc. We have chosen to not

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

log valid accesses (e.g. access to the web server, SMTP access to the mail server). We have however enabled logging on HTTPS access to the secure web server, as we feel that this will be useful as an audit trail of partner accesses, and possibly in troubleshooting. Similarly, we have chosen to log all VPN connections, both to provide an audit trail of access, and to assist in troubleshooting of connection attempts.

2.1.9 Finally, we will need to save the configuration changes above, and reboot the router.

2.2 Firewall Security Policy

Because the firewall is an appliance solution, with dedicated hardware, there is little in the way of unnecessary services and ports to disable. The tutorial below describes configuration of the firewall appliance, step-by-step. The security policy for the firewall is included, along with that of the VPN, IDS/IPS, and application filter, as they are all software modules on the InstaGate PRO firewall. In the verification section, we describe our plan, and actual results for verifying that the vendor has indeed done their job, and has patched the underlying LINUX OS to remove vulnerabilities, and that they have disabled those ports and services that are not necessary to the products function as a security appliance. We also will verify that our firewall is performing as we expect, given the security rules below. Please note, the eSoft InstaGate User Guide[12] was of great assistance in configuring the PRO firewall, however the step-by-step instructions below are my own version of how to configure the system (they are not copied from any user guide, in other words). The screen shots are actual screen shots from an InstaGate unit that was configured to implement the policies defined for the GIAC network.

2.2.1 Initial configuration:

The InstaGate ships from the factory with a LAN IP address of 192.168.1.1. In order to configure the unit from a laptop with an ethernet card, an ethernet crossover cable is needed. The cable is plugged into the LAN port of the InstaGate. All system

[12] http://www.esoft.com , and http://support.esoft.com . User manuals are not posted on either site, however they are downloaded to each appliance, and made available locally on the appliance. In addition, esoft hosts a live demo unit that is accessible at http://www.esoft.com/security_solution/hardware_products.cfm , look for “view demo”. By logging in to the demo unit, it is possible to view current manual pages using “online help”.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

configuration is done via a secure web interface. To access the system console, the following url is used:

Https://192.168.1.1:8001

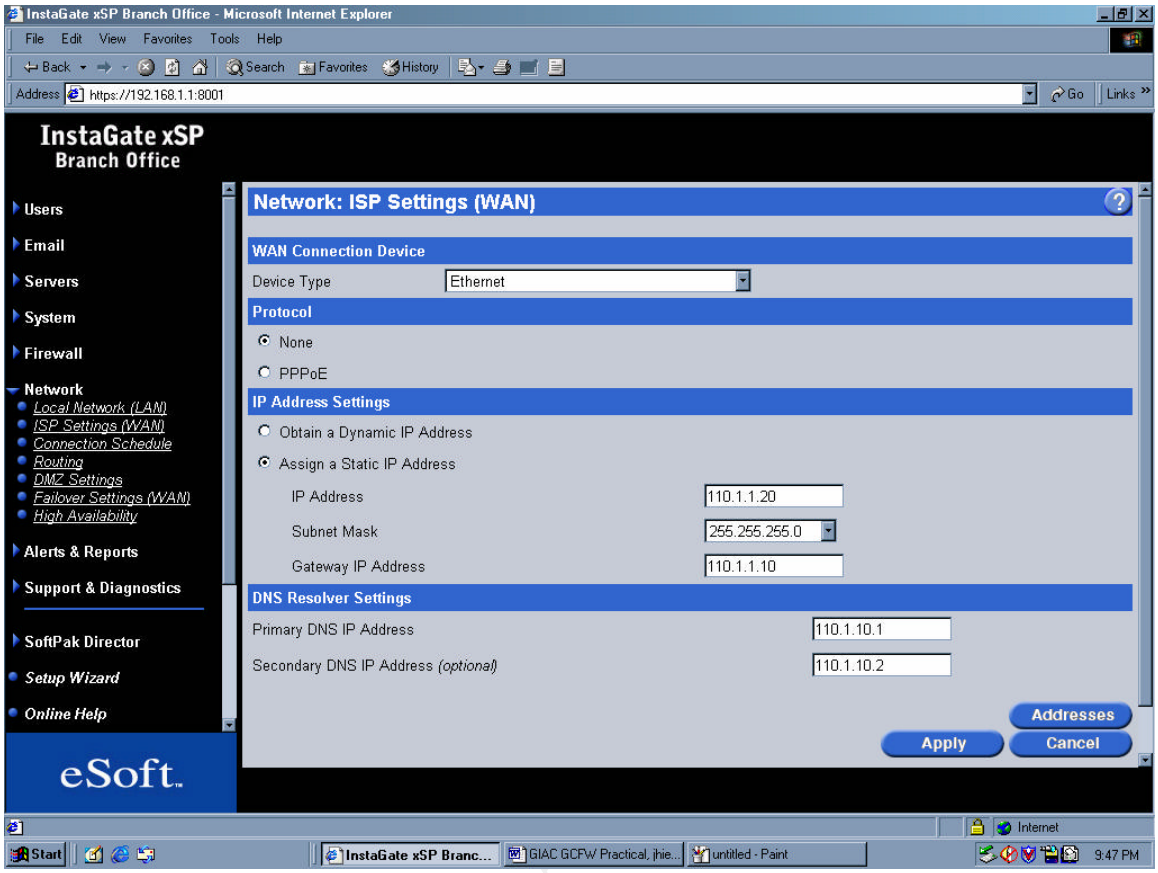
Accessing this URL brings up a login screen, and the default login and password are set to a factory default of:

Login: admin
Password: admin

Our first task is to change the password for the administrative ID, to something more secure than “admin”. This is done by selecting “System”, and then “Administrator” from the main menu, which brings us to a screen that allows the values to be changed. In addition, we have added a local administrator login and password, and enabled LCD access with a PIN.

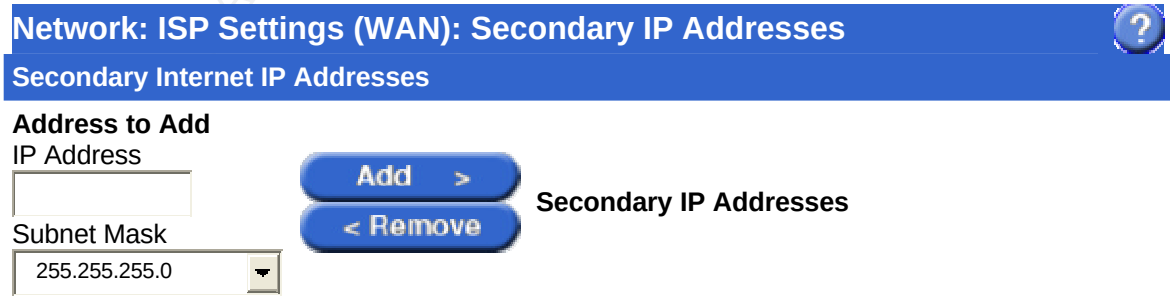
Once this is completed, we will establish the IP addresses for the Wan and DMZ ports, using the following screen, which is reached by selecting “Network” and “ISP Settings Wan” from the main menu. After making the necessary changes to the IP addresses, and gateway address, and applying the changes, the configuration for the Wan port looks like this:

© SANS Institute 2004, Author retains full rights.



Note that the InstaGate PRO will provide DNS services for GIAC, so the DNS addresses above are those of the ISP's DNS servers, to which the GIAC DNS servers will be resolving.

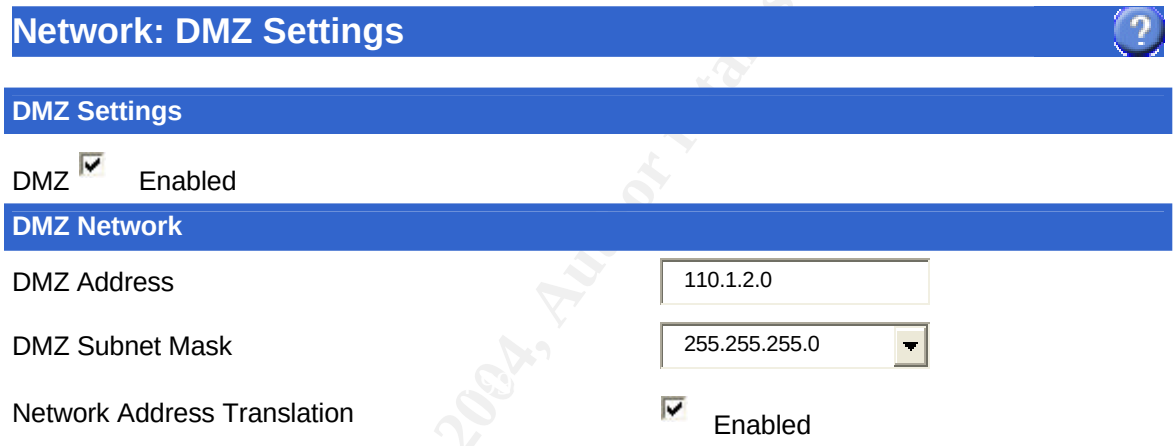
In addition, we will set up a secondary IP address, 110.1.1.30 that will be used as a NAT address for logging from the router, and that will redirect traffic to the internal address of the logging server, 192.168.3.2. This is performed by selecting "Addresses from the above screen, and entering the secondary addresses into the screen below:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

110.1.1.30/255.255.255.0

Next, we establish the IP addressing for the DMZ port, by selecting "DMZ Settings". This is achieved using a similar screen to the one shown above. We have set the DMZ port settings to an IP network of 110.1.2.0, with a subnet mask of 255.255.255.0.



The LAN port settings are performed on a similar screen, and we will leave them at the factory defaults, which are an IP address of 192.168.1.1/24, and DHCP enabled. Note- The InstaGate can be configured to inactivate the internal DHCP server, if the corporation already has a DHCP server in place on their LAN, for instance.

Note that some of these settings can be configured via an LCD panel on the front of the InstaGate PRO unit, including the WAN IP address and netmask, and DHCP settings.

Next, we will set the clock and the host name by selecting "System" and "local options" from the main menu (not shown for the sake of brevity).

The next task is to define the static routes that allow GIAC's network to reach the Internet. Selecting "Network" and "Routing" from the main menu allows the static routes to be added. After

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

adding the route entries needed for the GIAC network, our configuration looks like this:

Select	Target	Subnet Mask	Gateway
◉	192.168.4.0	255.255.255.0	192.168.1.2
○	192.168.3.0	255.255.255.0	192.168.1.2
○	192.168.2.0	255.255.255.0	192.168.1.2

Before establishing the firewall rules, we will enable logging, which is done via the “Firewall” and “Global options” selections from the main menu. A simple check box enables logging. There are 2 other global options that bear mentioning. One is “Respond to external pings”, which is a very important setting. It is presumably useful in some diagnostic situations, but should always otherwise be turned off for security reasons. The second is “Drop all fragmented packets” which is a quick means to have the firewall start dropping all fragmented packets. This feature can be used in the event there is a new attack hitting that takes advantage of fragmented packets. This capability should normally be turned off.

In terms of enabling e-mail for our network design, we have decided to use the InstaGate SCM appliance as the anti-virus and anti-spam gateway. To facilitate this, we need to enable mail relaying from the firewall to the InstaGate SCM, which is done via the e-mail configuration screen shown below:

Email: Server/Relay Settings

Email Server Status

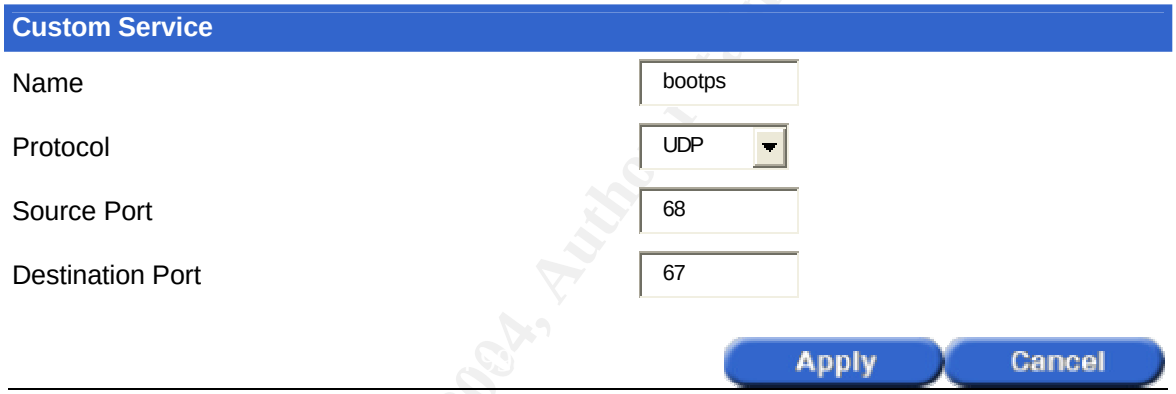
Email Server	☑ Enabled
Server Type	Relay
Mail Relay Configuration	
Domain Name	www.giacent
Relay Destination Address	192.168.1.3
Maximum Message Size	25 MB

2.2.2 Firewall rules configuration:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The InstaGate PRO is a menu driven system, and has pre-defined filters created for many protocols and services. Applying the filters is for the most part a point & click exercise. However, for more uncommon or esoteric protocols, ports, and services, custom services and policies can be easily supported and created.

For tutorial purposes, let's assume that we wanted to define a service that denies bootp access from a bootp client (UDP 68) to a bootp server (UDP 67). We do this by clicking "add" from the >firewall>custom services menu. We are then presented with the following screen. We create the policy by entering the name that we are giving to the custom service, the protocol (TCP, UDP, or ICMP) that it uses, and the source and destination port. This is shown on the following screen.



Once we have done this, we click apply, and the service will show up on the previously shown custom services screen, from which it can be used applied to any interface. Note that we do not need this service for our firewall implementation, we have only created the service to demonstrate how this is done on the InstaGate appliance.

The predefined protocols and services, and any customer ones that we have established (e.g. syslog) can be selected from the menu below (>firewall>custom services):

Firewall: Custom Services

Select	Service Name	Protocol	Source Port	Destination Port
◉	America Online	tcp	ANY	5190
○	IMAP	tcp	ANY	143

© SANS Institute 2004, Author retains full rights.
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

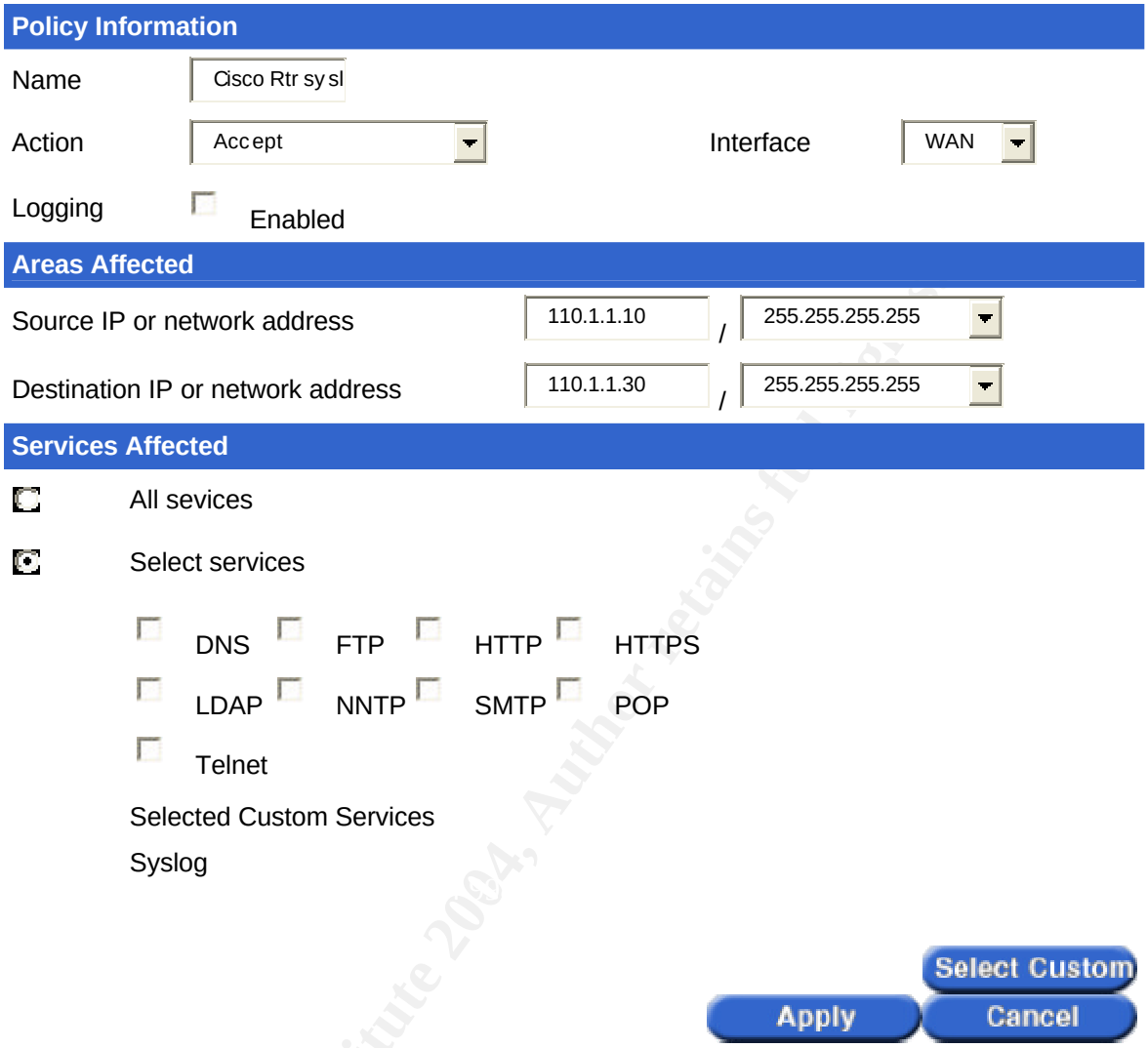
	Lotus Notes	tcp	ANY	1352
	Rlogin	tcp	ANY	513
	Rsh	tcp	ANY	514
	Secure IMAP	tcp	ANY	993
	Secure LDAP	tcp	ANY	636
	Secure News	tcp	ANY	563
	Secure POP	tcp	ANY	995
	SSH	tcp	ANY	22
	T.120	tcp	ANY	1503
	WinFrame	tcp	ANY	1494
	Echo Reply	icmp		0
	Echo	icmp		8
	Traceroute	icmp		30
	GRE	gre		
	IPSec (AH)	ah		
	IPSec (ESP)	esp		
	Syslog	tcp	514	514
	GMC	tcp	ANY	998
	bootps	udp	68	67

Add Delete Done

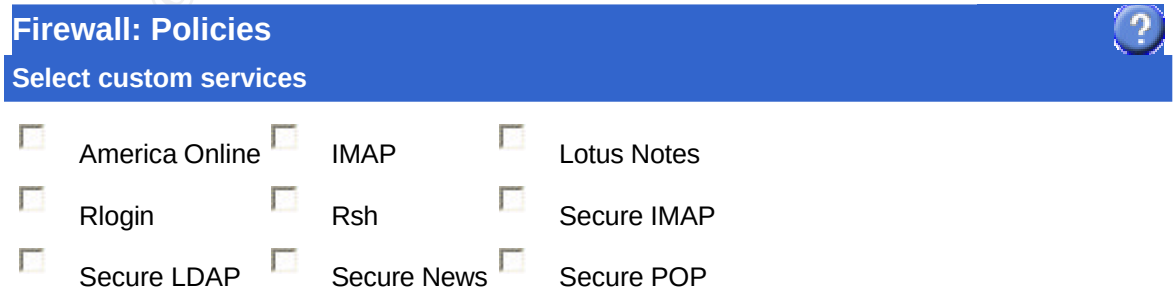
Next, we will configure the WAN interface. Note that the InstaGate preconfigures some of these services (those denoted System Services) when we enable VPN access. This will be discussed further later in the paper. For tutorial purposes, we will look at how we enable one of these services, namely the Cisco Rtr syslog policy. First, we access the >firewall>policies screen, and click on ADD, which brings up the following menu:

Firewall: Policies

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



We give the policy a name, define that it is an “accept” policy, define which interface we want it applied to, whether we want logging enabled (which we don’t, given the high volume of use), define the source and destination IP’s, and then either select a standard service as showm, or click on “select custom” to allow us to select the Syslog policy from the screen below:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

☐	SSH	☐	T.120	☐	WinFrame
☐	Echo Reply	☐	Echo	☐	Traceroute
☐	GRE	☐	IPSec (AH)	☐	IPSec (ESP)
☑	Syslog	☐	GMC	☐	bootps

Apply Cancel

Once we click on Syslog and Apply, the policy is then applied to the desired interface. We perform this sequence of steps for all policies that are required for the WAN interface, selecting either standard services that have been supplied by the vendor, or creating our own custom services. When complete, our WAN policies are as follows:

Firewall: Policies

Policies for Interface

Interface WAN

Select	Policy Name	Action	Source	Destination	Services
☐	*VPNREMOTEUSER-in* *	Accept	10.10.1.0/24	192.168.1.0/24	All services
☐	*IPSEC-IKE* *	Accept	Any	WANIP	(udp/500)
☐	*SMTP* *	Accept	Any	WANIP	(tcp/25)
☐	*IPSEC-ESP* *	Accept	Any	WANIP	(esp)
☐	*IPSEC-AH* *	Accept	Any	WANIP	(ah)
☐	Partners	Accept	Any	110.1.2.3/32	HTTPS
☐	Public Website Access	Accept	Any	110.1.2.2/32	FTP,HTTP,HTTPS
◉	DNS	Accept	Any	110.1.1.20/32	DNS
☐	Mail	Accept	Any	192.168.1.3/32	SMTP
☐	Cisco Rtr syslog	Accept	110.1.1.10/32	110.1.1.30/32	Syslog
☐	*VPNCLIENT* *	Accept	Any	WANIP	(tcp/999)
☐	deny wan	Deny	Any	WANIP	All services

Note: Policies will be processed in the order shown.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

** System Service*

The first 4 policies enable VPN's to function, and are established by the system when VPN software is present and enabled. The VPNREMOTEUSERIN allows incoming VPN connections to reach the LAN. The IKE policy allows Isakmp key exchange, the ESP policy allows IPSEC ESP protocol from any network address, and the AH policy allows IPSEC Authentication header traffic from any address. Taken together, these 4 policies enable IPSEC traffic to come in via the WAN interface, and to reach the 192.168.1.0 network. Our preference is not to accept VPN traffic from "anywhere", and we are suggesting that GIAC consider a global roaming agreement with a dial network provider. This could allow us in the future to identify the IP network of the service provider as the "source" above, with the appropriate netmask, so as to limit what networks we will accept VPN connections from. These policies are called system services because they are automatically enabled when the system is shipped with VPN software.

The Partners policy above was created to allow HTTPS traffic from partners to reach the secure web server on the DMZ/screened subnet.

The Public Website Access policy above was created to allow both HTTP and HTTPS traffic from partners to reach the secure web server on the DMZ/screened subnet.

The DNS policy above was created to allow DNS traffic from the Internet to reach the DNS server in the InstaGate.

The Mail policy above allows SMTP traffic to reach the InstaGate SCM's IP address. The InstaGate SCM content security appliance will act as a mail relay for mail traffic, relaying it to the internal mail server.

The Cisco Rtr Syslog policy allows syslog traffic from the Cisco border router to reach our logging server. This is done via NAT from the secondary IP address, 110.1.1.30, to the internal address of the logging server, 192.168.3.2 .

The VPNCLIENT policy is another system policy added by the system to support remote VPN users. The port that is opened up by this policy, TCP 999, is used to provide NAT services for the remote VPN users.

Finally, the deny wan policy will drop all other traffic not matching one of the preceding policies.

In deciding the order of the wan policies, we put the more explicit, and more frequently used policies at the top of the list, and the most general policies at the bottom of the list, because the InstaGate, like most firewalls, processes top-to-bottom.

© SANS Institute 2004, Author retains full rights.

Next, we will create policies for the DMZ interface:

Firewall: Policies

Policies for Interface

Interface DMZ

Select	Policy Name	Action	Source	Destination	Services
	DNS-DMZ-to-Internet	Accept	110.1.1.20/32	110.1.2.0/24	DNS
	Public Web Server-DMZ	Accept	Any	110.1.2.2/32	HTTP,HTTPS
	SQL	Accept	192.168.3.3/32	110.1.2.3/32	SQL-SRV,SQL-SRV-UDP,SQL-Monitor,SQL-Monitor-UDP
	Secure Web Srv Partner	Accept	Any	110.1.2.3/32	HTTPS
	denydmz	Deny	Any	110.1.2.0/24	All services

Note: Policies will be processed in the order shown.

* System Service

Up Down Copy

Add Modify Delete Done

The first policy above allows the web servers on the DMZ to use DNS to the DNS server on the InstaGate.

The second policy allows public web access from the internet to the public web server on the DMZ network.

The third policy allows the secure web server to communicate with the SQL server on the database and admin zone, using SQL.

The fourth policy allows partner access from the Internet to the secure web server, using HTTPS.

The final policy denies all other traffic into the DMZ.

Now we will configure the LAN interface:

Firewall: Policies

Policies for Interface

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Interface LAN

Select	Policy Name	Action	Source	Destination	Services
	VPNREMOTEUSER *	Accept	192.168.1.0/24	10.10.1.0/24	All services
	Web Access *	Web Access Control	Any	not LANIP	HTTP,HTTPS
	Admin DMZ access	Accept	192.168.3.0/24	110.1.2.0/24	HTTP,HTTPS,SSH
	DNS-lan	Accept	192.168.0.0/16	110.1.1.20/32	DNS
	FTP, HTTP, HTTPS	Accept	192.168.1.3/32	Any	FTP,HTTP,HTTPS
	Admin zone out	Accept	192.168.3.4/32	Any	FTP,HTTP,HTTPS
	admin ws 2 out	Accept	192.168.3.5/32	Any	FTP,HTTP,HTTPS
	SQL srv to secure web	Accept	192.168.3.3/32	110.1.2.3/32	SQL-SRV,SQL-SRV-UDP,SQL-Monitor,SQL-Monitor-UDP
	Mail out	Accept	192.168.1.3/32	Any	SMTP
	lan deny	Deny	192.168.1.0/24	110.1.1.0/24	All services

Note: Policies will be processed in the order shown.

* *System Service*

Up Down Copy
Add Modify Delete Done

The VPNREMOTEUSER policy is a system policy, automatically created by the InstaGate when VPN software is present.

The Web access policy above is a system service that is used to support the web access control capability of the InstaGate. This feature can be used to require outbound authentication of web usage, via username and password. We will not be using this for the GIAC network.

The admin DMZ access policy allows systems on the admin zone to access the systems on the DMZ.

The DNS –lan policy lets all IP's on the GIAC LAN reach the DNS server on the InstaGate.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The FTP, HTTP, and HTTPS policy allows these protocols to be used outbound from the GIAC employee workstation zone to the Internet, only via the InstaGate SCM proxy server. In order for this policy to work, and to allow employee access to the Internet, all employee workstations will need to be pointed to the proxy server on the InstaGate SCM.

The admin zone out policy allows FTP, HTTP, and HTTPS protocols to be used outbound from the admin zone to the Internet, for the first admin workstation.

The admin ws 2 out policy allows FTP, HTTP, and HTTPS protocols to be used outbound from the admin zone to the Internet, for the second admin workstation.

The SQL srv to secure web server policy allows the SQL server to communicate with the secure web server, using SQL protocols.

The Mail out policy was created to allow SMTP traffic to reach the internet from the SCM appliance, which is acting as a mail relay.

The final policy drops all other traffic (that which doesn't match one of the preceding policies) from the LAN interface.

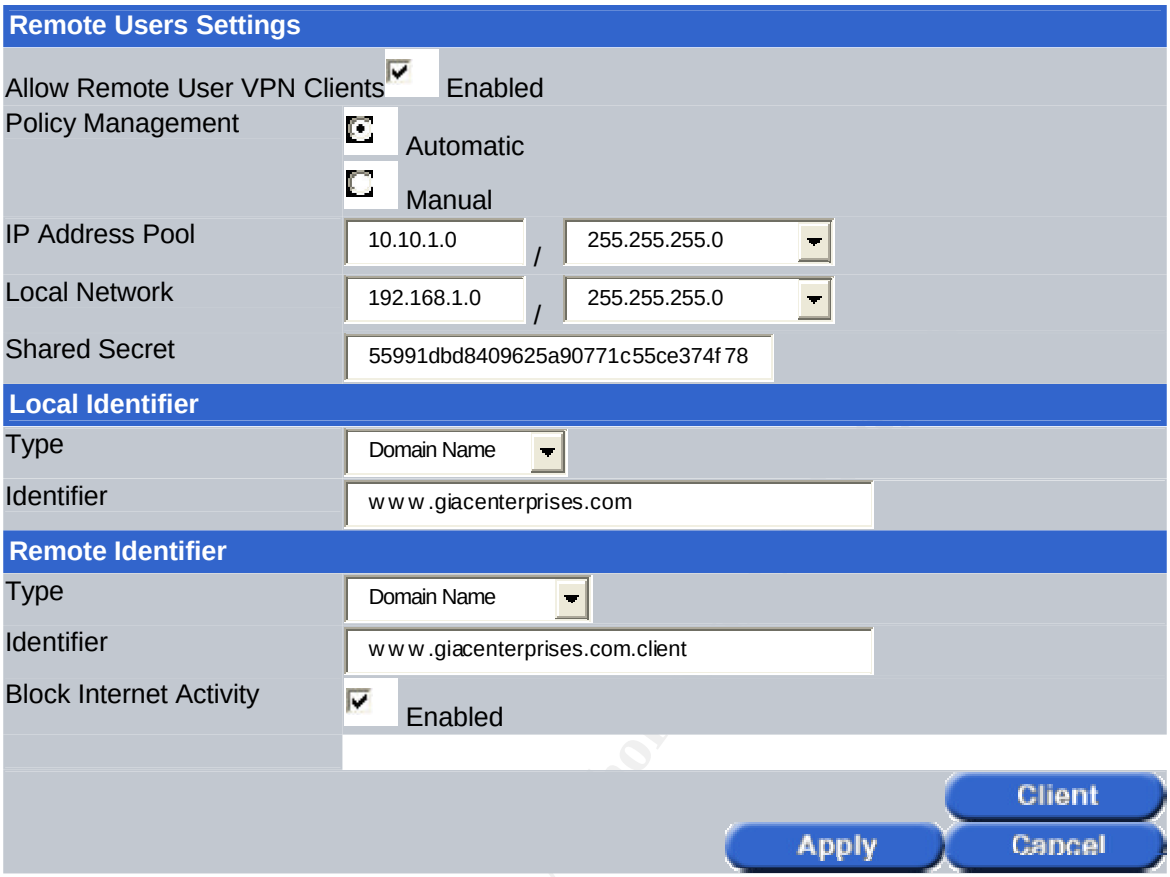
2.2.3 VPN configuration:

The InstaGate supports PPTP and IPSEC VPN protocols. We have chosen to implement IPSEC, because the encryption capabilities are stronger than PPTP's. Support is provided in the InstaGate for site-to-site VPN's, as well as dial/remote user VPN's. The GIAC network design only requires remote user VPN access, for salespeople and for company management. The InstaGate provides two means of configuring remote VPN users. The first is an automatic configuration mode, wherein the policies are defined centrally by the system administrator, and are automatically distributed to each client. Automatic mode precludes the need to configure each client system individually.

To configure remote VPN users automatically, we will first go the Users>Add users screen, and add all of our remote users, being careful to check the remote VPN access checkbox.

Next we go to Firewall>Remote User VPN and select "enabled" to allow remote user VPN clients, and "automatic" for policy management on the following menu:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.



Selecting automatic policy management means that the VPN policies will download automatically to each VPN client, as opposed to having to be manually configured on each remote workstation. The IP address pool setting is the addresses that will be dynamically assigned to remote VPN users. The Local Network IP address is the subnet that we are allowing the VPN users to have access to. The policy protection password is an extra administrative password that is used to protect access to the VPN policy that is automatically distributed to each client. The password must be communicated (by a secure, out-of-band method) to each remote VPN user in order for them to be able to "unlock" access the the required VPN policy.

Also, we have checked the block internet activity checkbox above. This disables remote clients from accessing the internet directly, while they have a VPN connection established. If we were to allow direct Internet connections while also connected to GIAC's network via a VPN tunnel, this would open up significant security holes, so we have chosen to disable this.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

From the Firewall>Remote User VPN menu, we can also click on "Client" to download the client VPN software, which we will distribute to each remote user.

The next step in establishing remote VPN users is to configure the client systems. The InstaGate can be configured to work with most standard IPSEC clients. Configuring the IPSEC client from eSoft is a straightforward process, because, as previously mentioned, the client downloads the policy from the InstaGate firewall automatically. The configuration that gets downloaded to the client includes the host name or IP address of the Instagate firewall, and the automatically generated shared secrets used in the IPSEC encryption. We can also define several security settings at the client, including the logon authentication protocol to be used (EAP, PAP, CHAP, MS-CHAP, MS-CHAP2- for our purposes we will use MS-CHAP2). Another important setting is whether or not to require encryption, and to disconnect if the server declines. Because the VPN client software will only be invoked when our remote users are connecting to the GIAC network, we want to set this to Yes. We also set the protocols that are allowed to be tunneled through the VPN, including TCP/IP, NetBEUI, file and printer sharing, and client for Microsoft Networks. Of these, we will disallow NetBEUI, as it is not needed in the remote user systems, and we will also disable file and printer sharing for security reasons. Finally, there is a setting in the client that can enable Internet Connection Sharing, which we will want to disable, as it is not needed in the GIAC remote access application.

Remote VPN users are required to authenticate with a user name and password to the InstaGate (which we established in the InstaGate configuration menu, Users>Add Users), before it will allow the VPN connection. We will recommend that GIAC use strong user authentication (2 factor) here for our VPN connections, by implementing Radius[13], and using SecureID's[14] and an ACE Server supporting Radius. Note that we have configured the InstaGate and the remote clients to use MSCHAP, which provides for a challenge-response based on cryptographic techniques to authenticate the remote client to the InstaGate.

In terms of the encryption algorithms possible on the InstaGate VPN server, we have a choice of two predefined proposal configurations as follows:

[13] ftp://ftp.rfc-editor.org/in-notes/rfc2058.txt
[14] http://www.rsasecurity.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

High Security — 3DES Enc, SHA-1 Auth, DH 2; 3DES Enc, MD5 Auth, DH 2

High Performance — AES 128-bit Enc, MD5 Auth, DH 2; AES 128-bit Enc, SHA-1 Auth, DH 2

We have opted for the high security configuration, which utilizes Triple DES encryption, with SHA-1 hashing algorithm, and MD5 authentication.

VPN Tips- if we do not want to add every remote user manually, and if we were using Radius (as recommended above) for user authentication, we could enable Radius in the InstaGate for remote authentication. Also, the InstaGate PRO does not presently support the creation of firewall rules that can be applied to traffic coming from VPN tunnels. Economic constraints have caused us to accept this limitation, however we can strengthen the security of VPN connections by limiting the allowed destinations on the LAN. We can do this by limiting the allowed destinations on the local network for VPN client connections. For example, on the remote user settings menu, if we wished to limit remote VPN users to just accessing the mail server, we could specify a local network of 192.168.2.2, instead of allowing access to the entire 192.168.0.0 network. This would limit the exposure posed by the VPN connections.

Remote Users Settings	
Allow Remote User VPN Clients	☑ Enabled
Policy Management	◉ Automatic ○ Manual
IP Address Pool	10.10.1.0 / 255.255.255.0
Local Network	192.168.1.0 / 255.255.255.0
Shared Secret	55991dbd8409625a90771c55ce374f78
Local Identifier	
Type	Domain Name
Identifier	www.giacenterprises.com
Remote Identifier	
Type	Domain Name
Identifier	www.giacenterprises.com.client
Block Internet Activity	☑ Enabled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.2.4 IDS/IPS configuration

The IDS/IPS module in the InstaGate was developed by Latis Networks, and is based on the SNORT (tm)[15] open source software. The IDS/IPS software is configured through the use of a menu system that is logically broken into three main sections or panels:

Manage system: In the Manage system section, configuration is performed as to what interfaces are going to be monitored. In the GIAC network, we want to look primarily at traffic coming in through the WAN interface, and traffic on the screened subnet/DMZ interface. In addition, it would be useful to look at traffic coming in via the LAN interface, if it doesn't impact performance adversely. In the event that a laptop user picks up something like the Blaster worm, while connected to another network, and then introduces it onto the GIAC LAN upon connecting to the network, having the IDS/IPS look at traffic on the LAN port would give us an early warning that something is amiss. Note that we have put filters in place to block Netbios related attacks from leaving the GIAC network. However, better to have some early warning on the LAN side of the firewall if this sort of thing occurs, and the ability to auto-block it is a nice capability if we choose to do so.

Manage rules: In this section, rules can be set to automatically block attacks, to prompt the system administrator in the "Make decisions" panel as to the action to take (block or ignore), or to never respond to this attack, i.e. disable the rule. There is also a quick-tuning capability that will automatically turn on or off rules based upon certain criteria. For example, if the company has no UNIX systems, quick-tune can turn all UNIX related rules off, as UNIX attacks pose no threat. Similarly, if there are no IIS web servers in use, many rules can be disabled. The impact of disabling rules for attacks that pose no threat to the GIAC

[15] SNORT is a trademark of Sourcefire, http://www.sourcefire.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

network is that the IDS/IPS subsystem, and the security appliance, will provide better performance.

Monitor, detect, and make decisions: This panel shows the IDS alerts that are detected, and allows the admnistrator ro take actions based upon the attacks that are flagged.

2.2.5 Application filter configuration

The application filter in the InstaGate allows for certain types of applications to be identified and blocked at the firewall. For our purposes, we want to block all Instant Messaging and peer-to-peer traffic on the GIAC network. App filter provides some other interesting capabilities, including allowing system administrators to track bandwidth utilization by protocol and application. In order to block IM and peer-to-peer traffic, we will simply configure it to identify and block any of the following:

AIMLogin, AIMXfer, AIMMsg, Aimster, AudioGalaxyLogin, AudioGalaxySearch, AudioGalaxyDownloadReq, AudioGalaxyXfer, Blubster, DirectConnect, Gnutella and applications built on the Gnutella protocol (Bearshare, Bodetella, Cooltella, Furi Launcher, Furi Updater, Gnewtella, Gnewtella 2, GnOtella, GnuCache, Gnucleus, Gnujatella, Gnumm, Gnuspace, Gnutella for Mac, Gnut, Gnute, Gnutmeg, Gnutella Crawler, Gnutella.it, GnutellaXfer, Gobobo, GTK-Gnutella, Hagelslag, Limewire, Mactella, Morpheus, MyGnut, MyTella, N-Tella, newtella, PeaGnut, Pi, Pygnut, Reflector, SeachLord, Tellaseek, Toadnode), Gnutella Web, GnutellaXfer, ICQLogin, ICQMsg, KaZaA, KaZaAXfer, MSNMessengerLogin, MSNMessengerXfer, Microsoft-DS, NNTP, Napster and applications built on the Napster protocol (including Amster, BeNapster, Blazter, Capster, Console Napster LT, DeWrapster, DiaRRIA, DJnap, Fanster, File Navigator, Gnapster, Gnome-Napster, GTK-Napster, Hackster, iNapster, JNap, J Napster, Jnerve, KNapster, Koog Epsilon, Lopster, Macstar, Macster, Music City, MyNapster, NapAmp, Napigator, Napkin, NapMan, Napsack, Napster for eos.htm, Napster/2, Napsterminator, Napster - Linux, Napster Server Manager, Napster Unban, Netstreak, iAssimilator, N-Dream Plug-In for Napster, OpenNap, Pakster, Rapster, Riscster, Snap, Socks2HTTP, Spyster, TekNap, TKNap, Unwrapper, Webnap, Wrapster, XMNap), Napster XferIn, Napster XferOut, Napster Xfer, NetBIOS-SSN, ScourExchange, ScourExchangeXfer, and SpinFrenzy.

All of the applications above are related to the use of IM and peer-to-peer/file sharing communications.

General tips and tricks, and potential problems:

1. The InstaGate PRO will act as a DHCP server for connected clients, rather than using static IP addresses.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. In addition, the InstaGate will act as a proxy server for HTTP, HTTPS, and FTP traffic. Configuration of this feature is done at each client, and requires that the IP address of the InstaGate (192.168.1.1 in the GIAC network) be entered into the client TCP/IP setting as the proxy server for these applications, with a target port of 8080. Using a proxy server is the preferred mode of operation from a security standpoint.
3. It is also worth mentioning that clients on the GIAC network will need to be configured with either DHCP, to obtain an IP address automatically, or with a static IP address in the 192.168.4.0 subnet.
4. Harden all components. All servers and networking components will have unnecessary services removed, and all of the Windows OS servers will be checked for mis-configuration and for known security vulnerabilities using Microsoft Baseline Security Analyzer.
5. 3rd party vendor access- we will restrict this, and lock it down. For example, for any diagnostic ports that our IT vendors wish to use, we will enable rigorous authentication in the form of dial back modems, or challenge-response, before allowing access.
6. We are recommend that GIAC bring in a vendor to scan all hosts on their network on a frequent, periodic basis, quarterly at a minimum, monthly if possible.
7. We are also recommending to GIAC that they invest in an automated patch management capability, to keep servers and workstations up to date with most current releases of OS's, and other key software components.

Vulnerabilities and mitigation suggestions for key components:

InstaGate PRO Firewall

A search of the vendor website revealed no open vulberabilities, or patches required.

Cisco 3620 Router

A search of the Bugtraq vulnerabilities database[16] revealed no known vulnerabilities in either the version of IOS that we are using (12.3), or in the 3620 router. A search of the vendor website turned up no vulnerabilities for 3620 routers running IOS 12.3.

2.3 Configuration of the InstaGate SCM content security appliance

[16] http://www.securityfocus.com

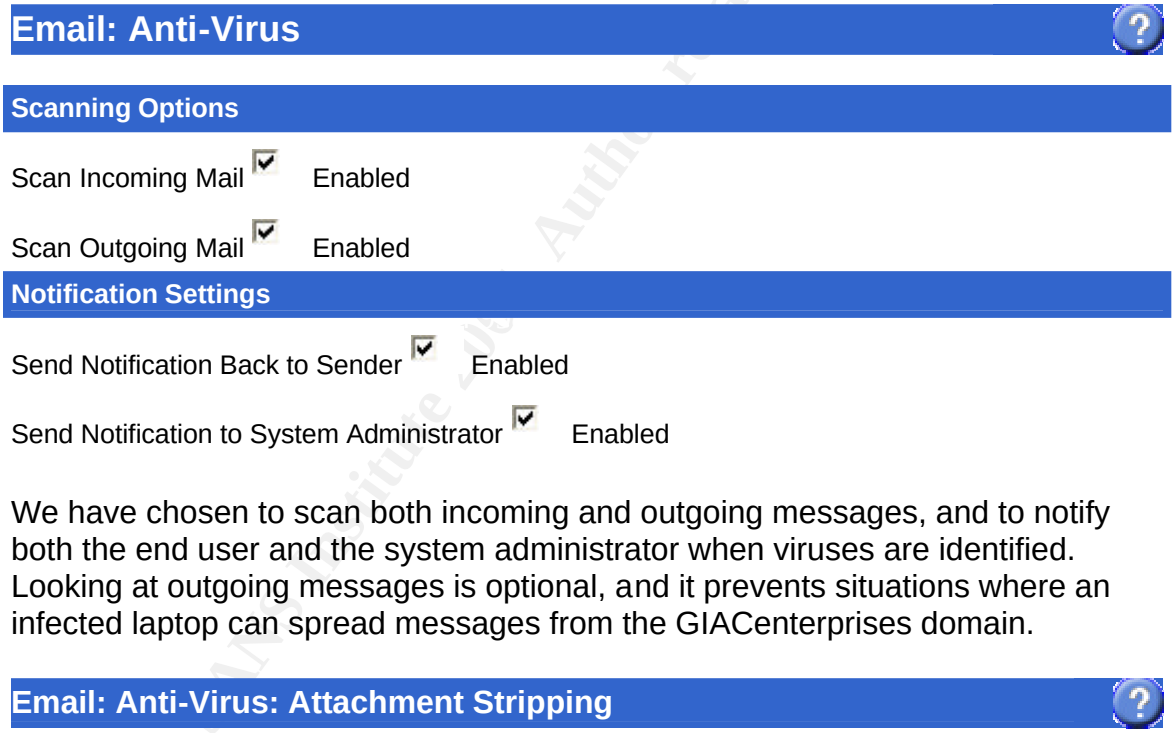
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

We are including a configuration for this system, because it is a key part of our perimeter security. Configuration of this appliance-based solution consists of identifying policies for filtering SPAM, and website filtering. In addition, the appliance acts as a gateway anti-virus solution, scanning all incoming and outgoing mail, and eliminating viruses. When setting up the firewall, we configured it to relay all mail to the content security appliance. We also configured it to limit all out-bound web traffic to only allow outbound access from the SCM's proxy server.

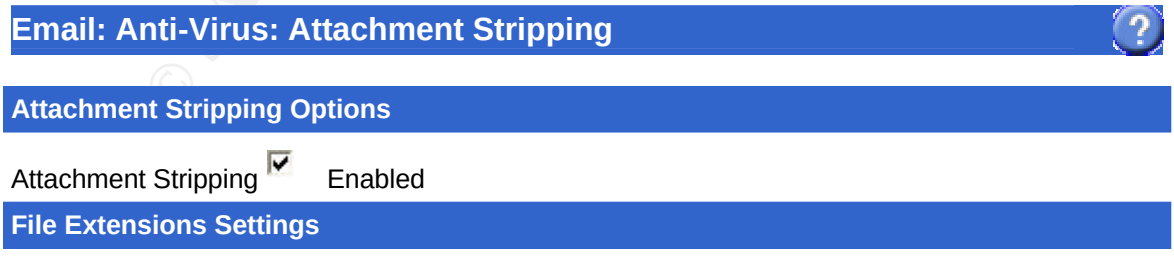
2.3.1 Anti-Virus configuration

Establishing the security and response policies for the anti-virus module is straightforward.

A configuration for the gateway anti-virus is shown below:

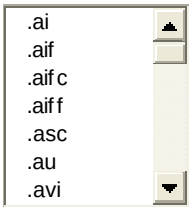


We have chosen to scan both incoming and outgoing messages, and to notify both the end user and the system administrator when viruses are identified. Looking at outgoing messages is optional, and it prevents situations where an infected laptop can spread messages from the GIACenterprises domain.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

File Extensions to Strip



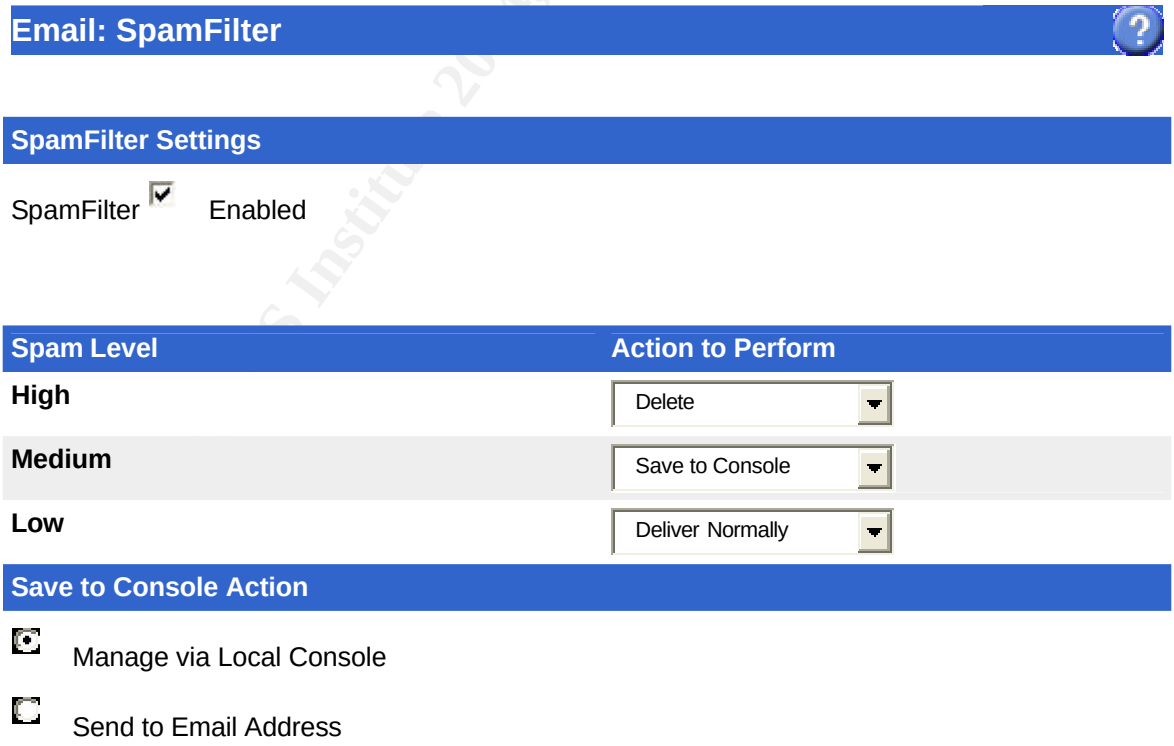
Additional File Extensions

On the configuration screen above, we can have the InstaGate SCM strip potentially harmful attachments from e-mails, including .exe's, .bat's, etc. We have chosen to strip any attachments that can include executable code.

The SCM holds messages found to contain a virus, and messages that have had an attachment stripped, in a quarantine folder, from which system administrators can release them if desired.

The AV module also requires configuration (intervals from minutes to days may be defined) as to the frequency of signature updates. We have configured the unit to check for updates every 5 minutes. There is little performance or bandwidth penalty for setting this value low, as the signature downloads are very small.

2.3.2 SPAM filter configuration



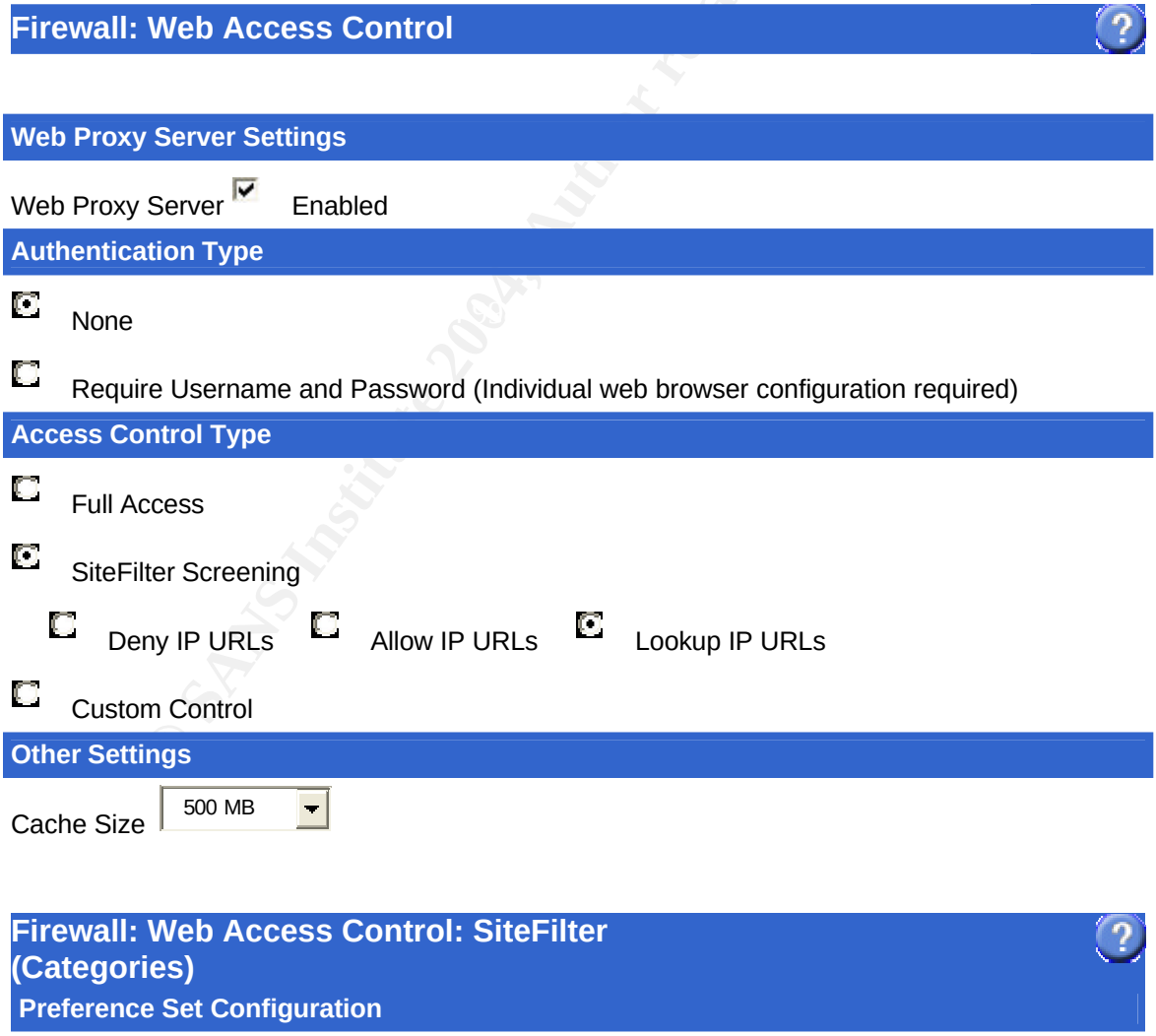
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Managing the SPAM filter is a straightforward process as well. Messages identified as potentially being SPAM get categorized as either high, medium, or low probability of being SPAM. We have chosen to automatically delete high probability messages, to save medium probabilities to the system admin console for inspection, and the deliver low probabilities normally. The SPAM filter uses several different techniques to identify potential SPAM.

An exception list can also be created to minimize false positives. For example, it is possible to create an exception for all mail from a specific domain, or a specific e-mail address, even though their messages contain some characteristics normally associated with SPAM.

2.3.3 Web access filtering configuration

The web access filtering capability of the SCM allows us to control what sorts of websites employees are allowed to access while using the corporate network.



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Preference Set Name	Corporate policy

Schedule

Day	Begin	End
Sunday	-----	-----
Monday	-----	-----
Tuesday	-----	-----
Wednesday	-----	-----
Thursday	-----	-----
Friday	-----	-----
Saturday	-----	-----

Block the following categories

☑ Sex	☑ Drugs	☑ Hate Speech
☑ Crim. Skills	☑ Nudity	☐ Online Sales
☑ Gambling	☐ Personal	☐ Job Search
☐ Sports	☐ Games	☐ Humor
☑ MP3 Sites	☐ Entertainment	☐ Lifestyle
☐ Extreme	☐ Chat	☐ Investing
☐ Gen. News	☐ Politics/Religion	☑ Dating
☐ Art/Culture	☐ Cults/Occult	☑ Usenet News
☐ Self Help/Health	☐ Travel	☑ Mature
☐ Webmail	☐ Portal Sites	☑ Anonymizer/Translator
☐ User defined category 0	☐ User defined category 1	☐ User defined category 2

We have defined a number of categories that GIAC management has deemed either not essential to anyone's job function, or against the company internet use policy. Sitefilter will block access to sites in these categories. Sitefilter uses the Secure Computing[17] site database of over 4 million URL's.

[17] http://www.securecomputing.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.0 Verification of Firewall Policy

Now that we have designed and implemented our secure network design for GIAC, our next task will be to audit the firewall implementation to ensure that our network is performing as we expect, that it is allowing GIAC's business operations to function, and that it is blocking the sorts of traffic that we designed it to. A document that was very useful in designing our audit plan was Auditing Your Firewall Setup[18].

3.1 Validation Plan

3.1.1 All scanning activity will be scheduled to occur during non-business hours, when we are least likely to affect GIAC's business operations. There is the risk that the scanning activity will cause some scanned systems to crash, or that they will adversely affect them in some way. Our cost estimate below allows some time for rebuilding some of the systems.

3.1.2 Estimate of costs to validate the firewall implementation:

Task	Estimated Hours	Estimated Cost (labor rate $100/hour)
Port scan firewall	3	300
Scan border router	1.5	150
Scan hosts on DMZ network zone	6	600
Perform backups of key internal systems	12	1200
Scan GIAC hosts and workstations on internal LAN	30	3000
Analysis of results	6	600
Reconfiguration of systems, networking components, and security components	10	1000
Patching high priority systems	12	1200
Bring all systems up, and network online	8	800
Totals	76.5	8,850

[18] Auditing Your Firewall Setup, Lance Spitzner, http://www.spitzner.net/audit.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Note that we have only estimated direct costs in terms of personnel/time. To the extent that systems are down and unavailable to the business, there would likely be other costs to the business as well, in terms of lost productivity.

3.1.3 We will ask GIAC management to sign-off on the scanning and validation activity, acknowledging the risks previously mentioned, as well as the anticipated costs.

3.1.4 The firewall is based upon a hardened LINUX appliance. The first part of the validation plan will be to port scan the firewall itself, from the external, screened subnet, and internal interfaces. This scan will verify whether the vendor has turned unnecessary services off on the appliance, and whether the OS has been patched against known LINUX vulnerabilities.

3.1.5 Scan the border router. Note that while this would be a part of the verification of the network, due to resource constraints (the lack of an actual Cisco 2650 router), we are unable to perform this step.

3.1.6 Scan the hosts on the screened subnet from the Internet, and from the internal network. We have simulated some of this activity due to resource constraints.

3.1.7 Verify that the allowed protocols from the internal network can reach the Internet side of the firewall (SMTP, HTTP, HTTPS, DNS).

3.1.8 Verify that the allowed protocols from the Internet into the screened subnet (TCP/HTTP, SMTP, DNS) work.

3.1.9 Verify that disallowed protocols and addresses from the Internet are indeed blocked, including private IP's, and the loopback address.

3.1.10 Verify that disallowed protocols from the internal network are blocked at the firewall.

3.2 Summary of validation

3.2.1 In order to verify that the firewall has been configured correctly, we will attempt access from the Internet/wan side, from the screened subnet, and from the internal network using a variety of different applications and protocols, to prove out the successful implementation of the firewall policy.

3.2.2 The primary tools used in this exercise will be the NMAP scanner, running on a Windows laptop, and ethereal to capture and analyze packets, as well as ping, FTP, and HTTP clients to test connectivity.

Audit Results

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Scanning the firewall from the internal LAN

Scan	Results
ping 192.168.1.1 ping 110.1.2.1 ping 110.1.1.2	Firewall responded to pings on the local gateway interface. Ping attempts to the DMZ interface and the WAN interface from the LAN timed out. Firewall logs indicate that our Lan deny rule caused the ICMP ping traffic to be dropped, which is what we expect to have happen. Feb 28 00:00:54 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT= MAC=00:01:4e:00:33:e5:00:a0:24:a8:39:4c:08:00 SRC=192.168.1.11 DST=110.1.1.20 LEN=48 TOS=0x00 PREC=0x00 TTL=128 ID=459 DF PROTO=TCP SPT=1073 DPT=999 WINDOW=16384 RES=0x00 SYN URGP=0
Connect scan	nmap -sT -PT -PI -O -vv -T 3 192.168.1.1 The Connect() Scan took 401 seconds to scan 1601 ports. Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port For OSScan assuming that port 25 is open and port 42685 is closed and neither are firewalled Interesting ports on pc1.internal (192.168.1.1): (The 1594 ports scanned but not shown below are in state: filtered) Port State Service 25/tcp open smtp 53/tcp open domain 139/tcp open netbios-ssn 548/tcp open afpovertcp 998/tcp open busboy 999/tcp open garcon 8080/tcp open http-proxy Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Syn scan	CMD: nmap -sS -PT -PI -O -vv -T 3 192.168.1.1 The syn scan turned up the same open ports as the connect scan. Comments- we expected 25, 53, and 999 and to be open, based upon our Lan interface rules. 8080, 139, 998 and 548 we did not expect to be open. We queried the vendor to determine why these ports are open, and what they are used for. Our plan as to how we will address these ports is described in the discussion of validation testing and results, and suggestions for improvements section below.
Fin scan	CMD: nmap -sF -PT -PI -O -vv -T 3 192.168.1.1 (no tcp responses received -- assuming all ports filtered) Nmap run completed -- 1 IP address (1 host up) scanned in 196 seconds
Xmas tree scan	CMD: nmap -sX -PT -PI -O -vv -T 3 192.168.1.1 (no tcp responses received -- assuming all ports filtered) Nmap run completed -- 1 IP address (1 host up) scanned in 194 seconds
Null scan	CMD: nmap -sN -PT -PI -O -vv -T 3 192.168.1.1 (no tcp responses received -- assuming all ports filtered)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	Nmap run completed -- 1 IP address (1 host up) scanned in 202 seconds Comments- Each of these scans (Xmas tree, Fin, and Null) turned up hundreds of "open ports", because they treat the absence of a response as an indicator that a port is open. The InstaGate, like most firewalls, drops xmas, fin, or null packets. Consequently, these scans produced many "open ports", which is an invalid analysis.
Ack scan	CMD: nmap -sA -PT -PI -O -vv -T 3 192.168.1.1 Starting nmap V. 3.00 (www.insecure.org/nmap) Host pc1.internal (192.168.1.1) appears to be up ... good. Initiating ACK Scan against pc1.internal (192.168.1.1) The ACK Scan took 255 seconds to scan 1601 ports. Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Interesting ports on pc1.internal (192.168.1.1): (The 1594 ports scanned but not shown below are in state: filtered) Port State Service 25/tcp UNfiltered smtp 53/tcp UNfiltered domain 139/tcp UNfiltered netbios-ssn 548/tcp UNfiltered afpovertcp 998/tcp UNfiltered busboy 999/tcp UNfiltered garcon 8080/tcp UNfiltered http-proxy Comments- This scan turned up the same unfiltered ports as the connect and syn scans.
UDP scan	CMD: nmap -sU -P0 -O -vv -T 3 192.168.1.1 (no udp responses received -- assuming all ports filtered) Nmap run completed -- 1 IP address (1 host up) scanned in 305 seconds Comments- The UDP scan had similar resuts to the XMAS tree, null, and fin scans, many ports were listed as "open", i.e not responding.

Scanning the firewall from the WAN network

Scan	Results
ping 192.168.1.1	Ping attempts to the LAN side of the InstaGate failed with a host unreachable message
ping 110.1.2.1	Ping attempts to the InstaGate Wan interface timed out, and the firewall logs indicate that the traffic was dropped 2004 Feb 28 01:02:13 InstaGate-xSP PF deny wan DROP: IN=eth1 OUT= MAC=00:01:4e:00:33:e6:00:00:86:5d:69:4b:08:00 SRC=110.1.1.11 DST=110.1.1.20 LEN=60 TOS=0x00 PREC=0x00 TTL=128 ID=3291 PROTO=ICMP TYPE=8 CODE=0 ID=512 SEQ=256
ping 110.1.1.2	Ping attempts to the DMZ interface also timed out, and were dropped by the firewall
Connect scan	Connect scans using TCP and ICMP turned up nothing. We ran NMAP using the –po option (don't ping). CMD: nmap -sT -P0 -O -vv -T 3 110.1.1.20

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

	The Connect() Scan took 808 seconds to scan 1601 ports. Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port For OSScan assuming that port 25 is open and port 43833 is closed and neither are firewalled Interesting ports on (110.1.1.20): (The 1598 ports scanned but not shown below are in state: filtered) Port State Service 25/tcp open smtp 998/tcp open busboy 999/tcp open garcon Remote operating system guess: Linux Kernel 2.4.0 - 2.5.20
Syn scan	CMD: nmap -sS -P0 -O -vv -T 3 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating SYN Stealth Scan against (110.1.1.20) Adding open port 998/tcp Adding open port 25/tcp Adding open port 999/tcp The SYN Stealth Scan took 540 seconds to scan 1601 ports. Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port For OSScan assuming that port 25 is open and port 37847 is closed and neither are firewalled Interesting ports on (110.1.1.20): (The 1598 ports scanned but not shown below are in state: filtered) Port State Service 25/tcp open smtp 998/tcp open busboy 999/tcp open garcon Comments- Port 25 we expect to be open, to allow for mail relaying. Port 998 is related to the Global Console Manager, which we do not want to be enabled. We discuss how to disable this function, and close this port, in a later section. TCP 999 is related to the VPN client, and is expected to be open.
Fin scan	CMD: nmap -sF -P0 -O -vv -T 4 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating FIN Scan against (110.1.1.20) Skipping host (110.1.1.20) due to host timeout Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds
Xmas tree scan	CMD: -sX -P0 -O -vv -T 4 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating XMAS Scan against (110.1.1.20) Skipping host (110.1.1.20) due to host timeout Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds
Null scan	CMD: nmap -sN -P0 -O -vv -T 4 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating NULL Scan against (110.1.1.20)

© SANS Institute 2004, Author retains full rights.

	Skipping host (110.1.1.20) due to host timeout Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds Comments-
Ack scan	CMD: nmap -sA -P0 -O -vv -T 4 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating ACK Scan against (110.1.1.20) The ACK Scan took 266 seconds to scan 1601 ports. Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port Interesting ports on (110.1.1.20): (The 1598 ports scanned but not shown below are in state: filtered) Port State Service 25/tcp UNfiltered smtp 998/tcp UNfiltered busboy 999/tcp UNfiltered garcon No OS matches for host (test conditions non-ideal). Nmap run completed -- 1 IP address (1 host up) scanned in 284 seconds
UDP scan	CMD: nmap -sU -P0 -O -vv -T 4 110.1.1.20 Starting nmap V. 3.00 (www.insecure.org/nmap) Host (110.1.1.20) appears to be up ... good. Initiating UDP Scan against (110.1.1.20) Skipping host (110.1.1.20) due to host timeout Nmap run completed -- 1 IP address (1 host up) scanned in 301 seconds

Scanning the firewall from the DMZ network

Scan	Results
ping 110.1.2.1 ping 110.1.1.2	Ping attempts to the InstaGate DMZ interface timed out, and the firewall logs indicate that the traffic was dropped by our deny dmz rule 2004 Feb 28 10:09:05 InstaGate-xSP PF denydmz DROP: IN=eth2 OUT= MAC=ff:ff:ff:ff:ff:ff:00:00:86:5d:69:4b:08:00 SRC=110.1.2.4 DST=110.1.2.255 LEN=96 TOS=0x00 PREC=0x00 TTL=128 ID=7106 PROTO=UDP SPT=137 DPT=137 LEN=76 Ping attempts to the InstaGate Wan interface failed, with a destination unreachable.
Connect scan Syn scan	CMD: nmap -sT -P0 -O -T 4 110.1.2.1 Starting nmap V. 3.00 (www.insecure.org/nmap) Skipping host (110.1.2.1) due to host timeout Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds CMD: nmap -sS -P0 -O -T 4 110.1.2.1 This scan produced the same results as above, timed out.
Fin scan Xmas tree scan Null scan	CMD: nmap -sF -P0 -O -T 4 110.1.2.1 CMD: nmap -sX -P0 -O -T 4 110.1.2.1 CMD: nmap -sN -P0 -O -T 4 110.1.2.1 These scans produced the same results as above, timed out.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ack scan UDP scan	CMD: nmap -sA -P0 -O -T 4 110.1.2.1 CMD: nmap -sU -P0 -O -T 4 110.1.2.1 These scans timed out.

The next set of scans and connection attempts are aimed at determining if we can get traffic through the firewall to systems on the DMZ, and Internet, from the LAN, DMZ, and Internet. These tests will validate that things we expect to be denied are, and that the protocols that we expect to be allowed through are in fact passed. Due to a lack testing equipment we were unable to exhaustively test all allowed protocols and services. However, we have documented that our firewall policies for each interface are doing what we expect them to.

Scanning systems on the DMZ from the Internet

Scan	Results
Ping 110.1.2.2	Request timed out, dropped by firewall
HTTP 110.1.2.2	HTTP requests passed through firewall, and seen by packet sniffer on DMZ lan segment
Connect scan Syn scan on 110.1.2.2	These scans found the following ports open: 80/tcp 443/tcp 20/tcp 21/tcp No other traffic was seen leaving the firewall by our packet sniffer on the DMZ.

Scanning a system on the Internet from the LAN (192.168.1.3)

Scan	Results
Ping 110.1.1.10	Request timed out, dropped by firewall
Http 110.1.1.10	HTTP requests passed through firewall, and seen by packet sniffer on WAN segment
Connect and Syn Scans on 110.1.1.10 from 192.168.1.3	All scan attempts timed out. Firewall logs showed many packets dropped by the Lan deny rule, including: 2004 Feb 29 16:13:47 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT=eth1 SRC=192.168.1.3 DST=110.1.1.10 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=2437 DF PROTO=TCP SPT=2987 DPT=45 WINDOW=16384 RES=0x00 SYN URGP=0 2004 Feb 29 16:13:47 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT=eth1 SRC=192.168.1.3 DST=110.1.1.10 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=2438 DF PROTO=TCP SPT=2988 DPT=665 WINDOW=16384 RES=0x00 SYN URGP=0

Scanning systems on the DMZ from the LAN

Scan	Results

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Ping 110.1.2.2	Pings did get through to 110.1.2.2
HTTPS 110.1.2.2	HTTPS traffic was seen on 110.1.2.2, by our packet sniffer
Connect and Syn Scans on 110.1.2.2 from 192.168.1.3	CMD: nmap -sT -P0 -O -T 4 110.1.2.2 (timed out) CMD: nmap -sS -P0 -O -T 4 110.1.2.2 Starting nmap V. 3.00 (www.insecure.org/nmap) Interesting ports on JDHLAPTOP (110.1.2.2): (The 1596 ports scanned but not shown below are in state: closed) Port State Service 80/tcp open http 135/tcp open loc-srv 139/tcp open netbios-ssn 445/tcp open microsoft-ds 1027/tcp open IIS Our firewall logs also showed scan traffic being dropped by the Lan deny rule: 2004 Feb 29 17:09:22 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT=eth1 SRC=192.168.1.3 DST=110.1.1.10 LEN=78 TOS=0x00 PREC=0x00 TTL=127 ID=3970 PROTO=UDP SPT=137 DPT=137 LEN=58 2004 Feb 29 17:09:24 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT=eth1 SRC=192.168.1.3 DST=110.1.1.10 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=3971 DF PROTO=TCP SPT=4317 DPT=7005 WINDOW=16384 RES=0x00 SYN URGP=0 2004 Feb 29 17:09:24 InstaGate-xSP PF lan deny DROP: IN=eth0 OUT=eth1 SRC=192.168.1.3 DST=110.1.1.10 LEN=48 TOS=0x00 PREC=0x00 TTL=127 ID=3972 DF PROTO=TCP SPT=4318 DPT=866 WINDOW=16384 RES=0x00 SYN URGP=0 Comments: The allowed ports that showed up on the scan correspond to the rules in our firewall for allowed traffic between the GIAC LAN and the DMZ.

3.3 Discussion of validation testing and results.

In doing our LAN scans of the firewall, we determined that TCP ports 8080, 139, and 548 were open. In discussing the uses for these ports, we found that 139 and 548 are used to support file sharing for Windows and Apple clients, respectively. The InstaGate can serve as a file server for local LAN users, something we have no need for in the GIAC network design. File service is turned on by default. These ports can be turned off by accessing the InstaGate console, selecting Servers, and deselecting File Server enabled. Port 8080 is used to allow the InstaGate to act as a proxy server, which we do not plan to do. We can disable proxy services in the InstaGate using the administrative interface by selecting Firewall>Web Access Control, and deselecting Web Proxy Server on the check box.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Regarding port 998, our scanning revealed that it is open on both the LAN and WAN. Our research with the vendor revealed that it is opened up when the Global Management Console is enabled. Global Console Management is a capability that allows multiple firewalls to be managed from a central location. Since we will not be using this capability, we will turn this port off by disabling the Global Management Console via the InstaGate administrative interface, selecting Global Management, and deselecting the check box. This will disable the port.

Although we were prevented from doing all of the testing that we would ideally do, owing to a lack of test equipment, the testing that we were able to do indicated that the firewall is dropping traffic as we intend, and is passing the traffic that we created ACCEPT rules for. In a more ideal situation, we would comprehensively test to ensure that all of our filters are working correctly, on all interfaces, by testing every allowed protocol/address combination.

3.4 Recommendations for improvement, based on testing findings

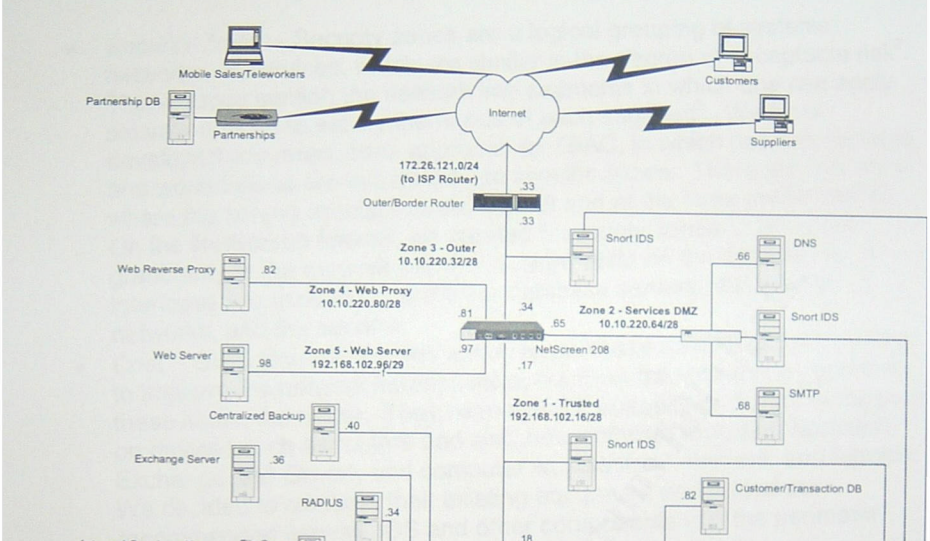
One simple thing that testing revealed is that we should enable logging for all of our Deny policies, so that we get better information in our logs. Our testing did not reveal anything that requires changing the design, or changing the policies to reflect GIAC's intended business operations, and security policy.

4.0 Design Under Fire

For the final portion of this assignment, we have chosen the following alternative design for GIAC's network to simulate an attempt to compromise it in a variety of ways-

Lawrence Manalo GCFW certification submission, August 7,2003, URL= http://www.giac.org/GCFW/Lawrence_Manalo_GCFW.pdf

Manalo's proposed network architecture is shown below:



© SANS Institute 2004 Author retains full rights.

Manalo's design uses the Netscreen 208 firewall (ScreenOS 4.03r1), and it uses a Cisco 3745 (12.2T IOS) router as the network access router. In order to perform actual attacks on this GIAC network design, with no prior knowledge of the network design and the key network components, it would be necessary to do significant reconnaissance of the network. Many of the following tools (presented in more or less the order that they might be used) would be useful in developing the information necessary to mount attacks:

- Gathering publicly available information on GIAC's website, DNS, mail server, and internal addressing, using applications such as nslookup, and nslookup based internet services
- Gather publicly available information from the GIAC website and other sites, and by using Google to search on key employee names and e-mail addresses. Employees who have used public forums to post messages may have unwittingly left clues as to their network topology in their e-mail headers, for instance. Looking at GIAC's press releases may identify some of their key supplier and channel partner relationships. Depending on how well locked down the GIAC corporate LAN is, we may want to target on of their partner's networks to see if we can establish a "back door" connection to GIAC via a trusted partner's network.
- Using social engineering to attempt to find information that is useful to an attack. This could include posing as an employee or as a partner and attempting to "con" confidential information out of a GIAC employee, or out of a partner IT staffer.
- Use traceroute to determine the routes used when communicating with GIAC's servers. Traceroute services are common on the web, and traceroute code is also found on many operating systems. Traceroute can help to determine what ISP is providing mail relay to GIAC. One avenue to try and develop information about GIAC's network is via the ISP's DNS

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

mapping. Traceroute can also be used to determine alternate connections that may exist into GIAC's site, via tunnels from partner sites, for instance.
- Using a Web browser to access the GIAC public website can help to identify the type of web server in use by GIAC, which helps to start the fingerprinting process.
- NMAP and other port scanners can assist in showing any open ports on target hosts, can help to fingerprint the targets, and can identify vulnerabilities that exist.

Once we have developed enough information about the GIAC network, including the components in use, and the network addressing scheme in use, our next step is to do some research on the key components, to look for known vulnerabilities and any exploit code that is in existence. Potential sources for this information include Security-Focus's Bugtraq list, the device vendors websites, CERT, the SANS Top 20 list, CVE, and ISS X-Force's database.

The Netscreen firewall used in this design has several known vulnerabilities, according to the Bugtraq[19] vulnerabilities database:

2003-10-03:	Netscreen ScreenOS DHCP Packet Buffer Padding Information Leakage Vulnerability
2003-07-31:	NetScreen ScreenOS TCP Window Size Remote Denial Of Service Vulnerability
2003-07-28:	NetScreen Non-IP Traffic Firewall Bypass Vulnerability
2003-06-25:	NetScreen ScreenOS Same Source IP Authentication Vulnerability
2003-04-17:	NetScreen Global PRO Policy Manager IPSec Tunnel Security Configuration Weakness
2003-03-07:	NetScreen ScreenOS Loss of Configuration Vulnerability

Of these, research into the versions of the Netscreen OS affected by each of the vulnerabilities turned up the following vulnerabilities that appear to be present in the version of ScreenOS used in the Manalo network design.

4.1 Firewall Attack

Of the three current Netscreen vulnerabilities affecting ScreenOS 4.03r1, the non-IP traffic firewall bypass seems promising in terms of potentially circumventing the firewall. However, launching the attack is impractical, as it would require physical access to the firewall. Sending any non-IP traffic from a remote location is not feasible- the Internet would not be able to get the traffic to the firewall. The second option in terms of a direct attack on the firewall, based upon known vulnerabilities, is the DHCP

[19] http://www.security-focus.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Information Leaking vulnerability. In order to launch this attack, we would need to send DHCP requests to the firewall through the internet connection, or alternately through VPN tunnels from remote VPN users or partners. Manalo's design wisely does not provide VPN access to suppliers. It does provide VPN access to TWISM, a marketing partner. This could potentially provide another avenue of attack using this vulnerability, assuming that we can penetrate the TWISM network. However, success of this attack will depend upon the Netscreen 208 firewall being configured to act as a DHCP server. Because Manalo has not configured the firewall to provide DHCP services, the attack would fail.

The ScreenOS TCP Window Size Remote Denial Of Service Vulnerability seems like the best possible choice for an attack on the firewall. In a nutshell, this vulnerability exists in ScreenOS versions 4.0.1r1-4.0.1r6, and and 4.0.3r1-4.0.3r2. The DOS condition symptom that the firewall exhibits is a crash and reboot. It is caused when an attacker attempts to access the management IP addresses using TCP, with an incorrect/invalid window size setting. In order to attack this vulnerability we will need to craft packets, using a tool such as Hping2 or Rafale. Because the advisories on the vulnerability are vague in terms of identifying the exact window setting that will cause the DOS condition, we will have to experiment with a number of different values. Rafale can allow for the creation of scripts to automate the testing of different window sizes. It can also allow us to create a packet with a source address from the internal network on the Manalo GIAC design, i.e. the 10.10.220.34 network.

Using Rafale, we would experiment with TCP crafted packets, with window sizes larger than 65,535 bytes.

Running this sort of an attack would result in the following. First, the access router will allow TCP 80 and 443 traffic to reach the 10.10.220.34 interface on the firewall. The firewall has been configured to disallow management services on all network interfaces except the trust zone, so the attack will fail. The only way to successfully exploit this vulnerability is to somehow gain access to GIAC's internal LAN.

Because Manalo has configured the Netscreen in such a way as to prevent the management IP interface from being accessed except by internal IP addresses, the design is only susceptible to this vulnerability from insiders, or from an attacker who can somehow find their way into the trusted network. Some suggestions to mitigate this vulnerability include the following. First, the vendor has issued maintennce releases that correct this problem, ScreenOS 4.0.1, r7 or greater, or ScreenOS 4.0.3 r3 or greater. We would suggest that the Manalo network upgrade to either of these as soon as possible. Other steps to mitigate the vulnerability include using SSH to do remote management, as it is not susceptible to

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

this TCP window size vulnerability, where Telnet and HTTP/HTTPS are. In addition, it would likely be possible to put a deny ACL in place in the border router that examines traffic for window sizes, and denies traffic which has invalid (too large) TCP window sizes.

4.2 DDOS Attack

This attack will use the resources of 50 compromised cable modem systems to try and cause a denial of service condition, where the operation of some aspect of GIAC's network using the Manalo design is adversely affected. We will attempt to attack the Cisco 3745 (12.2T IOS), and cause a DOS condition.

Having researched the version of IOS that is used in the Manalo GIAC design, we found a UDP diagnostic port DOS vulnerability on the Cisco website, and described in a technical document, Defining Strategies to Protect Against UDP Diagnostic Port Attacks[20]. The vulnerability is present in the version of IOS used in the Manalo network design, 12.2.

In brief, the vulnerability allows an attacker to send a large volume of traffic requesting UDP diagnostic services, and upon doing so, the attacker can consume all of the router's CPU resources. However, the Manalo GIAC design has wisely disabled TC and UDP based small services, which means that an attack based on this vulnerability would fail. Another possibility for a DOS attack, also found on Cisco's support pages, is related to the handling of SSH. The Cisco security advisory Scanning for SSH Can Cause a Crash[21] describes this vunerability and how to guard against it.

In brief, some Cisco IOS versions, upon receiving very large SSH packets, will react in a way that causes the CPU of the router to be largely consumed with trying to process the packet, causing a DOS condition.

Exploiting this vulnerability would be fairly simple, and would only require the use of a packet crafting tool such as HPING2[22] or Rafale[23] to create a very large SSH packet.

As Manalo's design does not specify whether SSH is enabled or not, this attack may or may not succeed, depending.

Suggested countermeasures to mitigate this sort of an attack include the following. Cisco has issued patches for the affected IOS versions. The

[20] http://www.cisco.com/warp/public/707/3.html
[21] http://www.cisco.com/warp/public/707/SSH-scanning.shtml
[22] http://www.hping.org
[23] http://www.packx.net

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

version that would correct this is 12.2(6b), and we would suggest implementing it quickly. In addition, turning off SSH access via the WAN port would be a good idea as well.

Another potential DOS attack would use a variety of attack methods and protocols to try and overwhelm the router, and it's relatively small T-1 line. In order to carry out this attack, we will need to compromise 50 broadband connected PC's. We will call these our zombies. In order to compromise 50 systems, we will borrow a page from spammers, by sending out messages with legitimate sounding subject lines to thousands of potentially valid mail addresses, i.e. using a "common names" sort of approach to well-know mail hosters such as yahoo, netscape, etc. Sending mail to jdoe@, jsmith@, and working our way through common first initials coupled with common last names will almost certainly get our message in front of real live systems. The "spam" will include an executable that when run, will load our malware daemon onto the prospective zombie machine. The executable will "phone home" to let our "master" know the IP address of the zombie, and will include a rate testing mechanism to inform us of the speed of the connection. Once we have 50 broadband zombie machines at our disposal, we're ready to move on to the next step.

In order to carry out this attack, we will use the TFN2K tool. The "spam" that we sent out has loaded the TFN2K daemon on the zombie systems. The zombie systems will now be listening for instructions from the master system.

Our master system will try to saturate the T-1 and overwhelm GIAC's public web server by flooding it with traffic of different types. We will have half of the zombie systems attack port 80 of the GIAC public web server, and the other half attack GIAC's web server by sending random types of traffic, aimed at various ports. The random attacks, mixed with port 80 TCP/SYN attacks will hopefully serve to confuse the poor GIAC personnel having to deal with this attack, and slow them down in terms of responding. TFN2K allows a mix of TCP, UDP, and ICMP based attacks, and the attacks can be TCP/SYN, Broadcast PING, ICMP PING, or UDP packet floods.

To invoke a SYN attack on port 80 of the GIAC web server in Manalo's design, our master will execute the following command:

#tfn –f 1sthalf.txt –i 10.10.220.80 –p 80 –c 5

where –f tells tfn to load a file containing 25 of our zombies, -i tells tfn to target the ip address that follows, -p tells it which port to target, and –c 5 tells it to use a TCP/SYN flood.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

For the other half of our zombies, where we want to use random attacks on the same server, the command syntax would be:

#tfn –f 2ndhalf.txt –i 10.10.220.80 –c 8

The –c 8 option tells tfn to use random attacks on random ports.

We will use a program on the master system to initiate the attacks every 10 minutes. To make it harder to pin down the attackers, we will rotate the attack type through the zombie machines with each iteration (so that each zombie sends a new attack with each iteration). This can be done by renaming the two files above with each iteration, effectively swapping the contents of the 2 files.

The attack may not succeed over a long period of time, but it will certainly disrupt their operations until they are able to react, and put some specific source filters in place. In the Manalo network design, mention is made of some IDS-like options that are enabled on the Netscreen firewall, including SYN attack, UDP flood, and ICMP flood. It is hard to tell from the description what response occurs when one of these is detected, but these features in the Netscreen may provide some level of defense, or at least quick identification of the attack type.

An excellent analysis of TFN2K, it's key components, how it operates, and how to mitigate attacks from it was written by Jason Balrow and Woody Thrower of Axent[24].

SYN flood/DOS attacks are particularly hard to prevent. Our suggestions as to how to mitigate this sort of an attack include possibly implementing mechanisms that may exist in the router and firewall that can handle flooding, and that are designed to help prevent system starvation. These might include rate limiting settings in these devices, and settings that address aggressive behaviors. In addition, packet shaping tools and devices that can automatically throttle certain kinds of traffic based upon configurable parameters could be investigated as a potential solution. Products such as PacketShaper[25] claim to be able to block flows to system resources after thresholds are exceeded, and to thus be able to automatically react to DOS attacks. A product of this sort installed between the firewall and the web server could help mitigate DOS attacks.

In addition, an incident response process could help in identifying and responding to security incidents, including DOS attacks. The policy should identify a qualified team responsible for responding (the Computer

[24] http.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0502/ISB0502JBWT.pdf
[25] http://www.packeteer.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Emergency Response Team, or CERT), and it should include an incident classification that allows incidents to react to the most serious incidents. In addition, it should allow for a sequence of activities based upon the level of urgency. For serious attacks like a DOS attempt, the sequence of activities will include assessment, log analysis to determine the nature and target of the attack, and business continuity actions.

4.3 Internal System Attack

We considered trying to compromise an internal system by gaining access from the public internet connection. A logical target is the public web server, which in the Manalo design is an IIS web server. The fact that it is using IIS means that we would have many vulnerabilities to choose from. However, looking at how the network is segmented, and at how the firewall rules have been established, it seems highly unlikely that we could actually get to an internal system, even if we fully compromised the public web server, and gained root access. For this reason, we have chosen to attempt to target an end user or a business partner w/ VPN access, and to either hack or "social engineer" our way in via a VPN "backdoor".

Our plan of attack will be to-

> Determine who their key executives are, and where they live, by researching GIAC thoroughly. Then, do a drive-by on each executives home, to see if they have WLAN equipment in operation. The equipment needed to do this is trivial, and programs like netstumbler[26] make identifying active WLAN's simple. If the 802.11 equipment does not have authentication and encryption enabled, we will piggyback on the WLAN, and attempt to access the corporate LAN using the VPN tunnel that is established when the executive accesses the corporate LAN.
>
> The process we would use to compromise the executive's system would be as follows:
>
> - Use netstumbler with a wireless card, and perhaps an antenna to amplify the signal. Doing a drive-by of each executive's residence, we would look for any active WLAN's that are shown.
> - For those WLAN's that are identified, we will look for those with encryption disabled. Netstumbler will identify access points, whether encryption is enabled, and the SSID (assuming SSID broadcast has not been turned off).
> - If encryption is enabled on the WLAN, we can still attempt to compromise the WLAN encryption. The

[26] Network Stumbler, Copyright © Marius Milner 2001-2002.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

vulnerabilities in both 128 bit and 40 bit WEP are very well understood. The 24 bit IV's used by WEP cause keys to be reused too frequently. In addition, tools such as Airsnort and WEPCrack provide capabilities to crack WEP encryption.

- We could also attempt a "man-in-the-middle" attack, by putting a rogue AP within wireless range of the authorized AP. As long as we know the SSID in use (which we will have learned via Netstumbler, if SSID broadcast is not turned off), the access device will not be able to distinguish our AP from the valid one, and we can learn things valuable to our attack, including authentication requests, and the secret key being used.

Our goal in tapping into an executives WLAN is to be able to use the VPN tunnel that they will have connecting their PC to the GIAC network. If the client has split tunneling enabled, we may not even have to target the PC itself, just the WLAN network. For example, many WLAN access points use default logins and passwords of "admin"/"admin". If we can gain control of the access point, and split tunneling is enabled, then we have a wide open backdoor into the GIAC network. Because the VPN connection would drop us directly into the 192.168.102.16 network (the GIAC internal LAN), we can then attempt to access GIAC's web server and attack it, or any other internal system. Some other good targets include including the Radius server (logins and passwords are stored here), fortunes server and fortunes database (GIAC's high-value intellectual property data is resident here), and internal DNS server (this can be used to help map the internal network).

If our first attack above fails, we will research their business partners/suppliers, and use many of the research steps discussed earlier to find out as much information about the partner networks as possible. Assuming that we can compromise one of their networks, if they have VPN access, and if they have not been restrictive about determining what systems on their network can use the VPN tunnels to GIAC, then it should be possible to tunnel back in to the GIAC internal network GIAC.

Failing this, we can attempt to social engineer our way in to a remote access port/modem on GIAC's data center equipment. This would involve posing as a systems engineer for an IT supplier company, and requesting the dial phone number and password so that we can perform a critical patch, upgarde, etc. Without trying to get information by social engineering, we could also just use a war

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

dialer program, and a password cracking tool (for example LC4[27]) on any modems that we identify.

There are several key points here. First, Manalo has done a very good job of securing the "internet perimeter", so much so that we believe it would be futile to attempt to compromise an internal system coming in through the Internet connection directly. Second, as with most organizations, there are likely many "softer" and easier targets among the overall GIAC IT infrastructure, in terms of the probability of compromising an internal system. And the tools that the black hat community has access to are so sophisticated, and so readily available, that successfully mounting any of these three attacks is more a matter of time and persistence than technical skill. In addition, because Manalo allows VPN access into all zones, including the trusted zone, compromising a business partner's network, or a GIAC executives home network, effectively compromises the GIAC internal LAN.

In terms of mitigating the attacks on the executives home LAN's, GIAC should mandate that all employees who work from home manage their local environment responsibly. This means using 128bit encryption on WLAN's, changing keys in frequently, turning SSID broadcast off, and using personal firewalls. In addition, it would be wise to enforce standards around the use of split tunneling (it should be disabled), and around the use of equipment like 802.11 access points, in terms of establishing hard to guess login ID's and passwords.

References

http://www.verisign.com

http://www.tripwire.com

http://www.cisco.com

[27] http://www.atstake.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

http://www.nai.com

http://www.stillsecure.com

http://www.apps.ietf.org/rfc/rfc1466.html

http://www.apps.ietf.org/rfc/rfc1918.html

http://www.sans.org/top20/

Inside Network Perimeter Security Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey, © New Riders Publishing 2003

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm

http://www.iana.org/assignments/ipv4-address-space

ftp://ftp.rfc-editor.org/in-notes/rfc2058.txt

http://www.rsasecurity.com

SNORT is a trademark of Sourcefire, http://www.sourcefire.com

http://www.securityfocus.com

http://www.securecomputing.com

Auditing Your Firewall Setup, Lance Spitzner, http://www.spitzner.net/audit.html

http://www.cisco.com/warp/public/707/3.html

http://www.cisco.com/warp/public/707/SSH-scanning.shtml

http://www.hping.org

http://www.packx.net

http.chi-publishing.com/portal/backissues/pdfs/ISB_2000/ISB0502/ISB0502JBWT.pdf

http://www.packeteer.com

Network Stumbler, Copyright © Marius Milner 2001-2002.

http://www.atstake.com

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.