

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

GIAC Certified Firewall Analyst
Practical Assignment
Version 2.0

Lesa Ludwig

October 20, 2003

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

GIAC Enterprises is a fortune cookie saying broker that has recently made the decision to go online. While the company has a strong commitment to its customers, suppliers and partners to protect the integrity of all business dealings, it is a small company employing only 40 people world wide and operating with a limited budget. Expanding into ecommerce has forced the company to rethink its security strategy and redesign its network to ensure that data and transactions are kept secure. This paper will examine a possible design for the company's network perimeter, an audit of the proposed design and an attack on another proposed design for the purpose of illustrating the point that security is a process not a product.

© SANS Institute 2003, Author retains full rights.

ASSIGNMENT 1

GIAC Enterprises has a small IT staff with expertise exclusively in the Windows environment and therefore prefers that, when possible, a Windows compatible solution is used.
In designing the network we must keep the following groups in mind:

- Customers (Companies or individuals that purchase bulk online fortunes)

  Connect to the web server on the external service network where they can browse the available fortunes and subscription packages. They can then use HTTPS to purchase and track orders through GIAC's custom web interface.

- Suppliers (Companies that supply GIAC Enterprises with their fortune cookie sayings)

  GIAC Enterprises contracts with a number of talented fortune tellers around the world. They connect to the external web server and then use HTTPS to upload their fortunes.

- Partners (International companies that translate and resell fortunes)

  Connect via VPN to connect to the partner database on the secure network.

- GIAC Enterprises employees located on GIAC Enterprise's internal network

  Customer service employees can use HTTP to access the Internet for research purposes. They have a web based application for accessing the internal customer database server in order to answer questions for customers who call in or to place orders for customers who are not comfortable placing orders over the Internet. This application was created by a consulting group that was hired by GIAC Enterprises last year. Prior to this employees would log into the database directly.

  Internal employees may also have a need to communicate internally and externally via email. Each employee is supplied with Outlook on their workstation.

- GIAC Enterprises mobile sales force and teleworkers
  GE has sales personnel who travel the globe looking for new customers. There is also a small group of employees who work remotely full time. These employees VPN to the internal network and access the same resources as internal employees or use HTTP and HTTPS to access the externally available systems.

- Public

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internet users who do not have a relationship with GE but are accessing the website or sending email to the company. These people will need access to the web server on the external service network and will need to be able to send email to the external email gateway.

Perimeter Devices:

Purpose of each perimeter device:
Border Router: This is the first line of defense. The border router is the first place incoming external traffic will enter as it comes into the network. The border router is designed to filter out any invalid traffic such as malformed packets or illegal addresses. This router is a Cisco 1711 Security Access Router running IOS 12.2.

Firewalls: GIAC Enterprises has chosen to use an IPCop version 1.3.0 firewall. This firewall is fork of Smoothwall, an open source firewall that runs on a hardened Linux kernel and is designed to take advantage of older hardware. Since GIAC has recently upgraded the workstations used by employees in the customer service area it has several older machines that are good candidates for this function.
With version 1.3 IPCop has moved to IPTables. IPtables has several advantages over its predecessor IPchains. IPtables is capable of stateful inspection of TCP, UDP and ICMP packets. IPtables simplifies how rules are processed and allows NAT to be separate from packet filtering which makes it easier to manage and more logical to apply. Finally lPTables improves on filtering capabilities and allows the administrator to rate-limit on both connections and logging to protect the network from flooding attacks.

External Firewall: This is the second line of defense. This device allows only certain types of traffic in based on a clearly defined ruleset. Traffic is allowed into the external service network or it is sent on to the secondary firewall. Only certain ports are allowed inbound to allow traffic to access the web servers or the internal network. All traffic that is not explicitly permitted is dropped by the firewall.

Internal Firewall: This device further filters traffic and allows only a very specific subset of packets to enter the inner service network and the internal network.

VPN Server: This device allows remote employees to authenticate to the internal network. It is located next to the external firewall. Users must authenticate to the VPN server and then authenticate to the internal network before being allowed access to protected resources. The VPN server will be a Windows 2000 box running Microsoft's VPN service. GIAC Enterprises will use this VPN to allow its remote employees and partners to connect to the internal network.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Intrusion Detection: GIAC does not believe that an intrusion detection system would be helpful at this time. Although the company recognizes the value of such a system it realizes that it does not have the staff or expertise necessary to make IDS useful in the GIAC Environment at this time.

SERVERS: GIAC Enterprises uses a standard server install consisting of Windows 2000 Server SP4 with any necessary patches applied before deployment. The systems are hardened following the guidelines at https://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/SecWin2k/06basewn.asp and http://nsa1.www.conxion.com/win2k/download.htm. All servers also run Symantec's Norton Antivirus Enterprise addition with signatures updated daily.

EMAIL: The external email server relays SMTP traffic through port 25 to the internal email server which runs Exchange 2000. The external email server runs Mail Sweeper 4.3 for SMTP to filter unwanted email attachments, block emails with inappropriate text (profanity, discriminatory language, spam) and add a layer of virus protection.

DNS: The DNS servers run Microsoft Windows 2000 with DNS service enabled. Only UDP traffic (port 53) is allowed to the DNS server on the external service network. The external DNS server is the only DNS server with access to the Internet and only to the root servers. All resolution requests are forwarded to the external DNS for the internal clients. The internal DNS server runs the DNS functions for the Active Directory structure. The internal and external DNS servers do not share records. This is known as split DNS.

WEB: There is one external web server running IIS 5.1 with URLscan (a tool to filter out invalid HTTP requests) and IISLockdown (a tool to eliminate unneeded services on the server). This server allows customers, suppliers and mobile employees to browse offerings, place and track orders and upload fortune files via HTTP (port 80) and HTTPS (port 443).

There is also an internal web server running IIS 5.1 with URLscan and IIS Lockdown. This server is for employees (either internal or mobile using the VPN) to access company information on the intranet (port 80) and use the web based database access tool.

DATABASE: The external database server runs SQL Server 2000. Only the web server may contact the database server. The external database replicates to the internal database server through the internal firewall over port 1433 every 15 minutes. Internal employees can contact the internal database server (also running SQL Server 2000) only via the proprietary web interface.

DC: The domain controllers are set up for Active Directory to manage the network. They are not allowed any access to or from the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

WORKSTATIONS: All workstations are deployed with Windows 2000 SP4 with all current patches. The browser is Netscape 7.1 secured according to the guidelines at http://www.nsa.gov/snac/support/guides/sd-10.pdf. All PCs and laptops have Symantec's Norton Anti-virus Enterprise Edition installed. Laptops are additionally deployed with the Zone Alarm Pro 4.0 personal firewall.

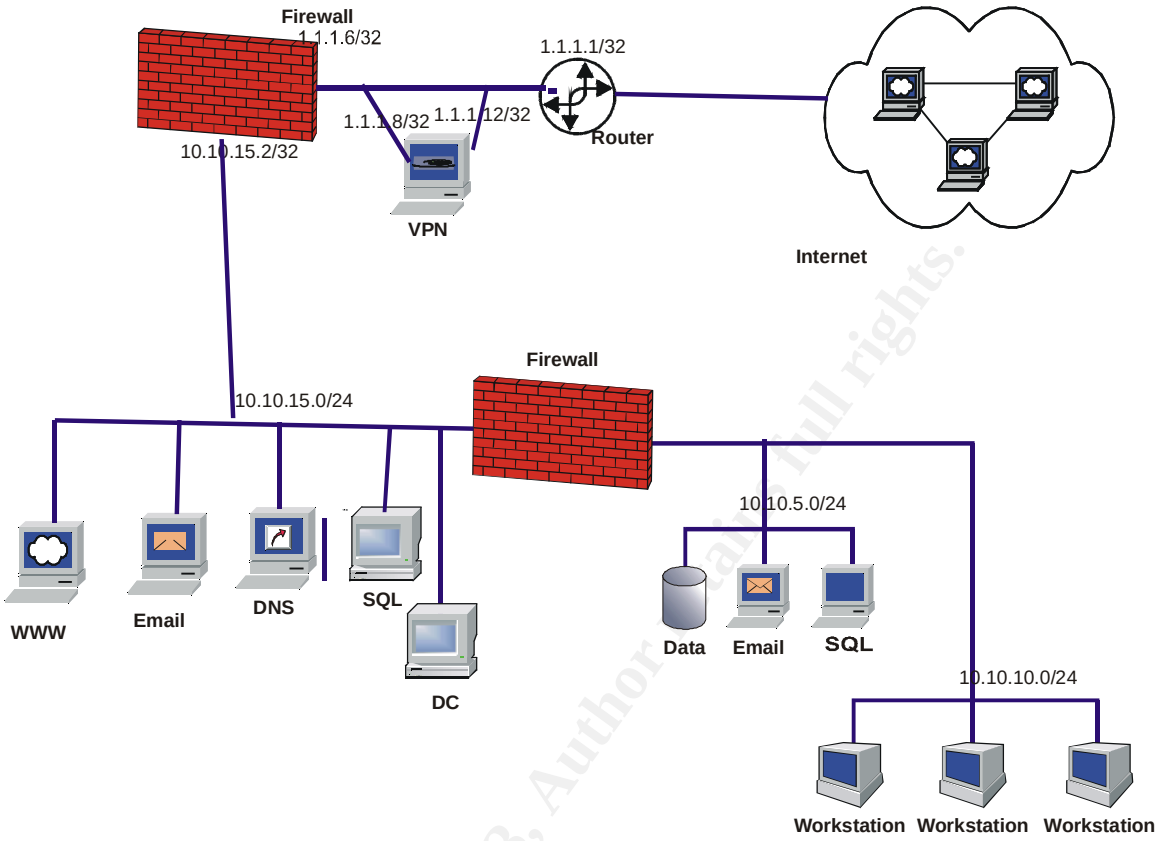
IP ADDRESSING SCHEME

For the purpose of this paper we will assume that GE has been assigned the public address range of 1.1.1.0/28. This range actually falls within the reserved category according to IANA, the address authority. Internally we will use addresses from the private address range of 10.0.0.0/8. This chart below details the addressing scheme.

Device	**IP Address/Range**
Router	1.1.1.1
Firewall – external interface	1.1.1.6
VPN Server – external interface	1.1.1.12
VPN Server – internal interface	1.1.1.8
VPN Clients	10.10.30.0/24
Service Network -External Web server -External DNS server -External Mail server	10.10.15.0/24
Internal Network Servers -Internal Mail server -Internal Domain controller -Database server -Internal database server	10.10.5.0/24
Internal Workstations	10.10.10.0/24

© SANS Institute 2003, Author retains full rights.

Network Diagram:



© SANS Institute 2003, Author retains full rights.

ASSIGNMENT 2

Border Router

The border router is the first line of defense in the perimeter. The device used by GE is a Cisco 1711 running IOS 12.2. In the policy below # indicates comments inserted by the author.

Securing the router:
#Enter into privileged mode to gain access to special commands for configuring
#the router:
enable

#Set name of the router:
hostname ge01

#enable encrypted passwords
service password-encryption

#turn on MD5 hashing for administrative password
enable secret <password>

#Turn off Identd an unnecessary service that relies on the computer
#administrator supplying the correct information:
no ip identd

#Turn off finger a command that will list logged on users and other account
#details.
no service finger

#Turn off bootp
no ip bootp server

#Cisco Discovery Protocol can be used to obtain information about the router's
#interfaces and about devices running behind the router. This needs to be
#turned off.
no cdp run

#GIAC is not running an X.25 network so this service can be turned off:
no service pad

#Turn off DEC MOP:
no service mop

#Turn off DNS name resolution to prevent the router from attempting to resolve
#addresses:
no ip domain lookup

© SANS Institute 2003, Author retains full rights.

```
#Turn off HTTP administrative interface:
no ip http server

#Enable inbound TCP keepalives
service tcp-keepalives-in
service tcp-keepalives-out

#Turn off proxy arp:
no ip proxy-arp

#Deny source routing
no ip source-route

#Stop directed broadcasts:
no ip directed-broadcast

#Prohibit IP unreachable responses:
no ip unreachables

#Prohibit ICMP mask-reply messages
no ip mask-reply

#Prohibit IP redirects
no ip redirects

#Disallow unnecessary broadcast forwarding
no ip forward-protocol port 69
no ip forward-protocol port 53
no ip forward-protocol port 37
no ip forward-protocol port 137
no ip forward-protocol port 138
no ip forward-protocol port 67
no ip forward-protocol port 68
no ip forward-protocol port 49
no ip forward-protocol port 42
no ip helper-address

#Disable NTP
ntp disable

#Disable SNMP service
no snmp server

#Set the logging servers:
logging 1.1.1.37
```

© SANS Institute 2003, Author retains full rights.

```
#Set the local buffer size
logging buffered 16000

#login banner
This is system is for the use of GIAC Enterprises authorized users only.  Any
        unauthorized access is subject to legal and civil penalties.

#The ingress filter will explicitly block that which we do not wish to allow in.
#Block non-routable or unassigned IP addresses
Access-list 101 deny ip 10.0.0.0 0.255.255.255 any
Access-list 101 deny ip 172.16.0.0 0.15.255.255 any
Access-list 101 deny ip 192.168.0.0 0.0.255.255 any
Access-list 101 deny ip 224.0.0.0 31.255.255.255 any
Access-list 101 deny ip 127.0.0.0 0.255.255.255 any
Access-list 101 deny ip 0.0.0.0 0.255.255.255 any
Access-list 101 deny ip 2.0.0.0 0.255.255.255 any
Access-list 101 deny ip 5.0.0.0 0.255.255.255 any
Access-list 101 deny ip 7.0.0.0 0.255.255.255 any
Access-list 101 deny ip 23.0.0.0 0.255.255.255 any
Access-list 101 deny ip 27.0.0.0 0.255.255.255 any
Access-list 101 deny ip 31.0.0.0 0.255.255.255 any
Access-list 101 deny ip 36.0.0.0 0.255.255.255 any
Access-list 101 deny ip 39.0.0.0 0.255.255.255 any
Access-list 101 deny ip 41.0.0.0 0.255.255.255 any
Access-list 101 deny ip 42.0.0.0 0.255.255.255 any
Access-list 101 deny ip 49.0.0.0 0.255.255.255 any
Access-list 101 deny ip 50.0.0.0 0.255.255.255 any
Access-list 101 deny ip 58.0.0.0 0.255.255.255 any
Access-list 101 deny ip 59.0.0.0 0.255.255.255 any
Access-list 101 deny ip 70.0.0.0 0.255.255.255 any
Access-list 101 deny ip 71.0.0.0 0.255.255.255 any
Access-list 101 deny ip 72.0.0.0 0.255.255.255 any
Access-list 101 deny ip 73.0.0.0 0.255.255.255 any
Access-list 101 deny ip 74.0.0.0 0.255.255.255 any
Access-list 101 deny ip 75.0.0.0 0.255.255.255 any
Access-list 101 deny ip 76.0.0.0 0.255.255.255 any
Access-list 101 deny ip 77.0.0.0 0.255.255.255 any
Access-list 101 deny ip 78.0.0.0 0.255.255.255 any
Access-list 101 deny ip 79.0.0.0 0.255.255.255 any
Access-list 101 deny ip 83.0.0.0 0.255.255.255 any
Access-list 101 deny ip 84.0.0.0 0.255.255.255 any
Access-list 101 deny ip 85.0.0.0 0.255.255.255 any
Access-list 101 deny ip 86.0.0.0 0.255.255.255 any
Access-list 101 deny ip 87.0.0.0 0.255.255.255 any
Access-list 101 deny ip 88.0.0.0 0.255.255.255 any
Access-list 101 deny ip 89.0.0.0 0.255.255.255 any
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Access-list 101 deny ip 90.0.0.0 0.255.255.255 any
Access-list 101 deny ip 91.0.0.0 0.255.255.255 any
Access-list 101 deny ip 92.0.0.0 0.255.255.255 any
Access-list 101 deny ip 93.0.0.0 0.255.255.255 any
Access-list 101 deny ip 94.0.0.0 0.255.255.255 any
Access-list 101 deny ip 95.0.0.0 0.255.255.255 any
Access-list 101 deny ip 96.0.0.0 0.255.255.255 any
Access-list 101 deny ip 97.0.0.0 0.255.255.255 any
Access-list 101 deny ip 98.0.0.0 0.255.255.255 any
Access-list 101 deny ip 99.0.0.0 0.255.255.255 any
Access-list 101 deny ip 100.0.0.0 0.255.255.255 any
Access-list 101 deny ip 101.0.0.0 0.255.255.255 any
Access-list 101 deny ip 102.0.0.0 0.255.255.255 any
Access-list 101 deny ip 103.0.0.0 0.255.255.255 any
Access-list 101 deny ip 104.0.0.0 0.255.255.255 any
Access-list 101 deny ip 105.0.0.0 0.255.255.255 any
Access-list 101 deny ip 106.0.0.0 0.255.255.255 any
Access-list 101 deny ip 107.0.0.0 0.255.255.255 any
Access-list 101 deny ip 108.0.0.0 0.255.255.255 any
Access-list 101 deny ip 109.0.0.0 0.255.255.255 any
Access-list 101 deny ip 110.0.0.0 0.255.255.255 any
Access-list 101 deny ip 111.0.0.0 0.255.255.255 any
Access-list 101 deny ip 112.0.0.0 0.255.255.255 any
Access-list 101 deny ip 113.0.0.0 0.255.255.255 any
Access-list 101 deny ip 114.0.0.0 0.255.255.255 any
Access-list 101 deny ip 115.0.0.0 0.255.255.255 any
Access-list 101 deny ip 116.0.0.0 0.255.255.255 any
Access-list 101 deny ip 117.0.0.0 0.255.255.255 any
Access-list 101 deny ip 118.0.0.0 0.255.255.255 any
Access-list 101 deny ip 119.0.0.0 0.255.255.255 any
Access-list 101 deny ip 120.0.0.0 0.255.255.255 any
Access-list 101 deny ip 121.0.0.0 0.255.255.255 any
Access-list 101 deny ip 122.0.0.0 0.255.255.255 any
Access-list 101 deny ip 123.0.0.0 0.255.255.255 any
Access-list 101 deny ip 124.0.0.0 0.255.255.255 any
Access-list 101 deny ip 125.0.0.0 0.255.255.255 any
Access-list 101 deny ip 126.0.0.0 0.255.255.255 any
Access-list 101 deny ip 127.0.0.0 0.255.255.255 any
Access-list 101 deny ip 169.254.0.0 0.0.255.255 any
Access-list 101 deny ip 173.0.0.0 0.255.255.255 any
Access-list 101 deny ip 174.0.0.0 0.255.255.255 any
Access-list 101 deny ip 175.0.0.0 0.255.255.255 any
Access-list 101 deny ip 176.0.0.0 0.255.255.255 any
Access-list 101 deny ip 177.0.0.0 0.255.255.255 any
Access-list 101 deny ip 178.0.0.0 0.255.255.255 any
Access-list 101 deny ip 179.0.0.0 0.255.255.255 any
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Access-list 101 deny ip 180.0.0.0 0.255.255.255 any
Access-list 101 deny ip 181.0.0.0 0.255.255.255 any
Access-list 101 deny ip 182.0.0.0 0.255.255.255 any
Access-list 101 deny ip 183.0.0.0 0.255.255.255 any
Access-list 101 deny ip 184.0.0.0 0.255.255.255 any
Access-list 101 deny ip 185.0.0.0 0.255.255.255 any
Access-list 101 deny ip 186.0.0.0 0.255.255.255 any
Access-list 101 deny ip 187.0.0.0 0.255.255.255 any
Access-list 101 deny ip 188.0.0.0 0.255.255.255 any
Access-list 101 deny ip 189.0.0.0 0.255.255.255 any
Access-list 101 deny ip 190.0.0.0 0.255.255.255 any
Access-list 101 deny ip 192.0.2.0 0.0.0.255 any
Access-list 101 deny ip 197.0.0.0 0.255.255.255 any
Access-list 101 deny ip 223.0.0.0 0.255.255.255 any
Access-list 101 deny ip 224.0.0.0 0.255.255.255 any

#Block netBIOS/IP ports
Access-list 101 deny tcp any any range 135 139
Access-list 101 deny udp any any range 135 139
Accees-list 101 deny tcp any any 445

#Block TFTP
Access-list 101 deny udp any any 69

#Block Syslog
Access-list 101 deny udp any any 514

#Block SNMP
Access-list 101 deny udp any any range 161 162

#Block  ICMP redirects and echo requests
Access-list 101 deny icmp any any host-redirect echo

#Allow anything that was not explicitly denied
Access-list 101 permit any any

#Define an access group and assign it to a specific interface:
Interface Serial 0
ip access-group 101 in


#Extended Egress.  This filter will help ensure that we are not leaking information
#out onto the Internet.
Access-list 102 deny tcp any any range 135 139
Access-list 102 deny udp any any range 135 139
Access-list 102 deny tcp any any 445
```

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
Access-list 102 deny tcp any any range 6000 6255
Access-list 102 deny udp any any 69
Access list 102 deny udp any any 514
Access-list 102 deny udp any any range 161 162
Access-list 102 deny icmp any any echo-reply unreachable
Access-list 102 permit 1.1.1.0 0.0.0.255 log
Access-list 102 deny any log-input

#Define an access group and assign it to a specific interface:
interface Ethernet 0
ip access-group 102 in
```

If every rule were to be logged it would generate an overwhelming amount of data. There are many misconfigured networks and automated attack tools that spoof addresses and continuously pour out unwanted traffic that will be dropped by the router. We would like to know if certain rules are triggered. If an internal machine is trying to access the Internet via an IP other than GIAC's assigned range it is important for GIAC to find that machine and fix the problem. It is also important to track any traffic that is being denied egress through the border router. This can help in troubleshooting network problems and in identifying compromised machines.

FIREWALL POLICY

Once the firewall is installed and all patches are applied it is time to configure the system and set up the rule base. The firewall is configured to compliment the router but the approach is the opposite. Instead of allowing anything that is not specifically denied, the firewall denies anything that is not explicitly allowed. The IPCop firewall is administered remotely via a web browser over either port 81 for insecure communication or 443 for secure traffic. By default only machines on the green interface can connect to IPCop via either the web interface or SSH. This can be manually configured to accept outside IP's but it is not recommended and will not be done here. In GIAC Enterprises' case a Windows 2000 Professional machine running Internet Explorer 5.0 SP2 is used from the internal network. We will go through the settings for the external firewall. In the section on the internal firewall I will highlight the differences.

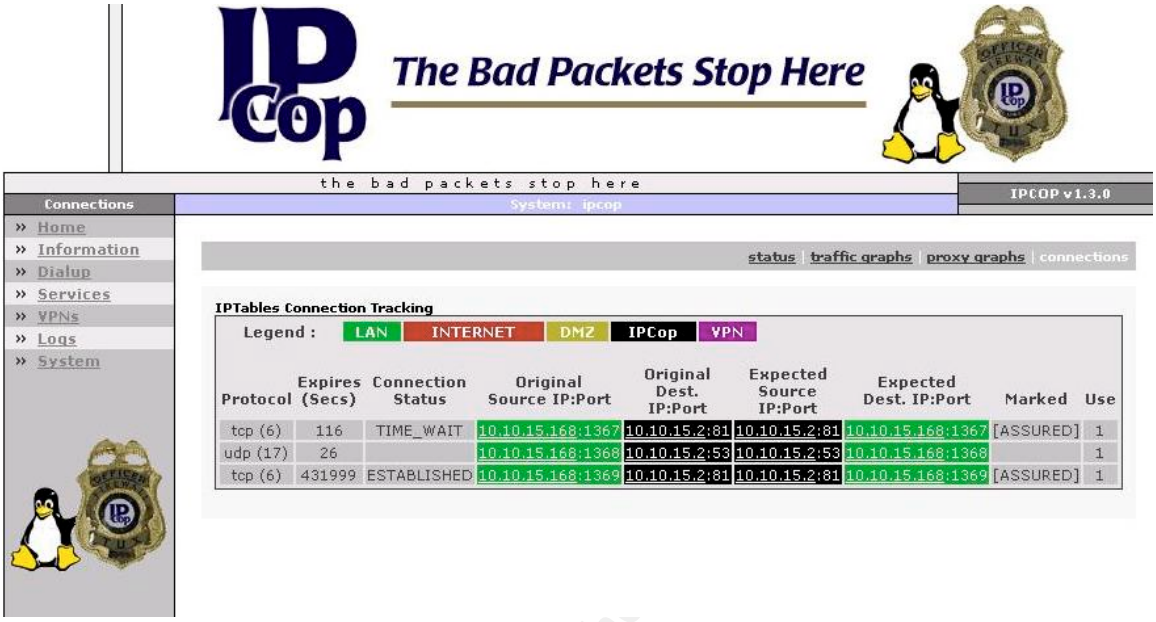
INFORMATION

The information page shows the status of all the services on the firewall. It also shows valuable information regarding disk and memory usage and uptime statistics. Also on this screen you can find information on each interface, what modules are loaded and the kernel version.

The connections section of the Information page shows the state table. IPCop is a stateful firewall which means that it tracks each tcp session and only allows

© SANS Institute 2003, Author retains full rights.

those sessions which have been established through an allowed rule. The state table shows the status of various connections to the IPCop firewall.



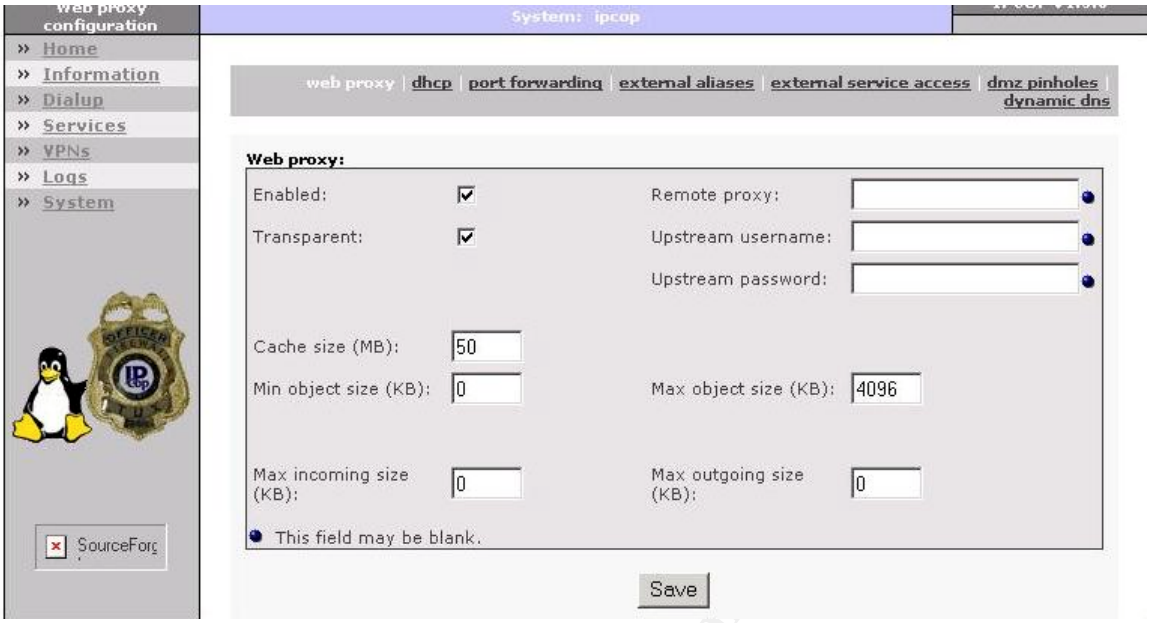
DIAL UP

The dialup tab allows you to set up your ISP connection via dialup or ADSL. GIAC Enterprises does not use this type of connection for their Internet service so nothing on this screen needs to be changed

SERVICES

The services window allows you to enable and configure the services that IPCop runs. It opens by default to the web proxy tab.

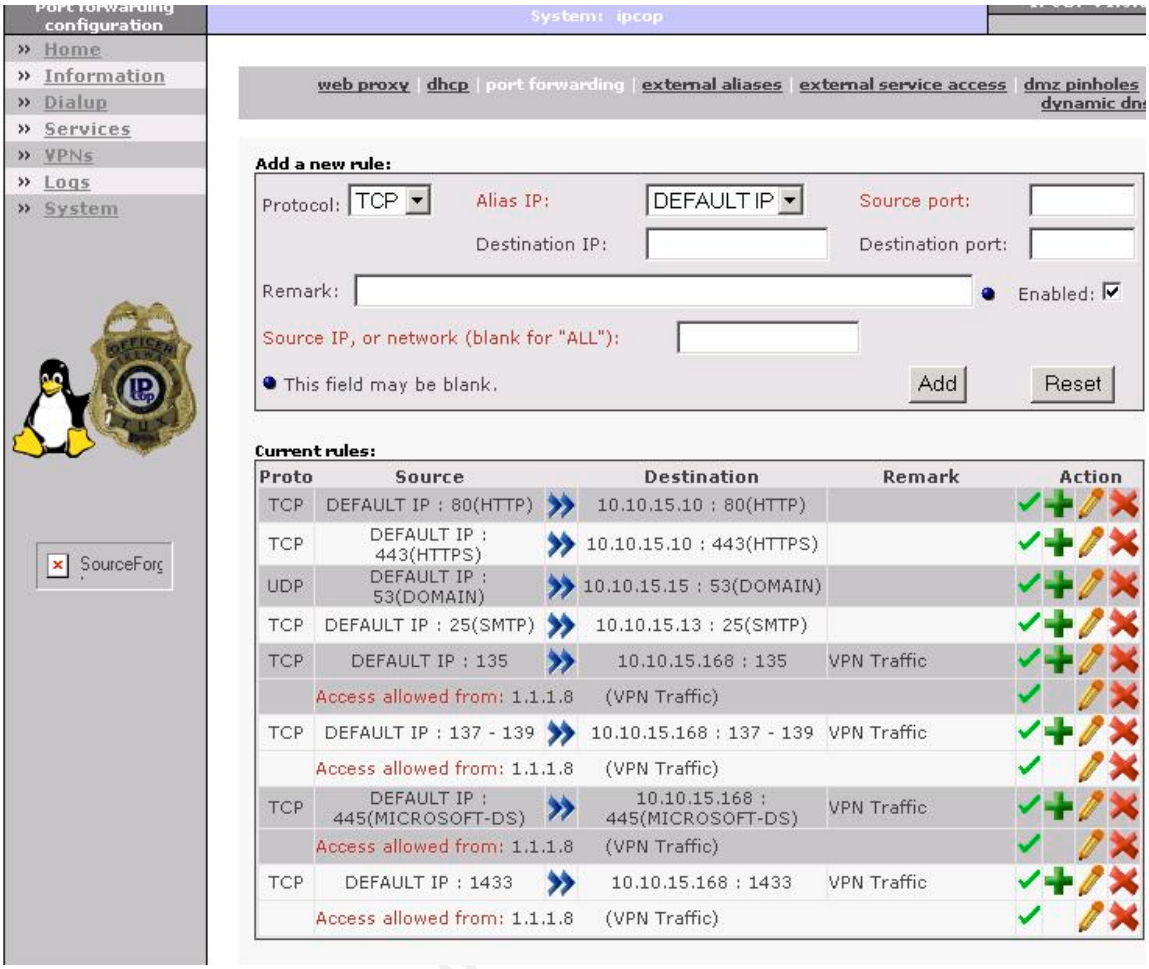
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



The web proxy service will make accessing web sites faster by caching FTP and web requests. HTTPS requests and pages containing user names and passwords will not be cached even if the service is enabled. This safeguard helps protect privacy interests and provides greater security for passwords. You can set the amount of disk space that is used for the cache. I will enable the proxy to speed up web browsing. I will make it transparent which means that I do not need to configure the users' browsers to use the proxy, they will automatically be directed to cached pages. If I had not enabled transparent I would have had to set each browser to use port 800 on the IPCop box as the proxy.
Although not desired at this time it is possible to configure the proxy to block certain sites by modifying the etc/hosts file to contain the IP of the offending website. Full instructions on this modification can be found in the IPCop FAQ. A patch is also available to content filtering if you desire such capability.

The DHCP service allows the IPCop firewall to act as a DHCP server for the network. Since all the machines connected to this firewall have static IP address we will not need to use DHCP on the external firewall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



Port forwarding allows you to direct traffic for a certain service to a different system. This is used for NAT on the IPCop. All traffic coming in to the network on a specific allowed port will be forwarded to an internal server. For instance GIAC's web server has an IP address of 10.10.15.10. We can set the rule to forward all inbound traffic for port 80 for normal web traffic and port 443 for secured web traffic to 10.10.15.10 on those respective ports. All other servers on the service network are setup in a similar fashion. This means that an attacker will only see the IP of the firewall and not any of the IPs on the internal network. As with the VPN server, it is possible to configure the firewall to accept certain traffic only from a specific IP address. If the router is doing its job it will not allow any traffic with a source of our legal IP range to reach the firewall so we have a relatively high certainty that any traffic coming from the IP address of the VPN server is indeed from that server.

In version 1.3.0 of IPCop, it is no longer necessary to use the external service access page to open the ports used for port forwarding. IPCop automatically opens any ports with a port forwarding setting.

The complete rules are:

TCP Port 80 (http) → 10.10.15.10 – this allows the public, customers, suppliers, and remote employees to connect to the web server to get information about GIAC Enterprises and the products that it sells.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

TCP Port 443 (https) → 10.10.15.10 – This allows customers, suppliers and remote employees to connect to a secured portion of the web server to perform transactions, check account status and update account information via encryption.
TCP Port 25 (smtp) → 10.10.15.13 – this allows the public, suppliers, customers and employees to send email to and receive email from GE.
UDP Port 53 (DNS) → 10.10.15.15 – this port is the standard port for DNS services. Only UDP is allowed. DNS can use TCP if there is a large amount of information that needs to be returned to the querier however for most DNS requests UDP is sufficient.
All traffic from the VPN server is routed to the internal firewall (10.10.15.168). This includes ports 135, 137, 138, 139, 445 for Microsoft networking and 1433 for SQL traffic. Because IPCop uses port 445 as its default https administration port some configuration on the firewall must be done to allow for standard Microsoft networking.
To change the default ports the administrator must SSH to the firewall and edit two files. The first file is /etc/httpd/conf/httpd.conf. All occurrences of port 445 in this file must be changed. I chose to use port 448. After that file is edited the web server must be stopped and restarted by issuing the following commands:

killall httpd
httpd –DSSL

Now that the default port has been changed, you must let the web interface know that this port is available for use. To do this edit the file called /home/httpd/cgi-bin/portfw.cgi. Substitute the new port number, 448 in this case, in the line my @tcp_reserved = (81,222,445). Now the standard method for adding a port forwarding rule can be followed.

The external alias section allows one to set up IPCop to use different external IP addresses for the machines behind the firewall. This could require manual manipulation of the firewall's routing table. Since GE intends to take advantage of NAT and port forwarding we do not need to use this feature.

The external service access feature in versions of IPCop previous to 1.3.0 was used in conjunction with the port forwarding feature to open access to the green networks for the services permitted. With version 1.3.0 this function is included in the port forwarding feature. The external service access section now controls access only to the IPCop device itself. Through this feature you can set up access for administration of the firewall from anywhere on the Internet. This type of access does not fit with GIAC's security policy therefore this feature will not be used.
Port 113 is open by default but there are no services GIAC wishes to allow that would use this port so I have closed it.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

DMZ pinholes can be used to allow machines on the orange (DMZ) network to connect to machines on the green (Internal) network. Since GIAC enterprises does not use an orange network interface on the firewall this part is not applicable.

Dynamic DNS allows entities without static IP addresses to use a subscription service to maintain a domain name pointed at their servers. Users of DYNDNS services must send updated information to their service provider every time their IP address changes, which could be every time they log onto their ISP. IPCop will handle updating the DYNDNS service automatically. This window on the IPCop allows such entities to input the appropriate information. GIAC has a static pool of addresses so this service does not apply to GIAC Enterprises.

The help window will walk an administrator through all the tabs in this section.

The IDS window allows you to enable Snort intrusion detection logging on your firewall. To enable click the box and save.

VPN

This function is primarily designed to allow VPN between IPCop firewalls but it can also inter-operate with other VPN solutions. GIAC will be using a different VPN solution so this will not be enabled.

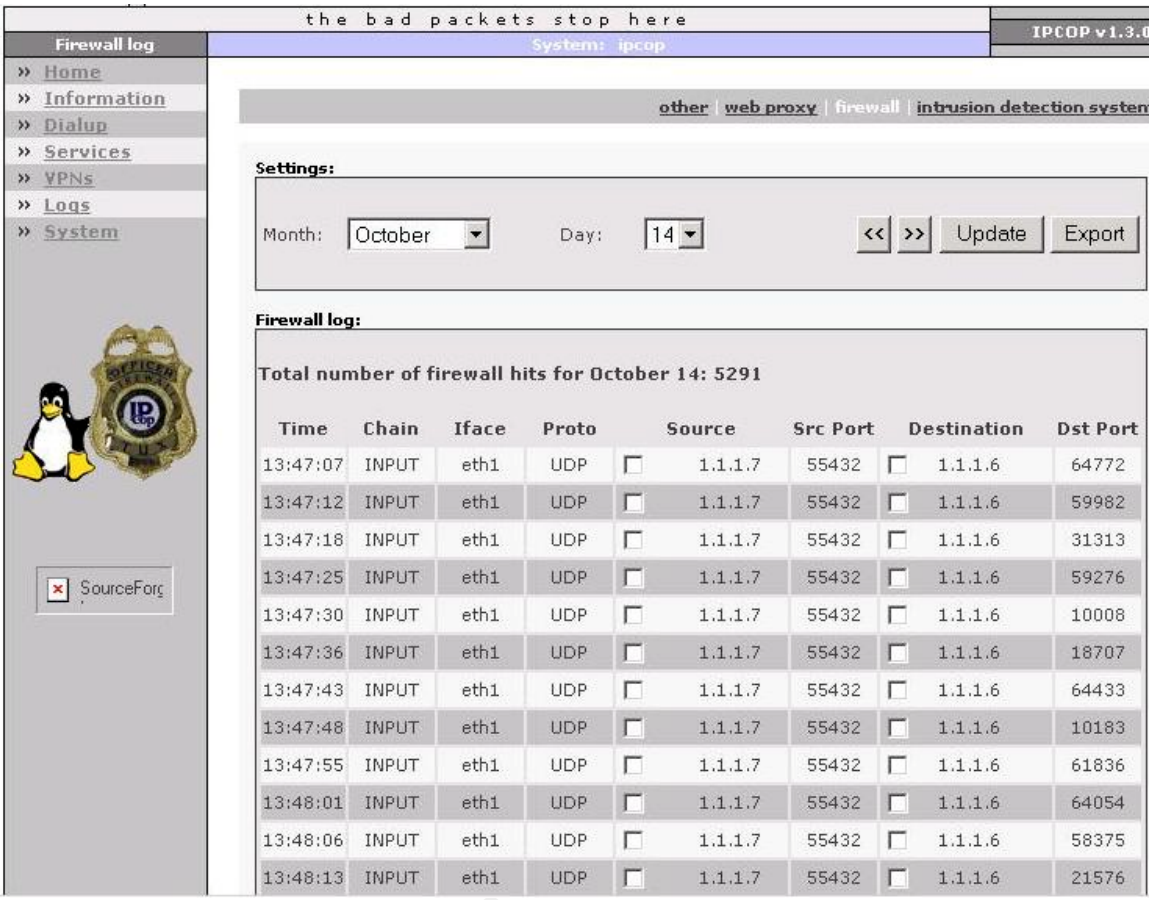
LOGS

The IPCop is capable of maintaining several different logs. These logs are broken out by other, web proxy, firewall, and intrusion detection systems. Logs can be viewed one day at a time. You can select the date you wish to view by using the drop down menus or you can step through days using the << and >> buttons.

The Other log keeps track of system and other miscellaneous logs. Each separate log can be selected from the Section drop down menu. There are nine different sections that track events such as connections to the firewall, DHCP and kernel activity and software updates to the firewall.

Proxy logs allow the administrator to see the files that have been cached by the proxy service. Filters can be put in place to prevent certain types of files from being kept in the proxy logs. The filters are enabled by checking the enable ignore filter box. The logs track the source IP and website as well as keeping a time log of web activity through the proxy.

© SANS Institute 2003, Author retains full rights.



Time	Chain	Iface	Proto	Source	Src Port	Destination	Dst Port
13:47:07	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	64772
13:47:12	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	59982
13:47:18	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	31313
13:47:25	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	59276
13:47:30	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	10008
13:47:36	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	18707
13:47:43	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	64433
13:47:48	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	10183
13:47:55	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	61836
13:48:01	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	64054
13:48:06	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	58375
13:48:13	INPUT	eth1	UDP	1.1.1.7	55432	1.1.1.6	21576

Dropped packets are tracked by the Firewall section of the logs. This log will display time, interface and the Iptables chain where the rule triggering the drop resides. The firewall logs are rounded out by including protocol, source port and IP address, and destination port and IP addresss. For information on a listed IP address, click the check box and press Lookup at the bottom of the list.
Logs for the intrusion detection system can be accessed under the aforementioned category. These logs identify the Snort ID number and priority of the rule that triggered the alert. Other tracking information such as IP information, timestamp, short description of the incident and hyperlinks to relevant information are also shown.
Logs are kept by the system for four weeks. GIAC Enterprises sees no need to setup an elaborate system for archiving the logs elsewhere. The firewall will be part of the normal backup rotation and as such all logs will be backed up onto removable media and stored in a secure offsite facility. In the event that GIAC network personnel need access to historic log data they can recall the backup tapes from storage following normal GIAC procedures.

SYSTEM WEB PAGES

Updates

Every time your IPCop firewall connects to the Internet it will check the IPCop update site for system patches. The updates page will allow you to see current

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

patch level, install updates and manually get updates to the firewall. Clicking on the Refresh Update List button will force IPCop to look for updates and download them to the machine that is running the browser upon which the administrator is browsing the update page. Once the updates are downloaded one can browse to the place where it is saved and apply it to the firewall. Only official patches work with this system. Some patches will cause the IPCop machine to reboot. Read all warnings on patches carefully and plan accordingly. The Opera web browser does not function correctly with this method of uploading.

Time

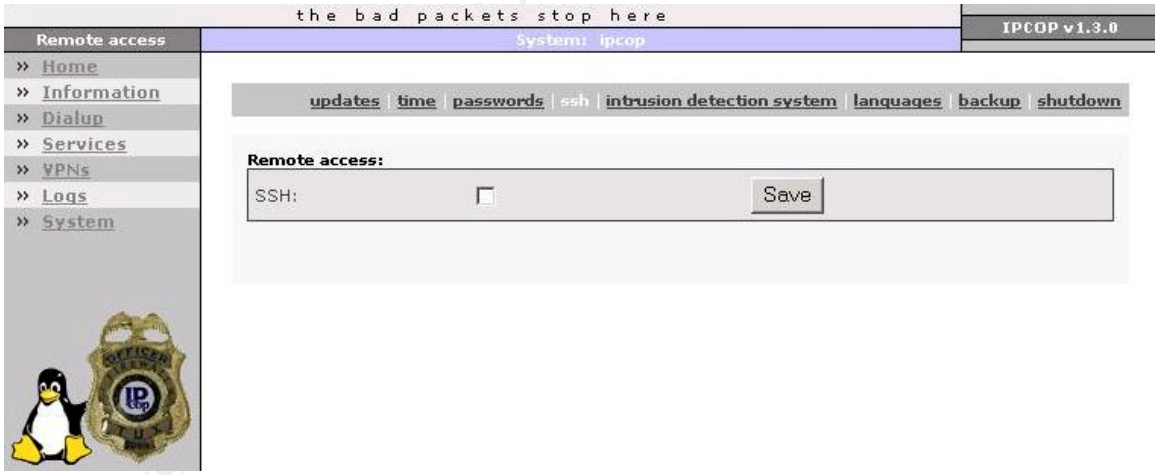
The time page allows the administrator to set up the firewall to use the network time protocol to ensure that the server is keeping accurate time. This setting can be set for an official Internet time server or for an internal server. You set up NTP by checking the enable box and entering the IP address of the NTP server(s) you wish to use. You may also set up the firewall to update its time every specified time interval or to require it to be manually updated by clicking on the Set Time Now button.

This feature on the IPCop only allows the firewall to update its own time. It is not equipped to serve as a time server for other machines on the network.

Passwords

From this screen you can update the admin or dial user passwords. Enter the desired password in the fields provided and click save.

SSH



This window allows you to enable SSH on the firewall for remote access. As a general rule this should be left disabled. When SSH is needed the admin can logon through the web interface and enable it. The admin must remember to disable it as soon as they are done using it. Any SSH client should be able to connect with the firewall when this is enabled however IPCop uses port 222 instead of the standard SSH port of 22.

© SANS Institute 2003, Author retains full rights.

Intrusion detection system
The intrusion detection system that is bundled with IPCop is Snort. Snort is a widely used, well-respected open source IDS. To turn on this functionality within IPCop you must check the box and click save.

Languages
The language screen allows you to choose in which language the IPCop screens will be displayed. During set up you were asked to select a language and that may be all that you need. If your chosen language was not available during setup you may be able to download it and activate it here.

Backup
With the backup screen you can create a backup of your configuration file on a floppy disk. To create the backup you should put the floppy disk in the drive and click on Backup. At this time IPCop cannot overwrite DOS formatted floppy disks. You must format the disk for Linux before you can complete your backup. All messages generated during the backup process will display on the Backup screen.
Should you need to restore your configuration from this disk you can reinstall IPCop. Early in the installation process you will be prompted for the system configuration floppy. At this point you simply put your floppy in the drive and click on the Restore button.

Shutdown
This screen allows remote shutdown and restart of the firewall.

INTERNAL FIREWALL

External Services:
There is no need to allow any traffic through on port 80 or 443 so we will disable those rules.
We will use this section to create rules that will allow our database server in the external service network to connect with the database servers on the internal service network. We will allow the database server (10.10.15.11) through the internal firewall on port 1433 to the internal database server (10.10.5.11).

The VPN will need to pass traffic to the internal network over ports 135, 137-139 and 445.

Although the machines on the internal network use dynamic IPs, we will not need to use the firewall as a DHCP server. The Windows domain controller will handle this task.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

RULES

IpCop is generally administered from the browser interface however there are times when an administrator wants to configure the firewall in a way that is not possible through the browser. This is done either by directly logging into the firewall if physical access is possible or via SSH over the network. Once you are logged into the firewall as root you may create custom rules using IPTables syntax. Here is where I will create egress rules to control the flow of traffic out of the GIAC network. This is necessary because IPCop has a default allow rule that enables any traffic leaving the network to pass unhindered. This could allow for information leakage, unauthorized user activity, or for automated attacks such as worms to leave the network and cause havoc on the Internet.

First I will create a new user defined chain. It is possible to put the new rules into an existing IPTables chain however that would require that any custom rules be reentered every time there is an upgrade to the firewall. The new rules are put in /etc/rc.d/rc.local to preserve them. Any text editor could be used to create the rules file and upload it to the firewall.

Create a new chain:
iptables -N CUSTOMINPUT
Syntax:
/sbin/iptables = invoke iptables
-A CUSTOMINPUT = Append the rule to the CUSTOMINPUT chain
-i = incoming interface
-p <protocol> = name of the protocol to which the rule should be applied
-s <IP> = source IP
--dport <port> = destination port number
-j <chain> = jump to a specific rule chain.

#The rules are as follows:
Drop all outbound packets that do not have a valid internal IP address:
iptables -A CUSTOMINPUT -i eth0 -s ! $GREEN -j DROP

#Allow DNS traffic out from internal network:
iptables –A CUSTOMINPUT –p udp –s $GREEN --dport 53 -j ACCEPT

#Allow HTTP traffic out from internal network:
iptables –A CUSTOMINPUT –p tcp –s $GREEN --dport 80 –j ACCEPT

#Allow HTTPS traffic out from internal network:
iptables -A CUSTOMINPUT -p tcp -s $GREEN --dport 443 -j ACCEPT

#Drop everything else that is attempting to user the external interface:
iptables -A CUSTOMINPUT -i eth0 -s $GREEN -j DROP

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

We do not need many rules because there are not many protocols over which internal machines are allowed to communicate. The last rule in the list automatically drops all traffic that was not permitted by a previous rule. This top down architecture makes it very important for the rules to be in order of most specific to least specific to ensure that the traffic matches the correct rule and is filtered appropriately.

VPN POLICY

Because of GIAC's predominantly Window's environment and the low number of users needing VPN, the company has decided to use the native VPN capabilities within the Windows 2000 operating system.

The first choice that must be made when going with this solution is whether to use L2TP or PPTP. Both use the same underlying protocol PPP (Point to Point Protocol) but from there they diverge.

PPTP or Point to Point Tunneling Protocol: PPTP was developed by Microsoft. It uses PPP (Point-to-Point Protocol) authentication methods. This protocol only supports Microsoft Point-to-Point Encryption (MPPE). The hosts involved in this type of data exchange maintain two connections. One connection to port 1723 is for maintenance traffic which consists of PPTP Echo Requests and PPTP Echo-Reply messages. The second connection is for the tunneled traffic. PPTP encrypts the packet and adds a PPP header and trailer. The PPP frame is then encapsulated in a GRE (Generic Routing Encapsulation) packet. The use of GRE restricts PPTP to use only on IP networks. Finally PPTP encapsulates the frame with an IP header and then adds a PPP header and trailer before sending the packet on its way.

L2TP or Layer 2 Tunneling Protocol: L2TP is a combination of PPTP and Layer 2 Forwarding which was developed by Cisco. This protocol takes the strengths of each of its component protocols and combines them into one standard. In L2TP, the PPP frame is encapsulated within a L2F frame which is then encapsulated inside a UDP datagram for transmission over IP networks. L2TP frames can be compressed and/or encrypted using IPsec (Internet Protocol Security) ESP (Encapsulating Security Payload). This combination is known as L2TP/IPsec.

GIAC will use the full capabilities of the Windows VPN product by allowing both protocols to be used. This policy will ensure that all users who are authorized and need access can log into the VPN. GIAC encourages its employees and partners to use the advanced security features of L2TP whenever possible. L2TP presents two unique technology challenges that must be met

1) IPsec does not play well with NAT (Network Address Translation). A technique known as NAT-T (Network Address Translation Transversal) is required. This technique is not supported on Windows 2000 server. For this reason GE will position its VPN server in front of the external firewall. The router will provide some protection and standard hardening

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

techniques will help protect the machine and the network from compromise.

2) L2TP requires each client and server to have a valid certificate for authentication. This requires GIAC to build a server to issue the certificates.

POLICY

Setting up a VPN server on a Windows 2000 server is very easy. We will review the steps needed to configure the VPN server in the tutorial section. After the initial installation and set up of the service it is time to set up the policy.

The first decision to be made is how to set up the PPTP or L2TP ports. You may select Remote access or Demand-dial routing connections or both. GE will allow for both. Here is where you also select the maximum amount of ports. This is done for each protocol. GE will scale back the number of ports allowed from the default of 128 to 50 ports on each protocol. This means that no more than 50 users can use each protocol at one time. This number can be adjusted whenever necessary.

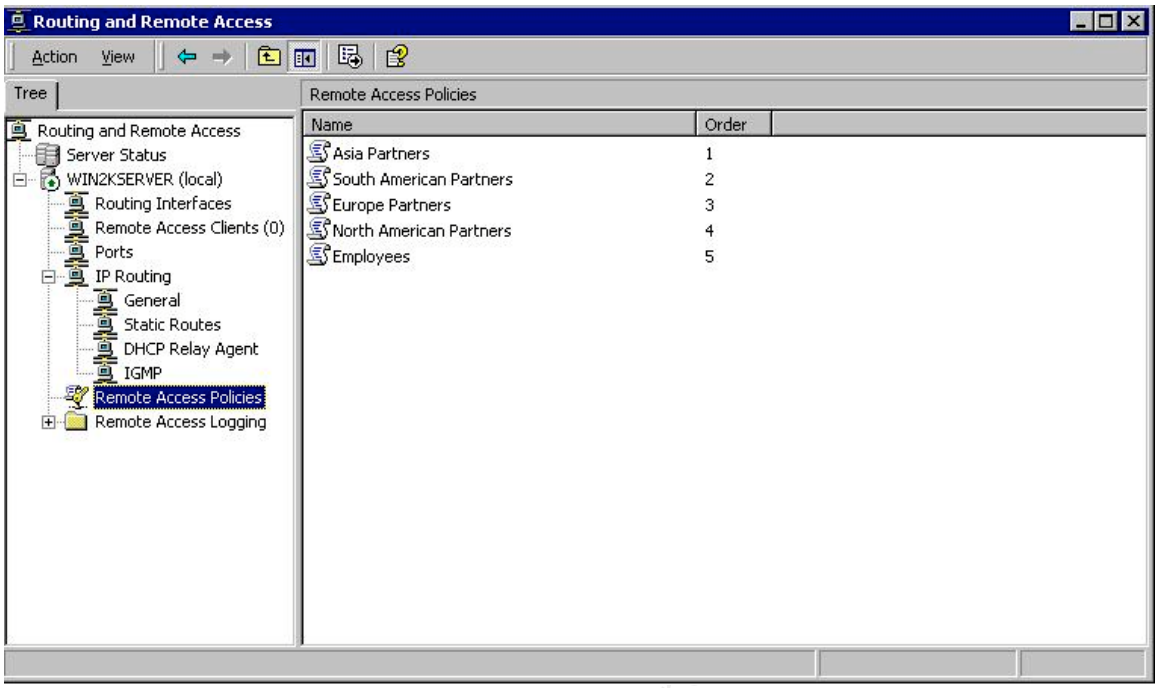
In order to facilitate the smooth flow of traffic, the server must be configured as a router. Once the Internet interface is identified, it is automatically configured with to allow only PPTP and L2TP traffic. All other traffic is dropped. In machines lower than Windows 2000 SP2 this must be configured manually. GE will select a medium amount of logging. GE will not track accounting information and will only accept MS-CHAPv2 (Challenge Handshake Authentication Protocol), MS-CHAP and CHAP authentication.

ACCESS POLICY

Access policies can be set by many parameters. Since this is a small enterprise with minimal access and basic security needs I will restrict access based on Windows groups that are predefined in the domain.

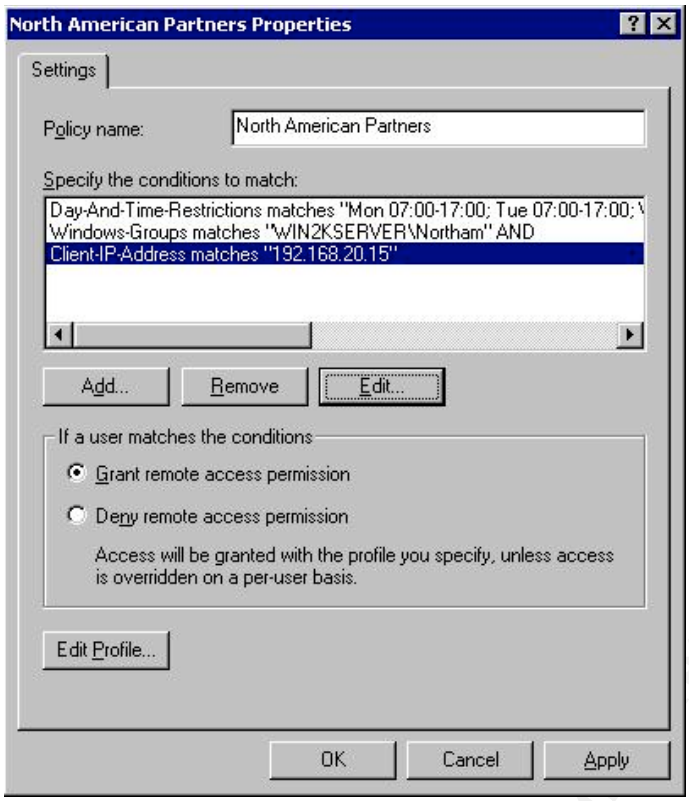
Select a name for the policy and click Next. At the Add Remote Access Policy screen select Add and you will be given a list of attributes you can select to configure your policy.

© SANS Institute 2003, Author retains full rights.



GIAC has separated its partners into regional groups. Each regional group will be allowed to access GIAC internal systems during time periods that correspond roughly to an 8-5 Monday-Friday work schedule. This will help to ensure that systems compromised either through physical access or remote access at a client's site will be limited in the time they have to do damage. Because the window is during working hours at the partner site, it is much more likely that someone will discover something amiss.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

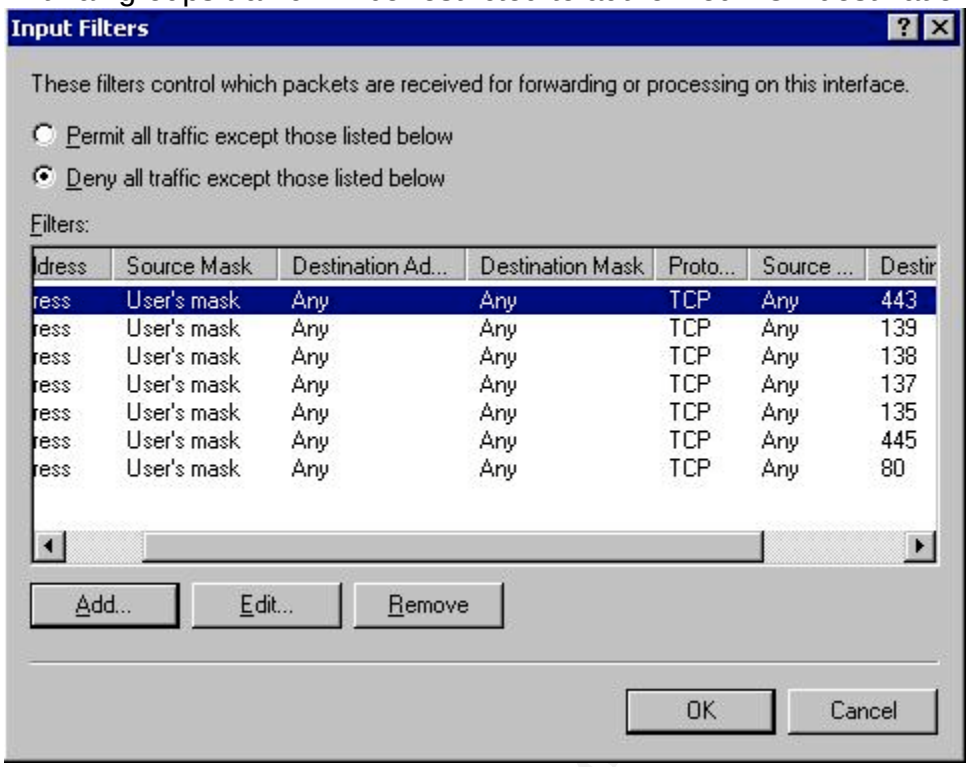


GIAC has no control over how its partners' networks are designed so it must make sure that its systems can support a wide variety of protocols and access methods. GIAC encourages its partners to use L2TP with GE supplied certificates. GIAC is protected by using network security in making sure that partner userids can only access systems which they will need to perform their business functions. GIAC will also put into place filters which only allow machines at authorized partner IP's to authenticate to the VPN server. Partners will be required to sign an agreement to maintain certain security standards including running current anti-virus software and taking reasonable precautions to ensure that GIAC's network is not compromised through their sites. Penalties for non-compliance include withdrawal of remote access privileges and possible financial liability for damages.

Employees who need access will be given 24/7 access but will be restricted by how they can authenticate to the network. Employees will be using GIAC supplied laptops which will be configured to use the L2TP protocol with certificates supplied by GIAC. As with the partners, network security restrictions will control user access to network resources.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

With all groups traffic will be restricted to authorized TCP destination ports.



VPN TUTORIAL

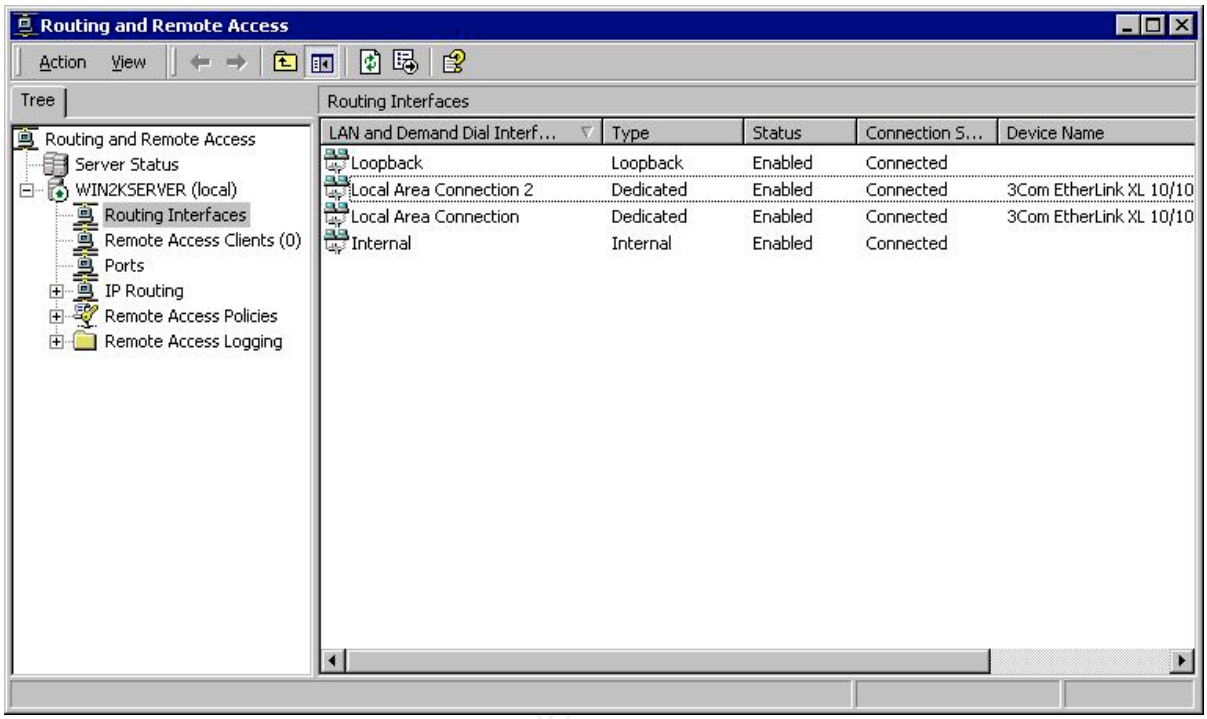
The nature of VPN on Windows 2000 does not allow it to be placed behind a firewall that does one-to-many network address translation as GIAC's IPCop is designed to do. As a result it will be placed in front of the firewall. Some would argue that putting a Windows machine in a high security position is not wise however GIAC's strength is in Windows technology and they will play to that strength. The management of GIAC's Information Systems department believes that a well configured and maintained Windows machine is more secure than a poorly configured Unix machine. They have therefore given the go ahead to use Windows 2000 on the VPN server outside of the firewall.

The server selected will be built using Windows 2000 Server SP 4 and all current patches will be applied. The server will be secured using standard GIAC deployment practices. Once the base operating system is secured as well as it can be we will begin to configure the VPN service.

The first step in deploying the VPN is to ensure that the network connections are functioning correctly. We will use 1.1.1.12 as the IP address of our external connection. The internal connection will be configured with the IP address of 1.1.1.8. The server will route the packets through to the external firewall. Once we have confirmed that the connections are working properly we can begin to configure the service on the server.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

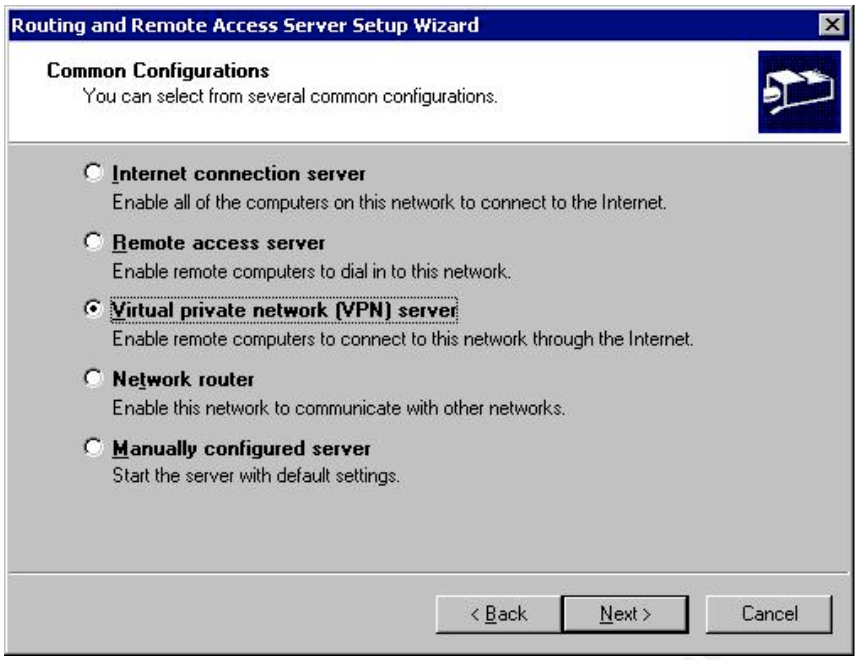
Bring up the Routing and Remote Access window from the Administrative Tools menu on the Start button.



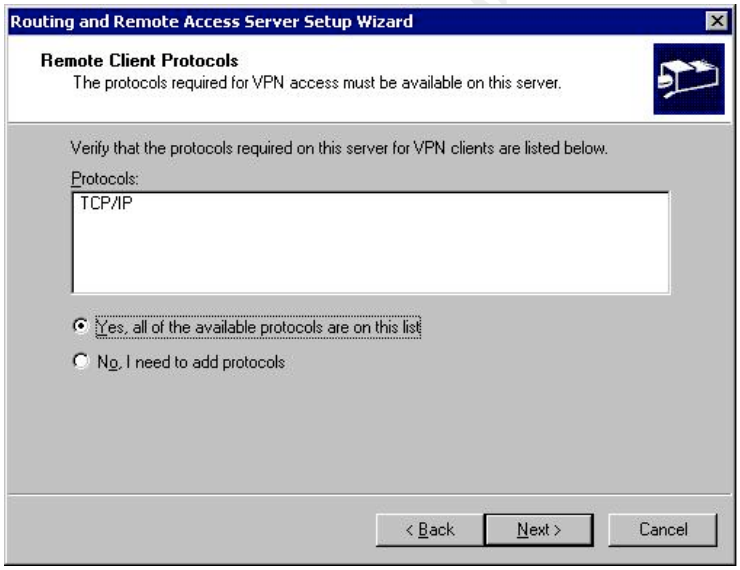
Select the name of the server in the tree (in this case WIN2KSERVER). Click Configure and Enable Routing and Remote Access on the Action menu. Click Next.

Select the radio button for Virtual Private network (VPN) server in the Common Configurations window. Click Next.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

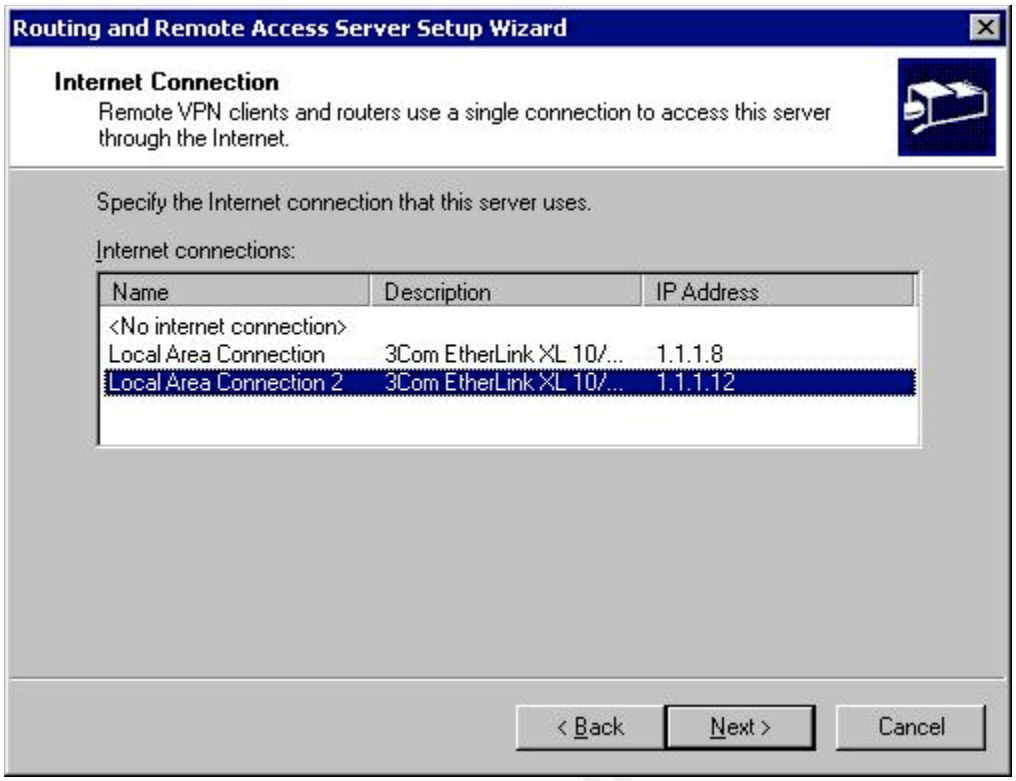


If TCP/IP is included in the list of required protocols then select Yes, all of the available protocols are on this list and click next. If the protocols you wish to use are not listed then you must add them to the server from the Network and Dial Up Connections folder before continuing with the VPN setup. Windows will automatically display help information on installing protocols after the user clicks Finish on the Cannot Continue screen.

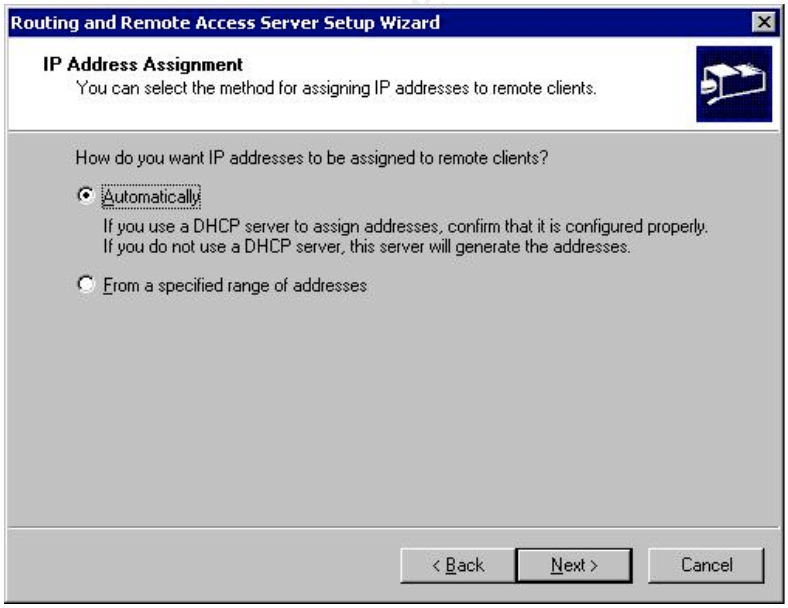


Select the connection that connects to the Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

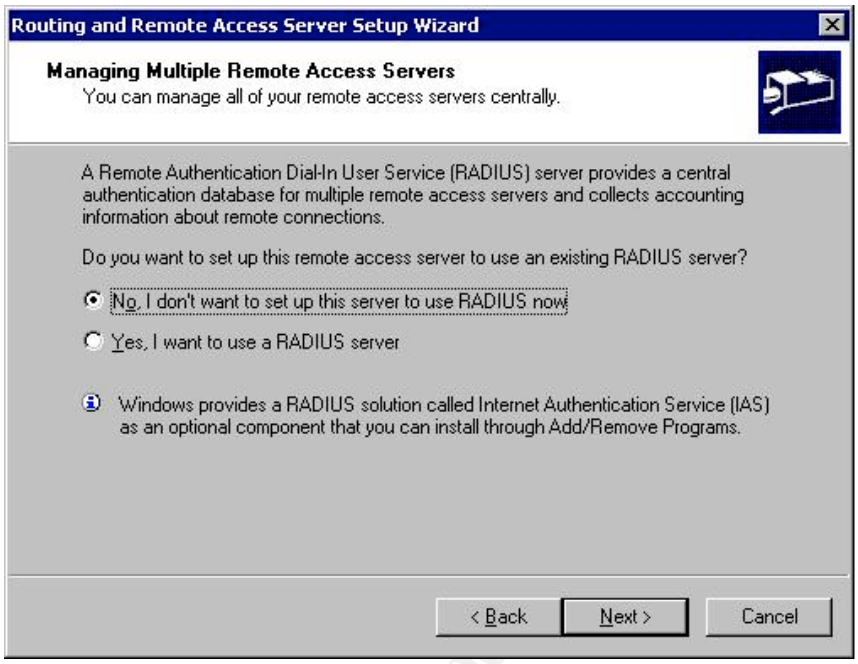


In the IP Address Assignment window you can either select a setting that will use the internal network's DHCP server to assign IP address to incoming clients or you can select a range of IPs to be used and allow the VPN server to function as a DHCP server. I will select Automatically.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The Managing Multiple Remote Access Servers window is next. Because this is a small operation and there is only one remote access server we do not need to use a separate RADIUS (Remote Authentication Dial-In User Service) server for authentication so I will select No, I don't want to set up this server to use RADIUS now. The VPN server will use it's own local user files to authenticate the incoming users. Windows offers IAS (Internet Authentication Service) as a RADIUS service that can be installed via the Add/Remove Programs window.



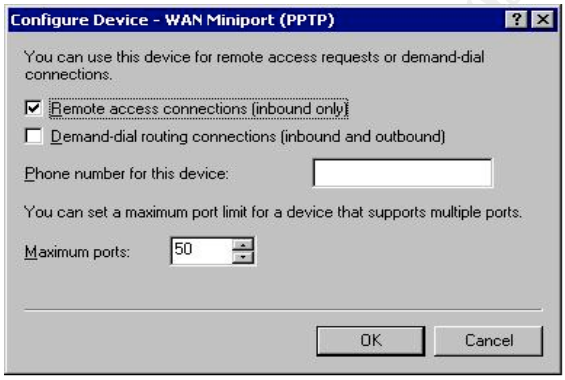
The Routing and Remote Access Server Setup Wizard is now complete. Click Finish.

Back on the Routing and Remote Access window right click Ports and select Properties.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



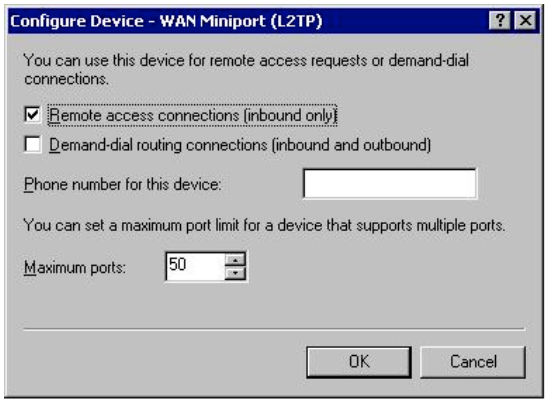
Each type of connection (PPTP, L2TP, Direct Parallel) must be configured individually. This is done by selecting the type of connection you would like to work with and clicking the Configure button. We'll start with PPTP.



Deselect the Demand-Dial routing box as we will not be allowing anyone to directly dial into a modem on the VPN server. Select Remote access connections. Because GIAC is a small operation I want to limit the number of simultaneous connections so I will set the maximum ports to 50. The maximum number of ports defaults to 128 and can be raised or lowered according to the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

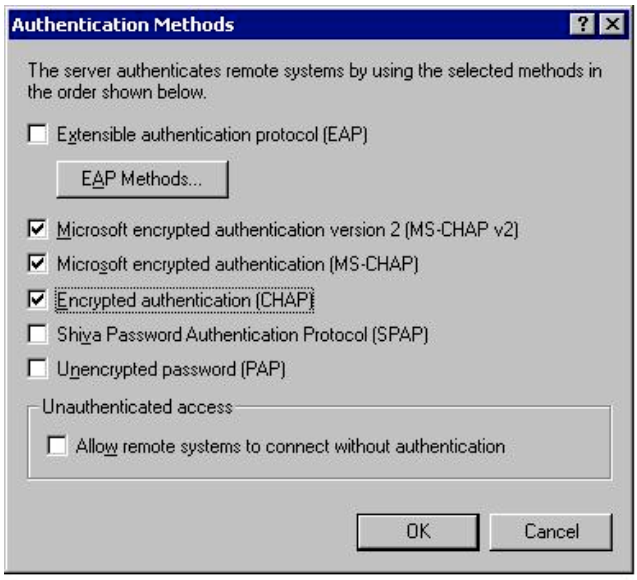
enterprise using the system. When lowering the number of ports during business hours you must be careful as you could disconnect users if the number of active connections is higher than the number of ports you select. Do the same thing for the L2TP device.



In order for this machine to correctly forward remote access traffic it must be enabled as a router. This is done by right clicking on the name of the server in the Routing and Remote Access window and selecting properties. Click the box for Router on the general tab and make sure that Local area network routing only is selected and LAN and Demand-dial routing is deselected.

Select the Security Tab and click on the Authentication Methods button. Select MS-CHAP v2, MS-CHAP and CHAP. No other authentication methods should be selected.

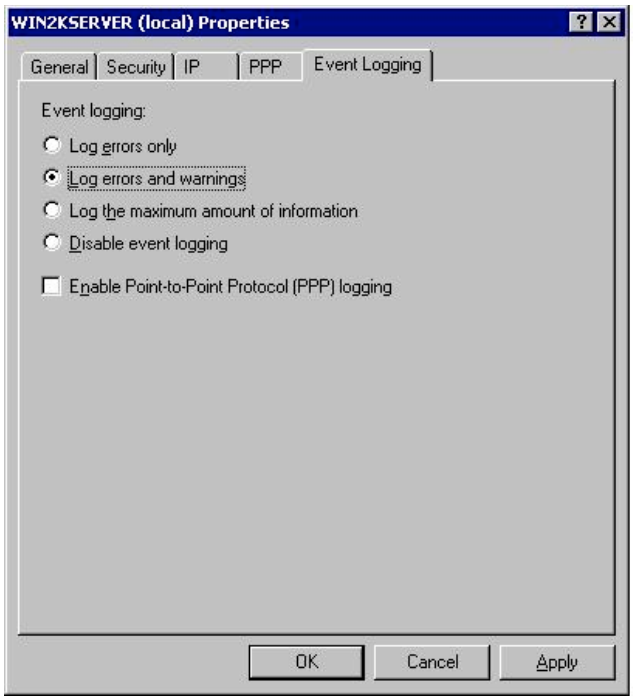
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



GIAC Enterprises uses password authentication via MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol version 2) for employees. This is a relatively strong authentication protocol that requires mutual authentication where the client is authenticated by the server and the server is authenticated by the client. GIAC enforces a password policy for all user ids that includes at least 10 characters using three of the following four types of characters: lower case alpha, upper case alpha, numeric, symbolic. Users are required to change their passwords every 60 days and may not use the same password for 12 iterations.

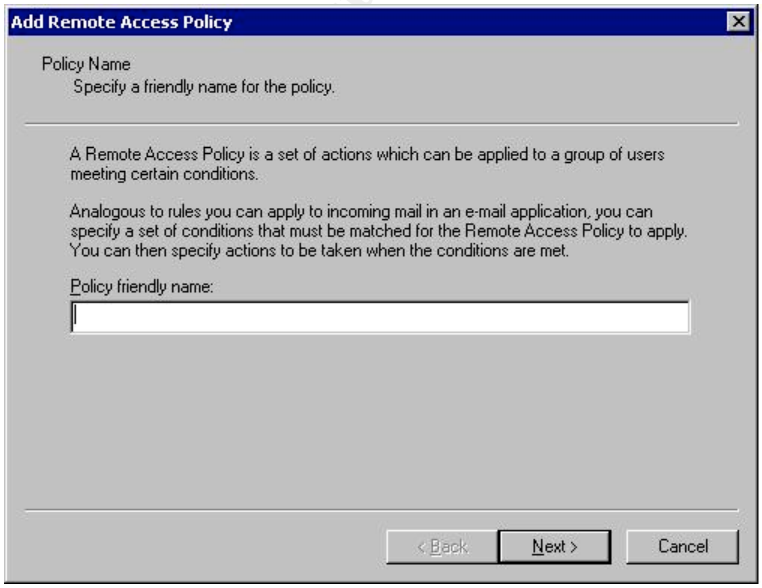
The final tab of interest on this window is the Event Logging tab. GIAC has already recognized that it does not have the resources or the desire to spend a great deal of time looking over logs so I will select Log errors and warnings.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



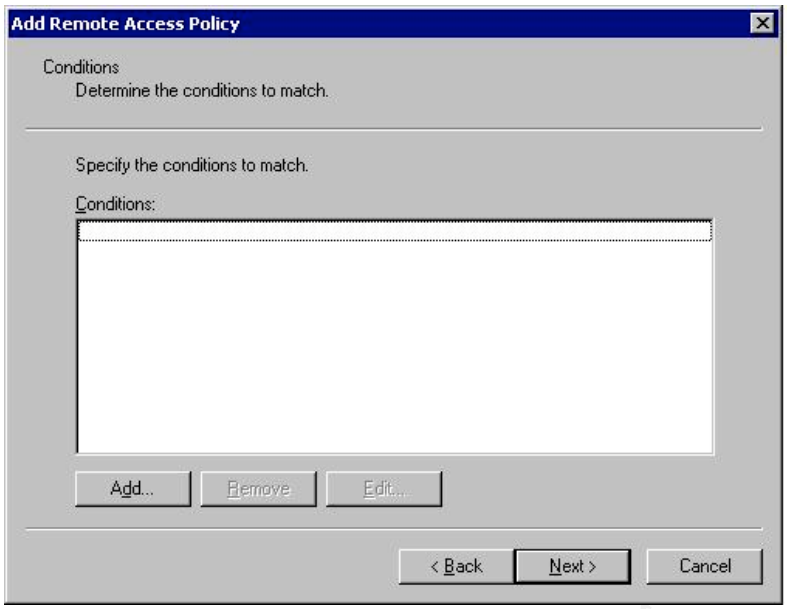
To set the policy for VPN usage click on Remote Access Policies. Delete the default policy of "Allow access if dial-in permission is enabled". If dial up connections were allowed on this server the default policy would be moved to the end of the policy list. To create a new policy right click on Remote Access Policy and select New Remote Access Policy.

You will be prompted to specify a name for this policy. Select a name that will be meaningful to anyone who might have need to look at the policies.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The next box will prompt you to determine the conditions you wish to match before allowing the connection. Select the Add button.

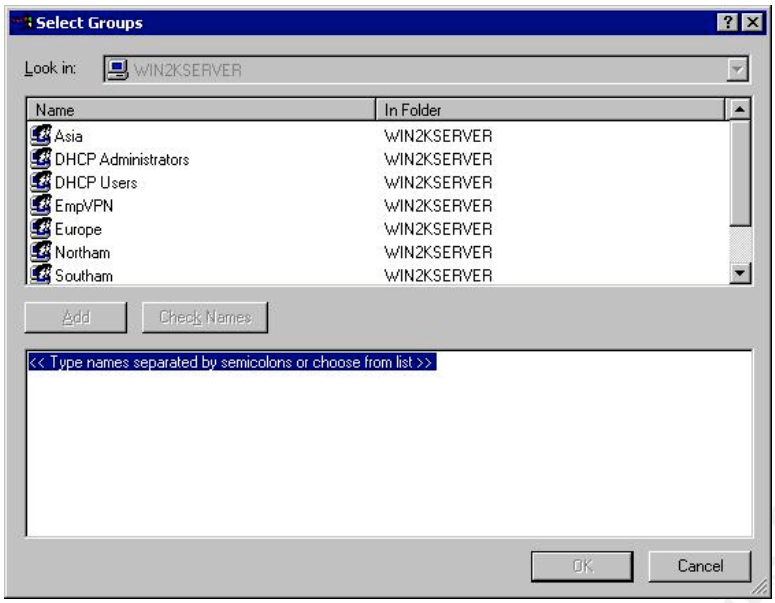


The next window will give you a list of options you can select to tailor your policy. You can refine the policy as much as you wish to fit your environment and security stance. You can set parameters to check for user id, group membership, protocol used, service type, day/time, origin or several other settings. For this tutorial we will select a simple policy of Windows-Groups.



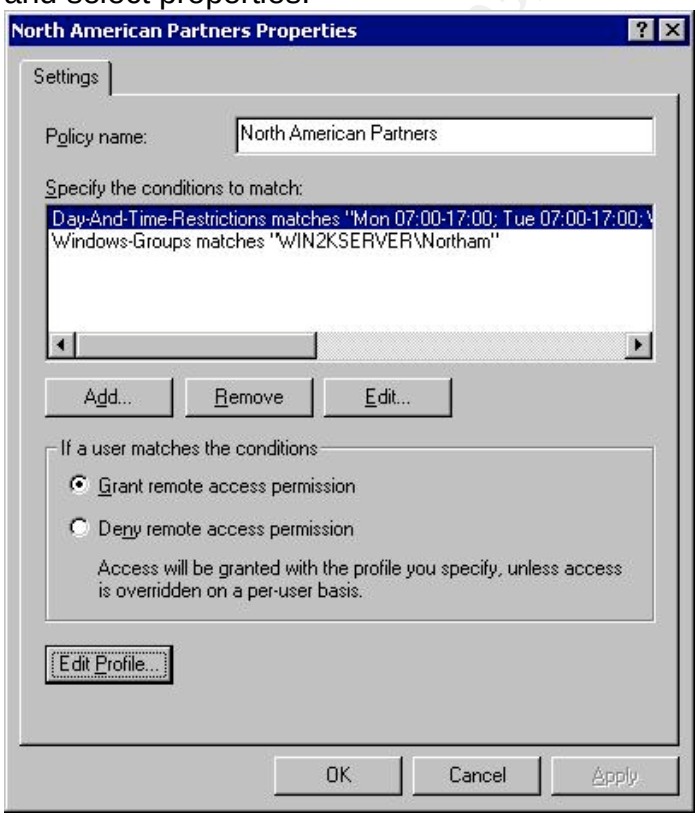
Select add

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



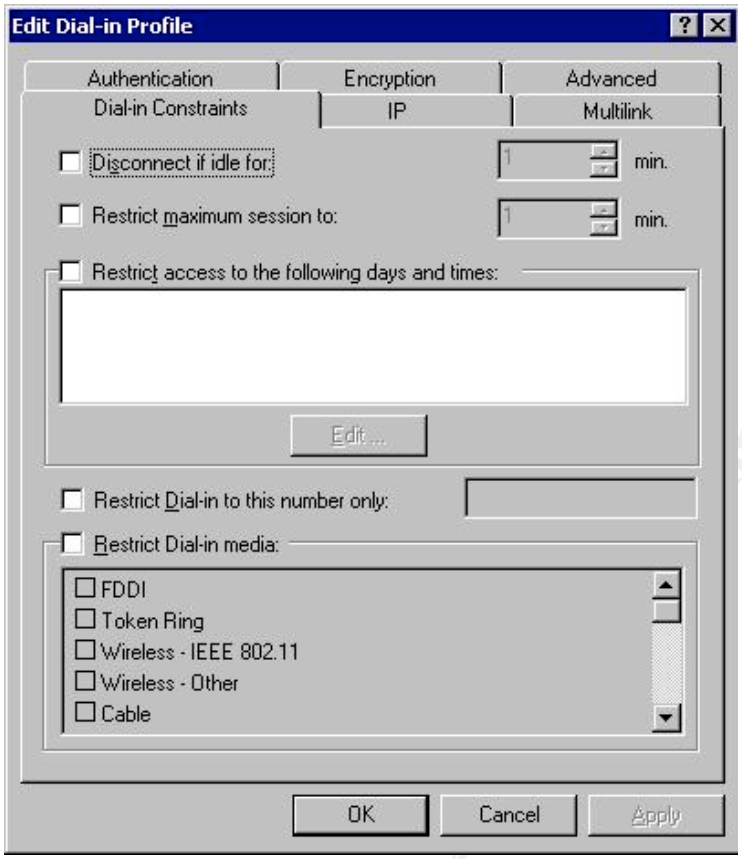
You may select as many groups as you wish by highlighting the group name and clicking the add button. If you wish to verify who is in the group you may highlight the group name and click on the check names button. This will verify the names and give you a chance to correct any that Windows cannot find.

To further refine the access policies right click on the policy you wish to modify and select properties.



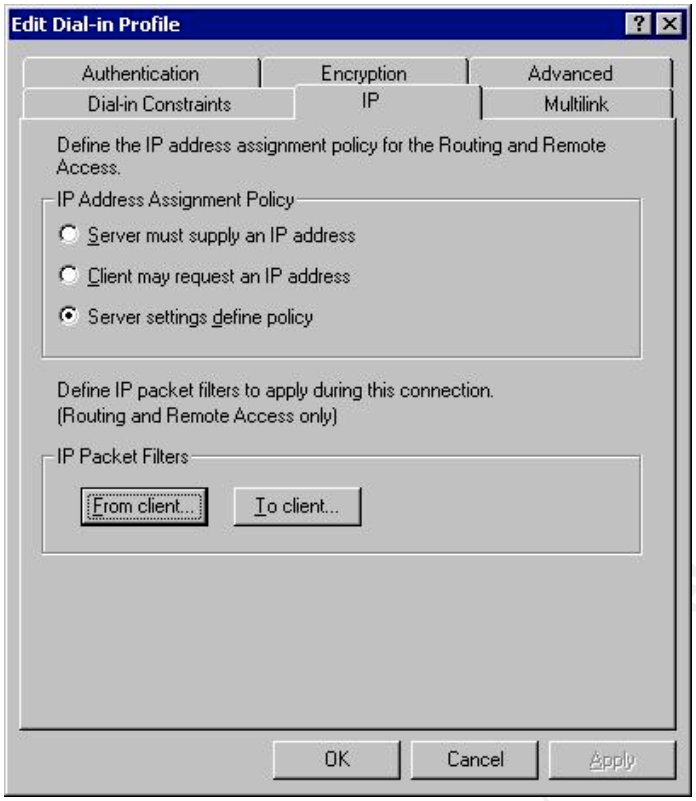
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Click on edit profile.
A window will come up that will enable the administrator to configure a variety of parameters.

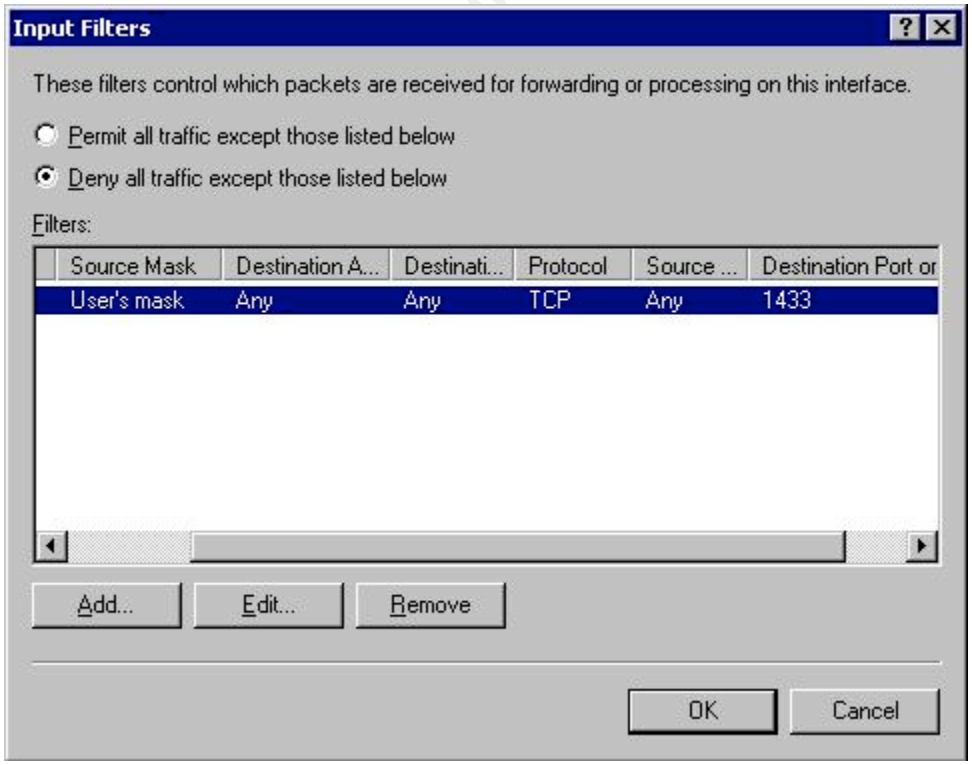


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Select the IP tab.



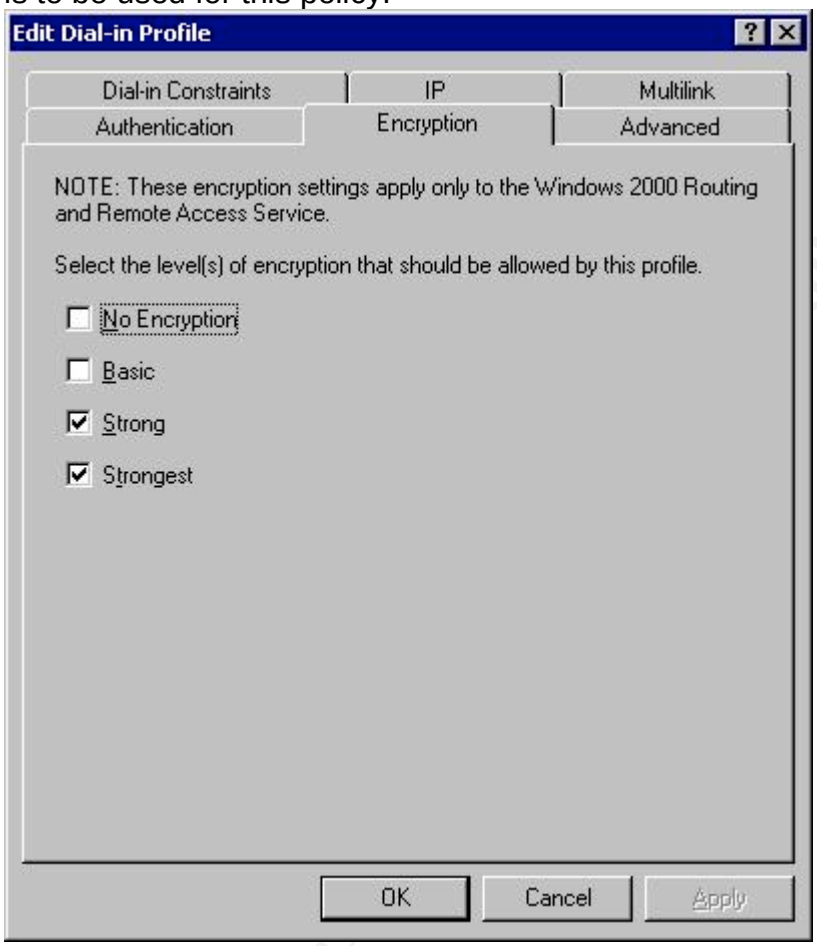
Click the From Client button.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

This will allow control over which packets are allowed from the client based on destination address, destination or source port and protocol. This can be configured in either a default allow or default deny policy.

The encryption tab allows the administrator to define the level of encryption that is to be used for this policy.



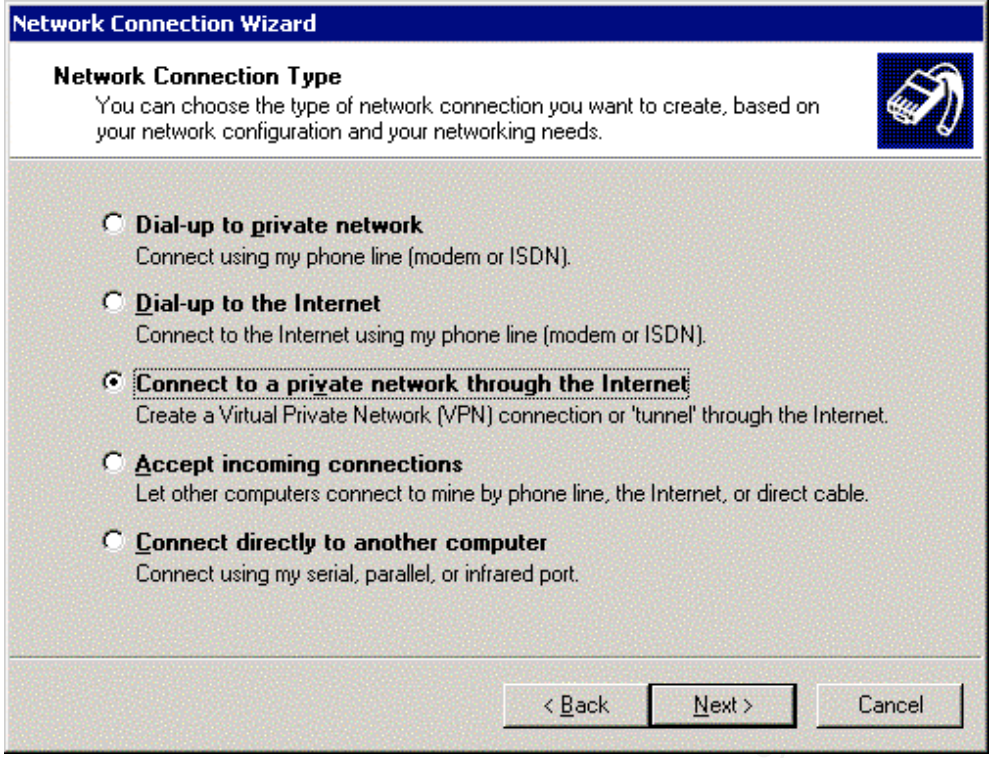
CLIENT SETUP

After the server is set up it is time to set up the clients. For the purpose of this tutorial I will examine setting up a Windows 2000 Professional workstation. The workstation will be using SP4 and has all the latest patches.

As with the server I first make sure the Internet connection is properly configured. GIAC does not accept direct dial connections so the remote employees will first dial in to a local ISP number for which GIAC has secured a contract.

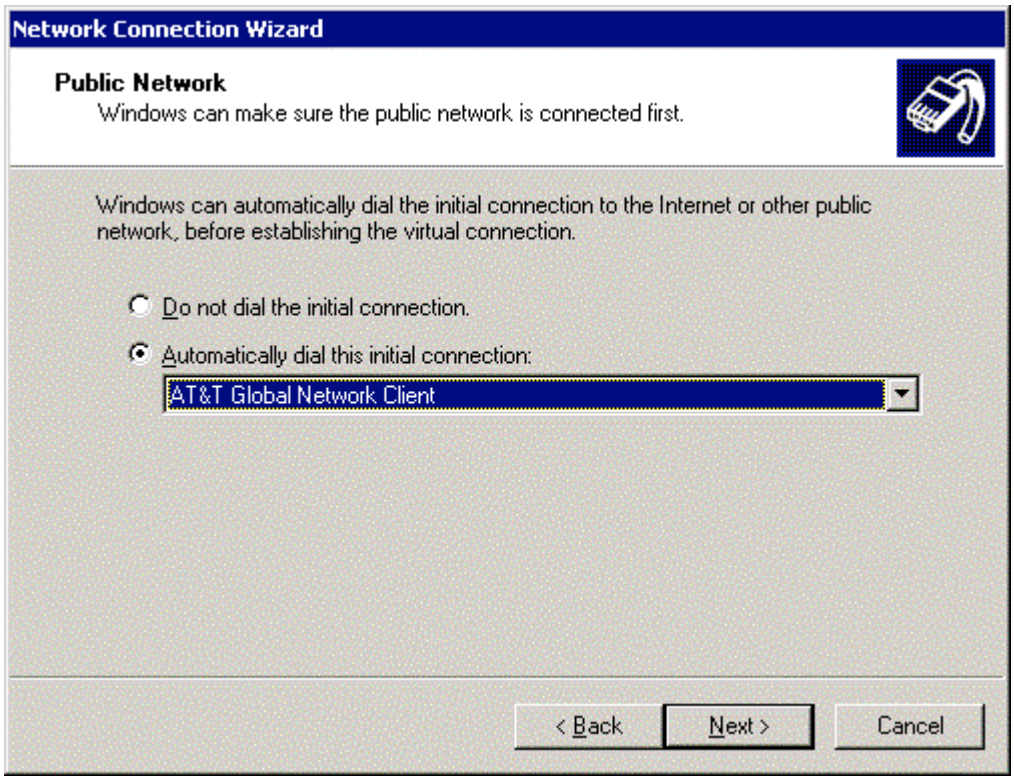
To configure the client connection select the Network and Dial-Up Connections options from the Settings menu on the Start button. Double click on the Make New Connection Icon. Click Next. Then select the Connect To a Private Network through the Internet option.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.



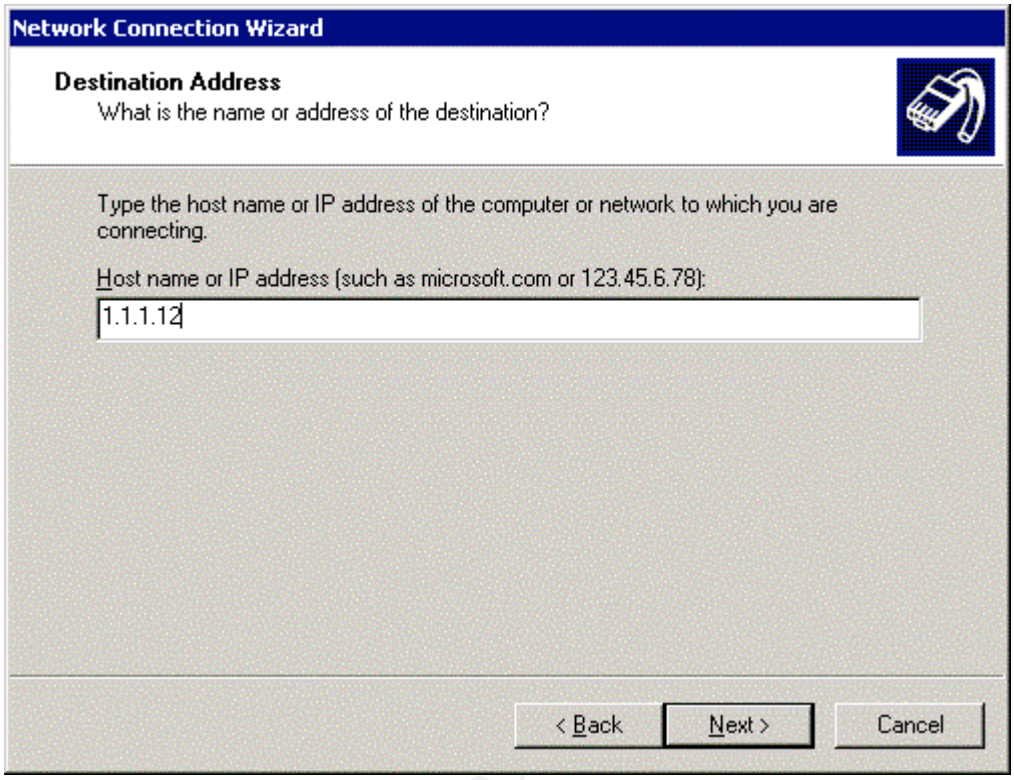
Click Next.

If you are connected to an always on connection such as a cable modem select Do Not Dial the Initial Connection. If you must use a dial-up connection for Internet connectivity select Automatically Dial This Initial Connection and select your dial-up Connection from the list. Click Next.



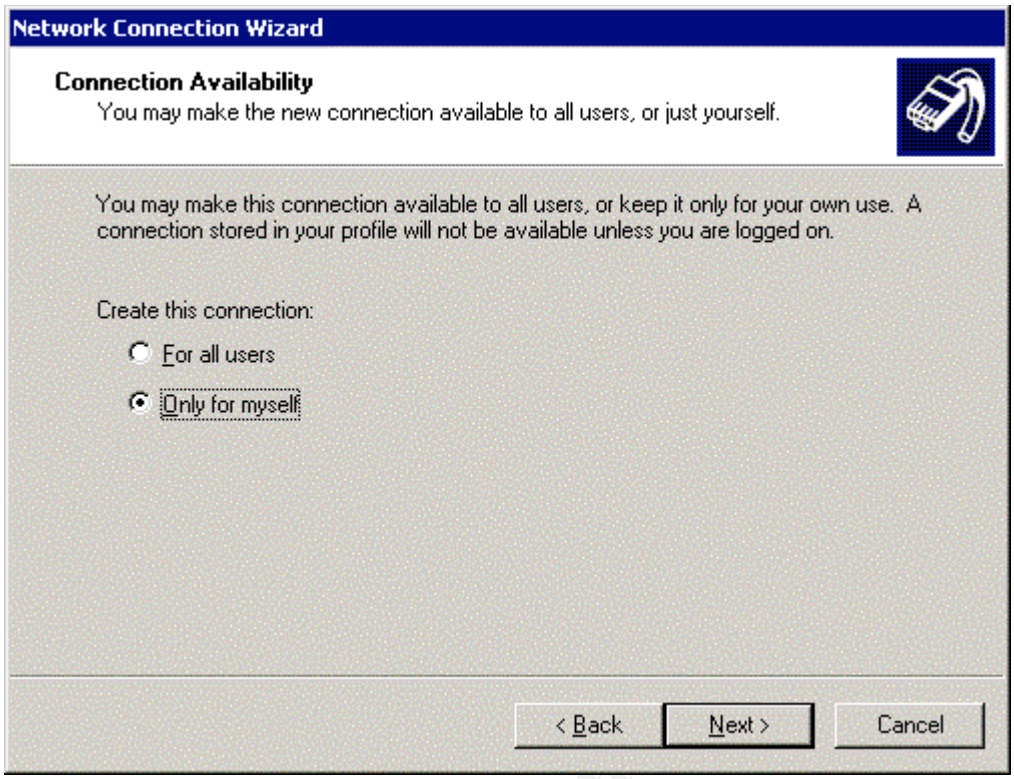
© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Type in the IP address or host name of the server to which you wish to connect. Click Next.



Select Only for Myself to ensure that this connection is only available when the selected user logs into the computer. Click Next.

© SANS Institute 2003,
As part of GIAC practical repository.
Author retains full rights.

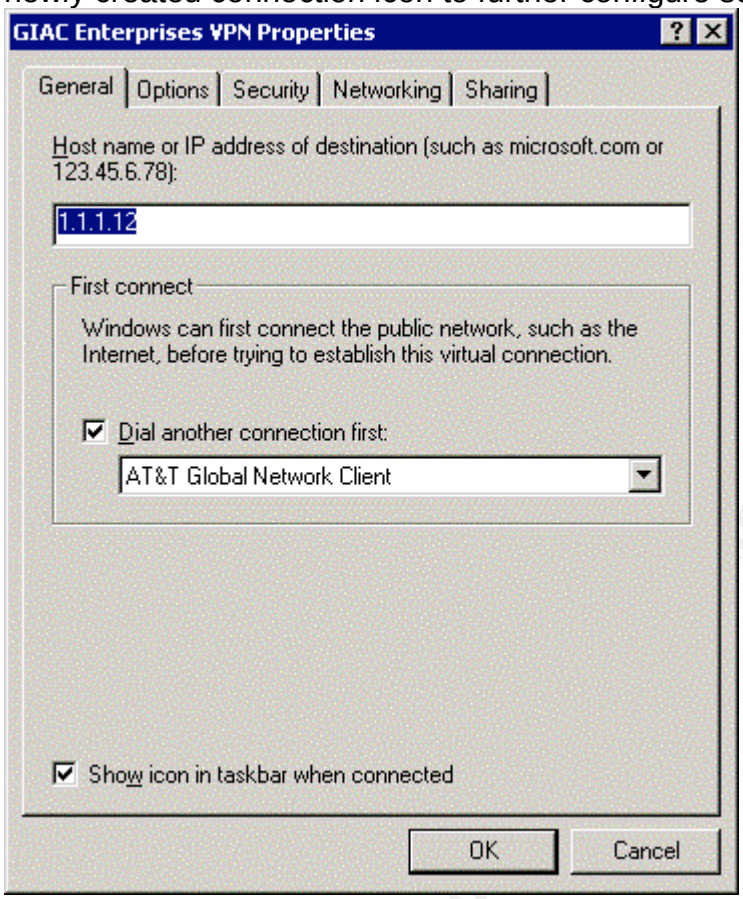


Type a name for the connection and click Finish. You may only do this if you are logged in as part of the Administrators group.

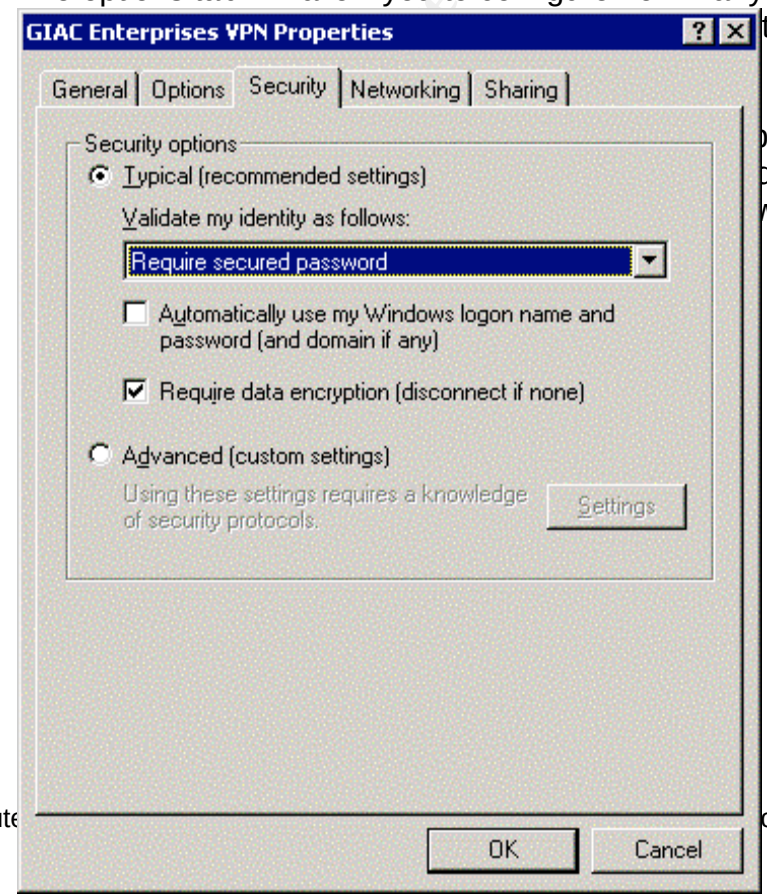


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

From the Network and Dial-Up Connections window you can right click on the newly created connection icon to further configure settings.

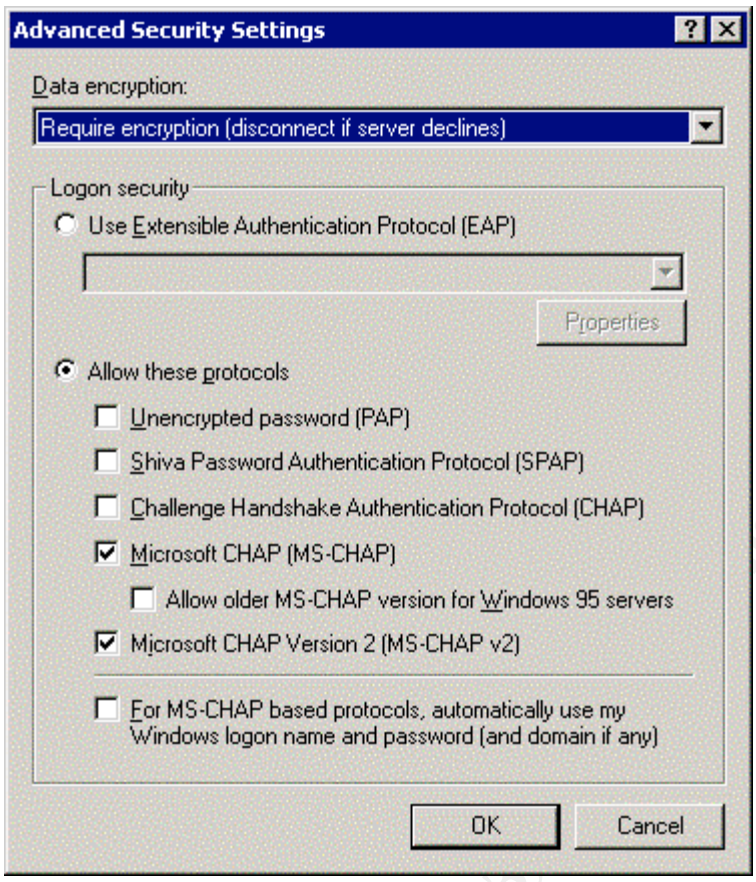


The options tab will allow you to configure how many times the client retries a
tion is dropped as well as
information.



ical security which includes
dvanced settings include
wider range of encryption

© SANS Institute ory. Author retains full rights.



The final two tabs allow you to enable split tunneling (connecting to two separate networks at the same time) and to configure the network settings such as protocol type and IP address. Once the settings are the way you want them click OK. To launch this connection double click on the icon. You will get a prompt for your user id and password and then the connection attempt will begin. The connection status window will let you know if the connection was successful.

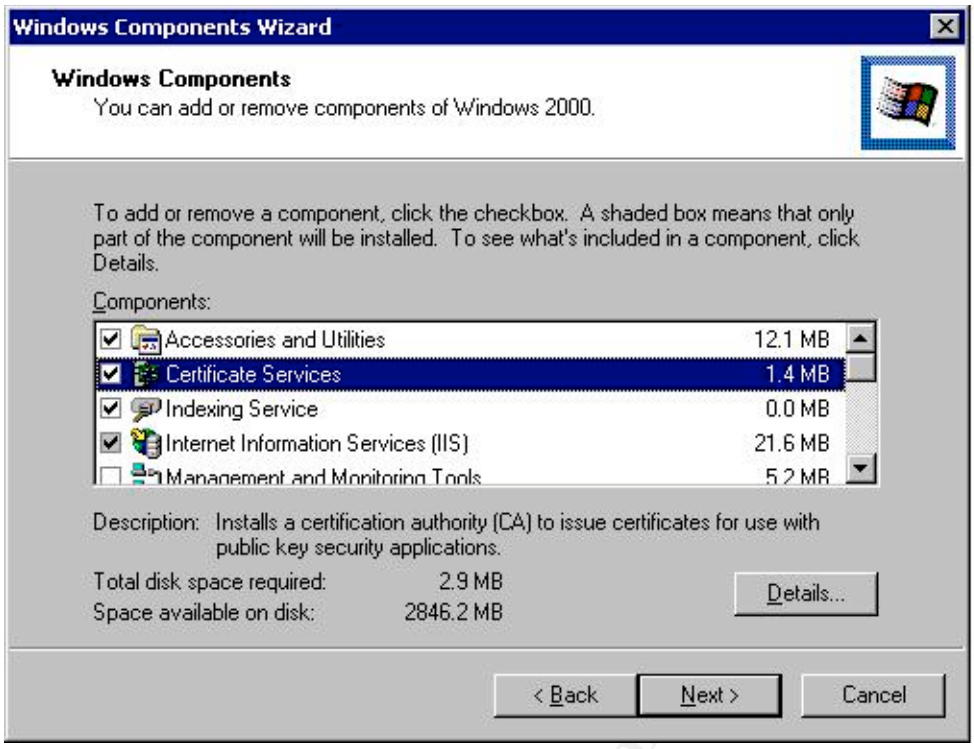
CERTIFICATES

In order for L2TP connections to work both the server and the client must have a certificate that authenticates them as being who they claim to be. The certificates are obtained from a certificate authority which may be in your network or at a trusted site.

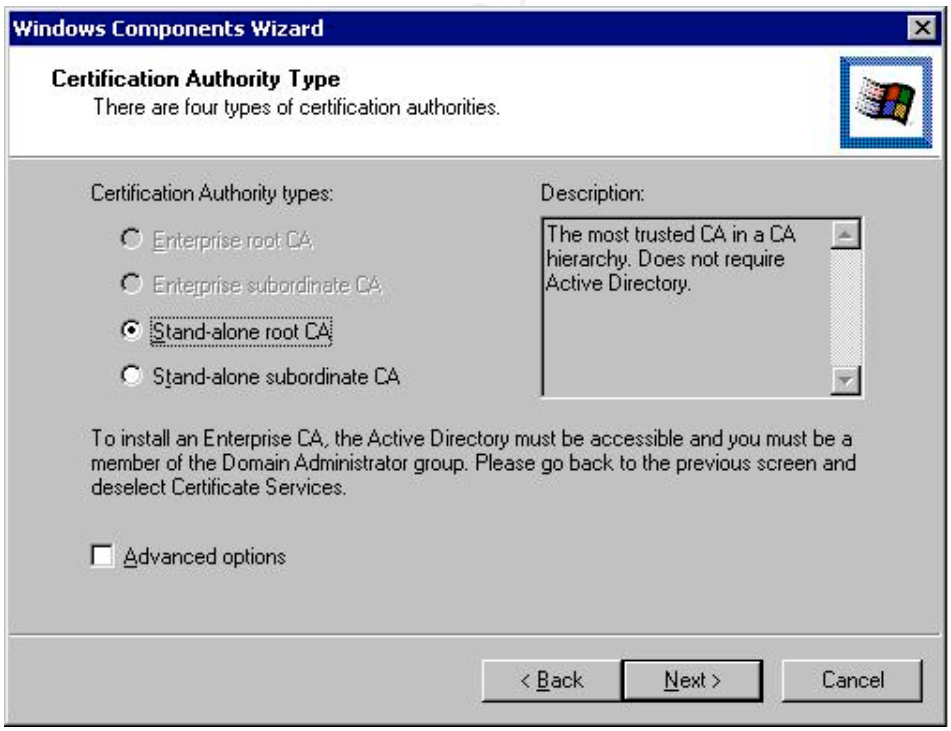
To create a certificate authority in a Windows 2000 environment you must start with a domain controller. Log on as Domain Administrator on the machine you wish to use as the CA. From the Add/Remove Programs menu select Add/Remove Windows Components to get to the Windows Components Wizard.

Select Certificate Services. You will be warned that the server cannot be renamed or removed from or rejoined to the domain after this service is installed. Click Yes. Next.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

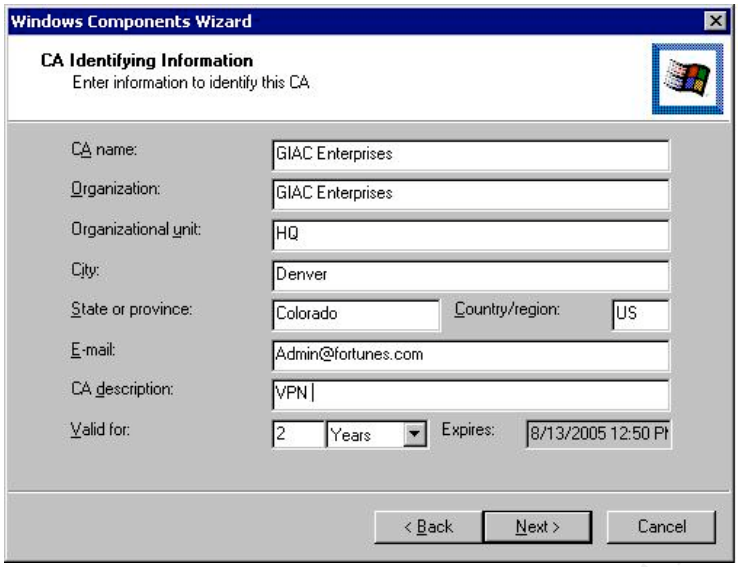


Select Enterprise root CA. You may select the Advanced options to specify encryption, key and hash settings. Next.

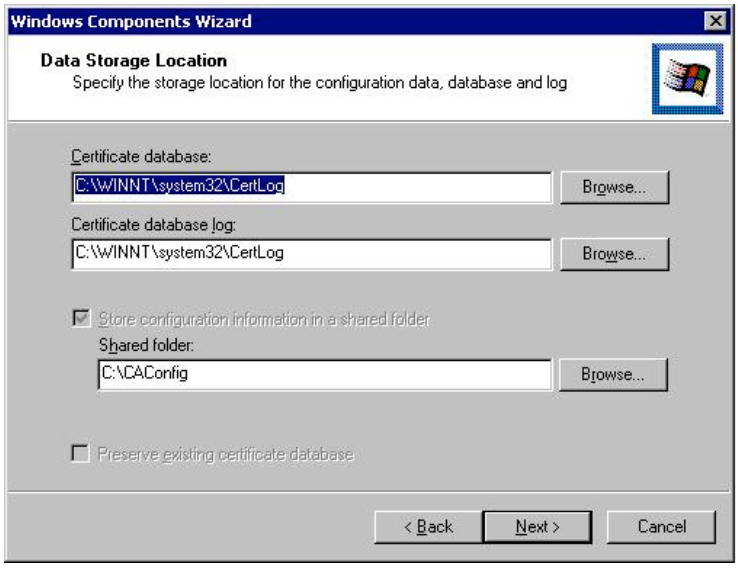


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Input the requested information to identify the server and organization. This cannot be changed. Validity duration is the amount of time the Certificate Authority will be valid before it must be renewed.



The storage location for the database and log and the shared folder are defined in the next window.



You will next be prompted to insert the Windows 2000 Server CD or specify the path for the installation files. Do so and the server will install the necessary files.

Certificates are distributed through a web interface which is enabled when the service is installed. This method of issuing certificates allows clients to initially

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

log into VPN using PPTP and then get their certificate so they can use L2TP. GIAC employees will have the certificates installed before they are issued their laptop.

© SANS Institute 2003, Author retains full rights.

Assignment 3

GIAC Enterprises has requested an audit of its primary firewall to ensure that it is enforcing the policy as expected. This test will focus on the firewall policies and will not be vulnerability assessment of the machines protected by the firewall. This audit will be performed by an outside vendor to ensure that the test is impartial and not tainted by the possibility of internal cover-up.

Plan the Audit

Timing

The general maintenance window for GIAC servers is between 12-6am Mountain Time Sunday mornings. We will perform our audit during this period when no other maintenance is being performed to ensure that all systems are running as they normally do but no other production processes will be active. This timing is designed to minimize the impact on GIAC's normal business operations.

Risks:

While every effort will be made to minimize the impact of the assessment, it is possible that network traffic could be disrupted. This could occur if the firewall reacts unexpectedly to any unusual packets it may receive during the audit. Another danger is that machines on the LAN which are not necessarily part of the audit may receive packets with which they cannot cope and they may hang or crash. With this in mind, GIAC will have technical support personnel on hand to respond to any problems during the test. GIAC executives have been briefed on the risks and have signed a waiver which indemnifies the vendor for any problems which might occur.

Hardware

Attack laptop – a laptop connected to the network through a hub and running Windows 2000 Professional to perform the scans against the firewall. This machine will also be running Windump.

Internal sniffer – a Windows 2000 Server on the DMZ network running Windump to sniff any traffic that gets through the firewall.

Tools

WinDump is a network sniffer that can be used to capture all packets going across the wire. The packets can then be imported into a number of different applications for sorting and filtering.

NmapWin: A Windows port of an open source vulnerability scanning product.

Tests

Both the filtering capabilities and the flow of traffic through the firewall need to be addressed in the audit. The scans will be performed against both ingress and egress filters and will include:

Port scan against the firewall

Connect to resources through open ports

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Cost Estimation:
Setup: 4 hours
Testing: 4 hours
Reporting: 2 hours
$125/hour * 10 hours = $1250.00

Conduct the Audit
Ingress:
Port Scan:
Nmap was used to scan for open ports on the firewall.
The first command used was:
nmap –v –sS –P0 –p 1-65535 –oN GIACAudit 1.1.1.6
-v = verbose. This is the recommended mode as it provides information on what nmap is doing as it is performing the scan. Can be used as –vv for even more information.
-sS = tells Nmap to perform a stealth TCP scan also known as a Syn-Fin scan.
-P0 = do not ping before scanning
-p 1-65535 = the ports that will be scanned
-oN C:\Audit\GIACAudit = write the results to normal output in file GIACAudit
1.1.1.6 = IP address to be scanned

Results:
Interesting ports on (1.1.1.6):
(The 65532 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp
80/tcp	open	http
443/tcp	open	https

Nmap run completed.

This result is what is expected. Port 80 and 443 are for web traffic. Port 25 is for SMTP. Port 53 for DNS did not show up because only UDP is allow on that part and this scan was for TCP ports.

When the IP address of the scanning machine is changed to match that of the VPN server the results are:
Interesting ports on (1.1.1.6):
(The 65526 ports scanned but not shown below are in state: filtered)

Port	State	Service
25/tcp	open	smtp
80/tcp	open	http
135/tcp	open	loc-srv
137/tcp	open	netbios-ns

© SANS Institute 2003, Author retains full rights.

138/tcp open netbios-dgm
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
1433/tcp open ms-sql-s

Nmap run completed.

This shows that in addition to the open ports in the previous scan, the MS networking ports (135, 137-139, 445) and the SQL port 1433 are open to the device at 1.1.1.8.

The next scan is known as an xmas scan. This scan sets the Syn, Urg, Fin and Push flags on TCP packets. The command is:
nmap –v –sX –p 1-65535 –n –oN GIACAudit2 1.1.1.6

Interesting ports on (1.1.1.6):
(The 3 ports scanned but not shown below are in state: closed)

Port	State	Service
1/tcp	open	tcpmux
2/tcp	open	compressnet
3/tcp	open	compressnet
4/tcp	open	unknown
5/tcp	open	rje
6/tcp	open	unknown
7/tcp	open	echo
…		
65525/tcp	open	unknown
65526/tcp	open	unknown
65527/tcp	open	unknown
65528/tcp	open	unknown
65529/tcp	open	unknown
65530/tcp	open	unknown
65531/tcp	open	unknown
65532/tcp	open	unknown
65533/tcp	open	unknown
65534/tcp	open	unknown
65535/tcp	open	unknown

Nmap run completed.

At first glance these results are alarming unless one understands how this scan works in nmap. The scanning tool expects a reset from any ports that are closed. If it does not receive a response, it assumes that the port is open. This is misleading as Iptables, the firewalling technology used in IPCop, is designed to silently drop these packets. We can validate the ability of the firewall to do as we

© SANS Institute 2003, Author retains full rights.

expect by examining the Windump captures on either side of the firewall. A Syn-Fin scan showed the same results.

Verify Port Forwarding:
In order to verify port forwarding is working we put in place a server on the internal network running a telnet server for each of the needed ports. I will attempt to connect to telnet over the ports that should be forwarded on the firewall. I have Windump running on each of the target servers to capture connection traffic.

Port 80

Prior to attempting to connect the firewall sends out a broadcast request for the target server to identify itself by MAC address so the firewall can forward the traffic to the correct machine:
06:25:52.065631 arp who-has 10.10.15.10 tell 10.10.15.2

The server with the corresponding IP supplies the requested information:
06:25:52.065676 arp reply 10.10.15.10 is-at 0:10:4b:cb:31:4f

This request for MAC address usually happens prior to any forwarding by the firewall. It is possible that the information is cached in the firewall's routing table. For the purpose of this report we will not include this part of the exchange for every test.

The three-way TCP handshake is successful:
06:25:47.067640 IP 1.1.1.7.1338 > win2kserver.80: S 965404040:965404040(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
06:25:47.067779 IP win2kserver.80 > 1.1.1.7.1338: S 3757451565:3757451565(0) ack 965404041 win 17520 <mss 1460,nop,nop,sackOK> (DF)
06:25:47.068150 IP 1.1.1.7.1338 > win2kserver.80: . ack 1 win 65535 (DF)

Data begins moving:
06:26:18.599261 IP 1.1.1.7.1338 > win2kserver.80: P 1:3(2) ack 1 win 65535 (DF)
06:26:18.785552 IP win2kserver.80 > 1.1.1.7.1338: . ack 3 win 17518 (DF)
06:26:18.901140 IP 1.1.1.7.1338 > win2kserver.80: P 3:5(2) ack 1 win 65535 (DF)
06:26:18.946251 IP win2kserver.80 > 1.1.1.7.1338: P 1:138(137) ack 5 win 17516 (DF)

Session is gracefully terminated:
06:26:18.946477 IP win2kserver.80 > 1.1.1.7.1338: F 138:138(0) ack 5 win 17516 (DF)
06:26:18.946822 IP 1.1.1.7.1338 > win2kserver.80: . ack 139 win 65398 (DF)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

06:26:20.051338 IP 1.1.1.7.1338 > win2kserver.80: F 5:5(0) ack 139 win 65398 (DF)
06:26:20.051440 IP win2kserver.80 > 1.1.1.7.1338: . ack 6 win 17516 (DF)

From the client side the traffic looks similar except that the IP address of the server is changed to the IP address of the firewall:
06:49:20.675975 IP win2kpro.1344 > 1.1.1.6.80: S 1200660431:1200660431(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
06:49:20.676367 IP 1.1.1.6.80 > win2kpro.1344: S 722181103:722181103(0) ack 1200660432 win 5840 <mss 1460> (DF)
06:49:20.676425 IP win2kpro.1344 > 1.1.1.6.80: . ack 1 win 17520 (DF)
Port forwarding is working correctly for HTTP.

Port 443
Three way handshake:
06:29:01.015459 IP 1.1.1.7.1340 > win2kserver.443: S 1013940240:1013940240(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
06:29:01.015607 IP win2kserver.443 > 1.1.1.7.1340: S 3805935827:3805935827(0) ack 1013940241 win 17520 <mss 1460,nop,nop,sackOK> (DF)
06:29:01.015959 IP 1.1.1.7.1340 > win2kserver.443: . ack 1 win 65535 (DF)

Traffic flow:
06:29:01.088253 IP win2kserver.443 > 1.1.1.7.1340: P 1:19(18) ack 1 win 17520 (DF)
06:29:01.088895 IP 1.1.1.7.1340 > win2kserver.443: P 1:4(3) ack 19 win 65517 (DF)
06:29:01.089189 IP win2kserver.443 > 1.1.1.7.1340: P 19:27(8) ack 4 win 17517 (DF)

Client:
06:54:19.334219 IP win2kpro.1352 > 1.1.1.6.443: S 1275348564:1275348564(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
06:54:19.334909 IP 1.1.1.6.443 > win2kpro.1352: S 4067777640:4067777640(0) ack 1275348565 win 17520 <mss 1460,nop,nop,sackOK> (DF)
06:54:19.334976 IP win2kpro.1352 > 1.1.1.6.443: . ack 1 win 17520 (DF)
06:54:19.336428 IP win2kpro.1352 > 1.1.1.6.443: P 1:251(250) ack 1 win 17520 (DF)
06:54:19.452479 IP 1.1.1.6.443 > win2kpro.1352: . ack 251 win 17270 (DF)
06:54:19.455632 IP 1.1.1.6.443 > win2kpro.1352: F 1:1(0) ack 251 win 17270 (DF)
06:54:19.455695 IP win2kpro.1352 > 1.1.1.6.443: . ack 2 win 17520 (DF)
06:54:19.455959 IP win2kpro.1352 > 1.1.1.6.443: F 251:251(0) ack 2 win 17520 (DF)

Port forwarding is working correctly for HTTPS.

© SANS Institute 2003, Author retains full rights.

Port 25
Initial contact and handshake:
06:32:13.122303 IP 1.1.1.7.1341 > win2kserver.25: S
1061933778:1061933778(0) win 65535 <mss 1460,nop,nop,sackOK> (DF)
06:32:13.122457 IP win2kserver.25 > 1.1.1.7.1341: S
3853970409:3853970409(0) ack 1061933779 win 17520 <mss
1460,nop,nop,sackOK> (DF)
06:32:13.122831 IP 1.1.1.7.1341 > win2kserver.25: . ack 1 win 65535 (DF)

Traffic begins flowing between the test box on the outside network 1.1.1.1 to the test machine on the inside network 10.10.15.13 over port 25. :
06:32:13.123221 IP win2kserver.25 > 1.1.1.7.1341: P 1:114(113) ack 1 win
17520 (DF)
06:32:13.229506 IP 1.1.1.7.1341 > win2kserver.25: . ack 114 win 65422 (DF)

Client trace:
06:56:05.593465 IP win2kpro.1353 > 1.1.1.6.25: S 1301923359:1301923359(0)
win 16384 <mss 1460,nop,nop,sackOK> (DF)
06:56:05.594031 IP 1.1.1.6.25 > win2kpro.1353: S 4094340749:4094340749(0)
ack 1301923360 win 17520 <mss 1460,nop,nop,sackOK> (DF)
06:56:05.594093 IP win2kpro.1353 > 1.1.1.6.25: . ack 1 win 17520 (DF)
06:56:05.594895 IP 1.1.1.6.25 > win2kpro.1353: P 1:114(113) ack 1 win 17520
(DF)
06:56:05.743106 IP win2kpro.1353 > 1.1.1.6.25: . ack 114 win 17407 (DF)

Port forwarding is working correctly for SMTP.

Egress:
For examining egress filtering we will put our target server on the red interface of the firewall and our attack box on the green interface.

Accessibility to the Internet:
port 80
06:43:33.541044 IP 1.1.1.6.1024 > 192.168.15.13.80: S
846786094:846786094(0) win 5840 <mss 1460> (DF)
06:43:33.541165 IP 192.168.15.13.80 > 1.1.1.6.1024: S
4024373114:4024373114(0) ack 846786095 win 17520 <mss 1460> (DF)
06:43:33.541325 IP 1.1.1.6.1024 > 192.168.15.13.80: . ack 1 win 5840 (DF)
06:43:33.541763 IP 1.1.1.6.1024 > 192.168.15.13.80: P 1:348(347) ack 1 win
5840(DF)
06:43:33.547237 IP 192.168.15.13.80 > 1.1.1.6.1024: P 1:19(18) ack 348 win
17173 (DF)
06:43:33.547396 IP 1.1.1.6.1024 > 192.168.15.13.80: . ack 19 win 5840 (DF)

port 443

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

06:46:27.200359 IP 1.1.1.6.1352 > 192.168.15.13.443: S
1275348564:1275348564(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
06:46:27.200509 IP 192.168.15.13.443 > 1.1.1.6.1352: S
4067777640:4067777640(0) ack 1275348565 win 17520 <mss
1460,nop,nop,sackOK> (DF)
06:46:27.200931 IP 1.1.1.6.1352 > 192.168.15.13.443: . ack 1 win 17520 (DF)
06:46:27.202614 IP 1.1.1.6.1352 > 192.168.15.13.443: P 1:251(250) ack 1 win
17520 (DF)
06:46:27.318084 IP 192.168.15.13.443 > 1.1.1.6.1352: . ack 251 win 17270 (DF)
06:46:27.321268 IP 192.168.15.13.443 > 1.1.1.6.1352: F 1:1(0) ack 251 win
17270(DF)
06:46:27.321656 IP 1.1.1.6.1352 > 192.168.15.13.443: . ack 2 win 17520 (DF)
06:46:27.321918 IP 1.1.1.6.1352 > 192.168.15.13.443: F 251:251(0) ack 2 win
17520 (DF)
06:46:27.321999 IP 192.168.15.13.443 > 1.1.1.6.1352: . ack 252 win 17270 (DF)
06:46:32.198866 arp who-has 192.168.15.13 tell 1.1.1.6
06:46:32.198913 arp reply 192.168.15.13 is-at 0:10:4b:cb:31:4f

port 25
06:46:32.198866 arp who-has 192.168.15.13 tell 1.1.1.6
06:46:32.198913 arp reply 192.168.15.13 is-at 0:10:4b:cb:31:4f
06:48:13.459124 IP 1.1.1.6.1353 > 192.168.15.13.25: S
1301923359:1301923359(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
06:48:13.459271 IP 192.168.15.13.25 > 1.1.1.6.1353: S
4094340749:4094340749(0) ack 1301923360 win 17520 <mss
1460,nop,nop,sackOK> (DF)
06:48:13.459666 IP 1.1.1.6.1353 > 192.168.15.13.25: . ack 1 win 17520 (DF)
06:48:13.460041 IP 192.168.15.13.25 > 1.1.1.6.1353: P 1:114(113) ack 1 win
17520 (DF)
06:48:13.608701 IP 1.1.1.6.1353 > 192.168.15.13.25: . ack 114 win 17407 (DF)
06:48:18.449867 arp who-has 192.168.15.13 tell 1.1.1.6
06:48:18.449916 arp reply 192.168.15.13 is-at 0:10:4b:cb:31:4f

Outbound Filters:
First we start with the Syn Scan:
nmap (V. 3.00) scan initiated Wed Oct 15 11:01:23 2003 as: nmap -v -sS -p 1-
65535 -n -oN GIACAuditout.txt 192.168.15.13
Interesting ports on (192.168.15.13):
(The 65503 ports scanned but not shown below are in state: closed)

Port	State	Service
7/tcp	open	echo
9/tcp	open	discard
13/tcp	open	daytime
17/tcp	open	qotd
19/tcp	open	chargen
25/tcp	open	smtp

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

42/tcp open nameserver
47/tcp open ni-ftp
50/tcp open re-mail-ck
53/tcp open domain
80/tcp open http
135/tcp open loc-srv
137/tcp open netbios-ns
138/tcp open netbios-dgm
139/tcp open netbios-ssn
443/tcp open https
445/tcp open microsoft-ds
500/tcp open isakmp
637/tcp open lanserver
1002/tcp open unknown
1025/tcp open NFS-or-IIS
1029/tcp open ms-lsa
1032/tcp open iad3
1034/tcp open unknown
1035/tcp open unknown
1036/tcp open unknown
1039/tcp open unknown
1433/tcp open ms-sql-s
1720/tcp filtered H.323/Q.931
1723/tcp open pptp
3037/tcp open unknown
3372/tcp open msdtc

Nmap run completed at Wed Oct 15 11:01:41 2003 -- 1 IP address (1 host up) scanned in 18 seconds
There are a large number of ports identified as open. This is expected as IPCop does not filter egress traffic by default. Many of these are standard services and are identified by the scan. 1034 is ActiveSync. 1035 is mxxrlogin. 1036 is Nebula Secure Segment Transfer Protocol. 3037 is HP SAN management. 1002 and 1039 are currently unassigned. The services identified by the port scan do not necessarily reflect the type of traffic that is flowing over these ports. The scanner matches open ports against its database based on IANA port number assignments. It is possible to alter the standard port on which a service is running.

An Xmas and Fin scan are next:
nmap (V. 3.00) scan initiated Thu Oct 16 14:08:48 2003 as: nmap -v -sX -p 1-65535 -n -oN GIACauditout.txt 192.168.15.13
Interesting ports on (192.168.15.13):
(The 65533 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http

© SANS Institute 2003, Author retains full rights.

1720/tcp open H.323/Q.931

Nmap run completed at Thu Oct 16 14:09:07 2003 -- 1 IP address (1 host up) scanned in 19 seconds

nmap (V. 3.00) scan initiated Thu Oct 16 14:10:52 2003 as: nmap -v -sF -p 1-65535 -n -oN GIACauditout.txt 192.168.15.13
Interesting ports on (192.168.15.13):
(The 65533 ports scanned but not shown below are in state: closed)
Port State Service
80/tcp open http
1720/tcp open H.323/Q.931

Nmap run completed at Thu Oct 16 14:11:10 2003 -- 1 IP address (1 host up) scanned in 18 seconds

The ports that were found open were ports 80 and 1720. Port 80 is http. Port 1720 is used for H323 to locate hosts for setting up web conferencing.

Evaluate the Audit

This audit is in no way meant to test the security or reliability of service or machines on the network. The audit focused solely on the policies on the primary firewall. Ingress filtering is working as it should. It is possible to stealth the firewall so that it shows all ports as closed in Xmas and Fin scans. This could be useful in confusing attackers by returning invalid reconnaissance data. While not as critical as blocking inbound traffic, egress filtering should to be tuned to eliminate unnecessary ports. This can be done by manually manipulating the rule chains as it was done on the internal firewall. A careful examination of all traffic is necessary before any egress rules are written to ensure that no legitimate business traffic is interrupted.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Assignment 4

This section will identify how a remote system can be attacked. The system I have chosen is from Richard Franken's (GCFW Analyst 408) GCFW practical. This paper can be found at http://www.giac.org/practical/GCFW/Richard_Franken_GCFW.pdf. There will be three parts to the attack. First I will attack the firewall itself. Then I will attempt to perform a Denial of Service attack. Finally, I will show how one could penetrate the perimeter and compromise an internal system. Note for the purpose of this paper we will use the IP addresses used in Mr. Franken's paper with the understanding that these are not addresses that would be used for legitimate traffic on the Internet. Mr. Franken's network diagram is below.

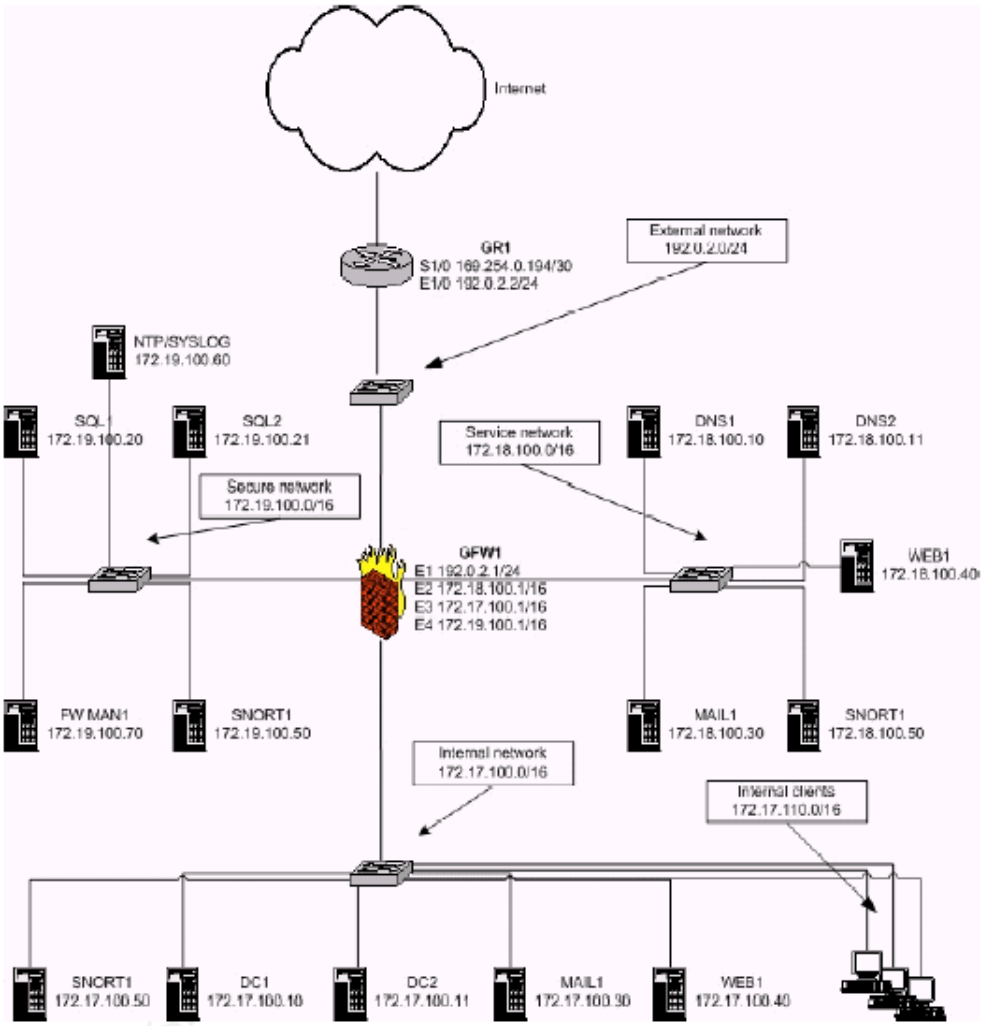


Figure 1

Before attempting any attack against the target some reconnaissance is in order. Nmap could be used here to try to ascertain the network architecture. In order not to arouse suspicion I would be careful to time my scans to be slow and infrequent. This means it will take much longer to do reconnaissance but there is

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

less of a chance of arousing suspicion and getting caught once the actual exploit is launched. While I am running the Nmap scan I will collect any responses using Windump. I can later analyze this file to determine OS of the responding machines.

Our final information gathering technique is to scour bulletin boards and newsgroups for any postings from the GIAC Enterprises domain. I may be able to find an employee name, email address and possibly username. I can use this information for social engineering by contacting the employee and trying to gain confidential information from them. I can also infer the naming schema used for userids and translate that into the userid for the president or other executives of the company.

Once my reconnaissance is over and I have analyzed the data I am ready to attack.

1) Attack the Firewall

Mr. Franken is running Checkpoint FW-1 NG FP3. There are few vulnerabilities in this product however he is running it on a Windows 2000 Server. I will attempt to gain control of or at least disrupt the Windows machine long enough to sneak my malicious traffic through.

For this attack I will use a very high profile Windows vulnerability, the RPC DCOM Interface Buffer Overflow. This vulnerability is an overflow in the Windows Remote Procedure Call interface to DCOM. The RPC protocol is used by Windows systems to communicate over the network. DCOM was incorporated into RPC to increase functionality. This protocol is accessible by default over port 135 however Microsoft has admitted to vulnerabilities over ports 139 and 445 also. It has been theorized that an exploit may work over ports 80 or 593.

A buffer overflow is caused when the application code was written not to check how many characters are being input into a particular variable. The result is the extra characters overwrite the adjoining memory. This can cause the machine to crash or for code that was sent in the input to be executed with the same privilege as the overflowed task. In the RPC DCOM buffer overflow arbitrary code can be executed but this can cause RPC services to crash unless the exploit code is written to send an exit thread to the target machine.

The exploit I am going to use is from OC192 Research Labs. The exploit is called dcom.c.
The command to run the exploit is
dcomexploit.exe <target> <ipaddress>

Target can be:
0 – Windows 2000 SP0 (english)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

1– Windows 2000 SP1 (english)
2 – Windows 2000 SP2 (english)
3 – Windows 2000 SP3 (english)
4 – Windows 2000 SP4 (english)
5 – Windows XP SP0 (english)
6 – Windows XP SP1 (english)

Since I believe my target is running SP 3 I will try that first.

dcomexploit.exe 3 192.0.2.1

If the above command did not work I would try:
dcomexploit.exe 4 192.0.2.1

If the exploit was successful I could connect to port 4444 on the firewall. Netcat is a versatile tool that would allow me to send a wide variety of instructions to the compromised box. If I did not succeed in compromising the firewall I may remove the exit thread and attempt to cause a denial of service on the machine which might allow me to sneak malicious traffic into the network while the firewall is rebooting.

This attack would most likely not work on Mr. Franken's system as he has hardened the OS and does not allow unneeded services to cross into his network.

2) DOS attack
I have gained control of 50 high speed home users' machines and will use a distributed denial of service tool to attempt to disallow service to any legitimate user attempting to use the target network. During this attack I (master) will instruct my compromised hosts (agents) to send a stream of packets to the victim. Each attacker by themselves could do nothing more than cause an annoyance and maybe some wasted analyst time but by coordinating the attack of all 50 machines the combined amount of data overwhelms the victim's network using up bandwidth and causing some devices to crash.

The tool I will use is TFN2K by Mixter. This tool can be used to perform TCP/SYN, UDP, ICMP ping and broadcast ping attacks. It can also instruct its agents to alternate between the four different attack types. It is difficult to trace back to a TFN2K master because all traffic between the master and agents is encrypted and the IP address of the master can be spoofed. These two features will give me greater odds at not being caught.

There are two different phases to this attack. The first is the communications phase where I will send a command to my agents. This command will tell them who to attack and what kind of traffic to send. In order to make myself harder to trace I will randomize the protocol I use to send commands to the agents. This

© SANS Institute 2003, Author retains full rights.

setting will alternate between TCP, UDP and ICMP. I will also intersperse my command packets with packets sent to random addresses to further confuse anyone who might try to trace me.

By design I don't expect any response from my agents. Instead I will send each command 20 times and monitor my victim's web sites for signs that the denial of service is working.

The second phase is the flooding phase. This is where the compromised hosts begin to send traffic to the victim. My agents will send a combination of TCP, UDP and ICMP packets to the target network. It is unlikely that with only 50 machines I can actually cause a denial of service against a properly configured and relatively secure network but I could cause a noticeable degradation in performance and cause a great deal of anguish to the network administrators at the target site.

There are several steps my victim can take to protect his network from this attack including locking down the firewall and border router, using an IDS to identify and react to the attack, and using a number of tools designed to scan for TFN2K agents.

The first recommendation, locking down the firewall, is a good first step toward protecting yourself from any type of attack. To lock down the firewall ensure that any unnecessary services are stopped and unneeded ports blocked. Also make sure protocols that are not essential to the business are not allowed into the network. The border router can be configured to rate limit SYN packets (see http://www.cisco.com/warp/public/707/newsflash.html). This can cause legitimate traffic to be dropped so careful testing is recommended to determine the best setting for this parameter for a particular network.

Using an intrusion detection system to identify and react to the attack is another option. The easiest way to identify TFN2K is the string of A's in the packet. A signature can be developed to identify these packets. The IDS can then alert the appropriate parties who can respond in whatever manner is prescribed by the victim's incident response procedures. A more dangerous method is to allow the IDS to make changes on the firewall to block the IP addresses that are identified as the source of the attack. This technique must be used with extreme caution as a false positive or an attack spoofing an important client or partner's address range could result in a self inflicted DOS.

Finally you could try to use a tool to gain control of the attacking agents and instruct them to stop. Tfn2kpass will reveal the password set when the binary was built. This password can be used to instruct the attacking machines to stop the attack but the tool only works if you have local access to the machine. Other tools such as find_ddos and RID work by locating the agents so the machines on which they reside can be cleaned.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3) Compromising an internal system

For this attack I will go after the email systems. During my reconnaissance I found a recent posting on a golfing bulletin board from an executive at the target company. This posting was made from the office and I have what I believe to be a valid email account.

Mr. Franken is using a highly secured Windows 2000 server running Mail Sweeper 4.3. On May 13, 2003 a vulnerability in the way Mail Sweeper handles filenames for attachments was announced (bugtraq id 7568). I hope to use this flaw to bypass mail filtering and get to the internal email server.

The vulnerability works by creating a file with multiple extensions filled with white space. I will use this to drop a back door called insider.exe onto the executive's machine.

```
Return-Path: bad_guy@attack.com
From: User A <bad_guy@attack.com>
To: User B <Big_wig@GIAC.com>
Subject: Fw: FYI
Date: Mon, 11 Aug 2003 13:38:19 -0000
MIME-Version: 1.0
X-Mailer: Internet Mail Service (5.5.23)
Content-Type: multipart/mixed ;
boundary="----_=_NextPart_000_02D35B68.BA121FA3"
Status: RO

This message is in MIME format. Since your mail reader does not
understand
this format, some or all of this message may not be legible.

- ------_=_NextPart_000_02D35B68.BA121FA3
Content-Type: text/plain; charset="iso-8859-1"

Hi,

Thought you might enjoy this!

Cheers,

Bad Guy



- ------_=_NextPart_000_02D35B68.BA121FA3
Content-Type: text/plain;
      name="really    long   file    name   .doc   .vbs"
Content-Disposition: attachment;
      filename=" really    long   file    name   .doc   .vbs"

`Back door installer
```

© SANS Institute 2003, Author retains full rights.

'Send me all your data.

- ------_=_NextPart_000_02D35B68.BA121FA3

When the executive opens his email the Trojan will be installed onto his computer. The insider program will establish a connection back a specially prepared server running a cgi program over HTTP port 80. The client is identified via a 32-character id that is used for all communication. User, logon domain, location, operating system and connection type are all sent back to the server automatically. From there I can program my server to send commands to the client to do anything I want. I can also set the compromised host to check back in with the server randomly for more instructions. From this foothold I may be able to compromise other machines on the internal network. I can also search for information on the company and other users who may have sensitive information I can use or sell. All communication is carried out via HTTP Post commands, which should sneak past firewalls and proxy servers.

It is unknown whether this attack would work. There is a patch for this vulnerability but it is uncertain if the victim's network administrators have had a chance to apply it. It also relies on the exec's email address being valid and that he would open the email. Certain AV software may be able to detect the presence of our Trojan and user awareness training would encourage users not to open emails if they do not recognize the sender. I could increase the odds of my attack working by sending it to several different people in the company.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References:

General:
team-cymru. The Bogon Reference Page.
http://www.cymru.com/Bogons/index.html

http://www.iana.org/

Brenton, Chris. et al. Track 2 – TCP/IP. SANS Institute. 2003.
Brenton, Chris. et al. Track 2 – Packet Filters. SANS Institute. 2003.
Brenton, Chris. et al. Track 2 – Firewalls. SANS Institute. 2003.
Brenton, Chris. et al. Track 2 – Defense in Depth. SANS Institute. 2003.
Brenton, Chris. et al. Track 2 – VPNS. SANS Institute. 2003.
Brenton, Chris. et al. Track 2 – Network Design and Assessment. SANS Institute. 2003.

Cisco Router:
http://www.cisco.com

Wright, Joshua L. and Stewart, John N. Securing Cisco Routers: Step by Step. SANS Publishing. 2002.

Firewall
Deker, Peter; Moller, J.S., et. al. posts to IPCop and Web Proxy Bulletin Board. September 2003.http://secureit-now.net/ipcsupport/modules.php?op=modload&name=forums&file=viewtopic&t=792&highlight=rules&sid=b3b4520c173c4ba4163e624ee2d35d6a
Hatch, Brian. Egress Filtering for a Healthier Internet. February, 2003.
http://www.hackinglinuxexposed.com/articles/20030213.html
http://www.ipcop.org
Lowth, Chris. post to comp.security.firewalls newsgroup. June 2003.
http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2003-06/1437.html
Stephens, James C. Iptables. September 5, 2003.
http://www.sns.ias.edu/~jns/security/iptables/

VPN:
HOW TO: Install and Configure a Virtual Private Network Server in Windows 2000. June 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;308208

The Cable Guy. August 2001. Layer Two Tunneling Protocol in Windows.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0801.asp

Virtual Private Networking with Windows 2000: Deploying Remote Access VPNs. August 2002.
http://www.microsoft.com/windows2000/techinfo/planning/incremental/vpndeploy.asp

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

National Security Agency Security Recommendation Guide. March 2003
http://nsa1.www.conxion.com/win2k/download.htm

Machine certificates for L2TP over IPSec VPN connections. Windows 2000 Server Documentation. February 2000.
http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_VPN_us26.htm

Step by Step Guide to Setting up a Certification Authority. February 16, 2000.
http://www.microsoft.com/windows2000/techinfo/planning/security/casetupsteps.asp

Exploits:
Franken, Richard. GCFW Practical Assignment. March 2003.
http://www.giac.org/practical/GCFW/Richard_Franken_GCFW.pdf

Mixter. Tribe Flood Network 3000.
http://packetstorm.linuxsecurity.com/distributed/tfn3k.txt

Barlow, Jason and Thrower, Woody. TFN2K – An Analysis. Revision 1.1. February 10, 2000.
http://packetstorm.linuxsecurity.com/distributed/TFN2k_Analysis.htm

Strategies to Protect Against Distributed Denial of Service Attacks. April 29, 2003.
http://www.cisco.com/warp/public/707/newsflash.html

Simple Nomad. Tfn2k.
http://razor.bindview.com/tools/desc/tfn2k_readme.html

The FreeBSD Ports Collection: security rid 1.0.
http://www.gufi.org/~gmarco/pepo/pkg.pl?file=Makefile&dirname=security%2Frid

ReadMe for MAILsweeper for SMTP Version 4.3.8. Revision 1.1. April 2003.
http://www.clearswift.com/download/bin/Patches/ReadMe_SMTP_438.htm

O'Neal, Martin. Corsaire Security Advisory – Clearswift MAILsweeper MIME attachment evasion issue. March 7, 2003.
http://cert.uni-stuttgart.de/archive/bugtraq/2003/03/msg00142.html

Rogers, Paul. RE: E-Mail Content Filtering Systems. July 20, 2001.
http://cert.uni-stuttgart.de/archive/vuln-dev/2001/07/msg00093.html

Internet Security Systems Security Alert. Flaw in Microsoft Windows RPC Implementation. July 16, 2003.

© SANS Institute 2003, Author retains full rights.

http://xforce.iss.net/xforce/alerts/id/147

Nmap
Network Reconnaissance Techniques.
http://www.insecure.org/nmap/OSDEM_Presentation/

Browser:
The Network Applications Team of the Systems and Network Attack Center. Guide to Securing Netscape 7.02. April 2003.
http://www.nsa.gov/snac/support/guides/sd-10.pdf

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

APPENDIX
IPCop rc.firewall file

```
#!/bin/sh

. /var/ipcop/ppp/settings
. /var/ipcop/ethernet/settings
IFACE=`/bin/cat /var/ipcop/red/iface | /usr/bin/tr -d '\012'`

iptables_init() {
      echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
      echo 0 > /proc/sys/net/ipv4/conf/all/accept_redirects
      echo 0 > /proc/sys/net/ipv4/conf/all/accept_source_route
      echo 1 > /proc/sys/net/ipv4/conf/all/log_martians

      # Reduce DoS'ing ability by reducing timeouts
      echo   30 > /proc/sys/net/ipv4/tcp_fin_timeout
      echo    0 > /proc/sys/net/ipv4/tcp_window_scaling
      echo    0 > /proc/sys/net/ipv4/tcp_timestamps
      echo    0 > /proc/sys/net/ipv4/tcp_sack
      echo 1024 > /proc/sys/net/ipv4/tcp_max_syn_backlog

      # Flush all rules and delete all custom chains
      /sbin/iptables -F
      /sbin/iptables -t nat -F
      /sbin/iptables -X
      /sbin/iptables -t nat -X

      # Set up policies
      /sbin/iptables -P INPUT DROP
      /sbin/iptables -P FORWARD DROP
      /sbin/iptables -P OUTPUT ACCEPT

      # This chain will log, then DROPs "Xmas" and Null packets which
might
      # indicate a port-scan attempt
      /sbin/iptables -N PSCAN
      /sbin/iptables -A PSCAN -p tcp  -m limit --limit 10/minute -j LOG
--log-prefix "TCP Scan? "
      /sbin/iptables -A PSCAN -p udp  -m limit --limit 10/minute -j LOG
--log-prefix "UDP Scan? "
      /sbin/iptables -A PSCAN -p icmp -m limit --limit 10/minute -j LOG
--log-prefix "ICMP Scan? "
      /sbin/iptables -A PSCAN -f      -m limit --limit 10/minute -j LOG
--log-prefix "FRAG Scan? "
      /sbin/iptables -A PSCAN -j DROP

      # Disallow packets frequently used by port-scanners, XMas and
Null
      /sbin/iptables -A INPUT   -p tcp --tcp-flags ALL ALL  -j PSCAN
      /sbin/iptables -A FORWARD -p tcp --tcp-flags ALL ALL  -j PSCAN
      /sbin/iptables -A INPUT   -p tcp --tcp-flags ALL NONE -j PSCAN
      /sbin/iptables -A FORWARD -p tcp --tcp-flags ALL NONE -j PSCAN
}

iptables_red() {
```

© SANS Institute 2003, Author retains full rights.

```
	/sbin/iptables -F RED
	/sbin/iptables -t nat -F RED

	# PPPoE / PPTP Device
	if [ "$IFACE" != "" ]; then
		# PPPoE / PPTP
		if [ "$DEVICE" != "" ]; then
			/sbin/iptables -A RED -i $DEVICE -j ACCEPT
		fi
		if [ "$RED_TYPE" = "PPTP" -o "$RED_TYPE" = "PPPOE" ]; then
			if [ "$RED_DEV" != "" ]; then
				/sbin/iptables -A RED -i $RED_DEV -j ACCEPT
			fi
		fi
	fi

	if [ "$IFACE" != "" -a -f /var/ipcop/red/active ]; then
		# DHCP
		if [ "$RED_DEV" != "" -a "$RED_TYPE" = "DHCP" ]; then
			/sbin/iptables -A RED -p tcp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
			/sbin/iptables -A RED -p udp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
		fi
		if [ "$PROTOCOL" = "RFC1483" -a "$METHOD" = "DHCP" ]; then
			/sbin/iptables -A RED -p tcp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
			/sbin/iptables -A RED -p udp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
		fi

		# Allow IPSec
		/sbin/iptables -A RED -p 47  -i $IFACE -j ACCEPT
		/sbin/iptables -A RED -p 50  -i $IFACE -j ACCEPT
		/sbin/iptables -A RED -p 51  -i $IFACE -j ACCEPT
		/sbin/iptables -A RED -p udp -i $IFACE --sport 500 --dport
500 -j ACCEPT

		# Outgoing masquerading
		/sbin/iptables -t nat -A RED -o $IFACE -j MASQUERADE
	fi
}

# See how we were called.
case "$1" in
  start)
	iptables_init

	# Limit Packets- helps reduce dos/syn attacks
	/sbin/iptables -A INPUT -p tcp -m tcp --tcp-flags SYN,RST,ACK SYN
-m limit --limit 10/sec

	# CUSTOM chains, can be used by the users themselves
	/sbin/iptables -N CUSTOMINPUT
	/sbin/iptables -A INPUT -j CUSTOMINPUT
	/sbin/iptables -N CUSTOMFORWARD
	/sbin/iptables -A FORWARD -j CUSTOMFORWARD
```

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

```
      /sbin/iptables -t nat -N CUSTOMPREROUTING
      /sbin/iptables -t nat -A PREROUTING -j CUSTOMPREROUTING

      # Accept everyting connected
      /sbin/iptables -A INPUT   -m state --state ESTABLISHED,RELATED -j
ACCEPT
      /sbin/iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j
ACCEPT

      # localhost and ethernet.
      /sbin/iptables -A INPUT   -i lo         -j ACCEPT
      /sbin/iptables -A INPUT   -p icmp       -j ACCEPT
      /sbin/iptables -A INPUT   -i $GREEN_DEV -j ACCEPT
      /sbin/iptables -A FORWARD -i $GREEN_DEV -j ACCEPT

      # accept all traffic from ipsec interfaces
      /sbin/iptables -A FORWARD -i ipsec+ -j ACCEPT

      # Port forwarding
      if [ "$ORANGE_DEV" != "" ]; then
            # This rule enables a host on ORANGE network to connect to
the outside
            /sbin/iptables -A FORWARD -i $ORANGE_DEV -p tcp \
                  -o ! $GREEN_DEV -j ACCEPT
            /sbin/iptables -A FORWARD -i $ORANGE_DEV -p udp \
                  -o ! $GREEN_DEV -j ACCEPT
      fi

      # RED chain, used for the red interface
      /sbin/iptables -N RED
      /sbin/iptables -A INPUT -j RED
      /sbin/iptables -t nat -N RED
      /sbin/iptables -t nat -A POSTROUTING -j RED

      iptables_red

      # XTACCESS chain, used for external access
      /sbin/iptables -N XTACCESS
      /sbin/iptables -A INPUT -j XTACCESS

      # PORTFWACCESS chain, used for portforwarding
      /sbin/iptables -N PORTFWACCESS
      /sbin/iptables -A FORWARD -j PORTFWACCESS

      # DMZ pinhole chain.  setdmzholes setuid prog adds rules here to
allow
      # ORANGE to talk to GREEN.
      /sbin/iptables -N DMZHOLES
      /sbin/iptables -A FORWARD  -o $GREEN_DEV -j DMZHOLES

      # Custom prerouting chains (for transparent proxy and port
forwarding)
      /sbin/iptables -t nat -N SQUID
      /sbin/iptables -t nat -A PREROUTING -j SQUID
      /sbin/iptables -t nat -N PORTFW
      /sbin/iptables -t nat -A PREROUTING -j PORTFW
```

© SANS Institute 2003, Author retains full rights.

```
      # last rule in input and forward chain is for logging.
      /sbin/iptables -A INPUT   -m limit --limit 10/minute -j LOG --
log-prefix "INPUT "
      /sbin/iptables -A FORWARD -m limit --limit 10/minute -j LOG --
log-prefix "OUTPUT "
        ;;
  stop)
      iptables_init

      # Accept everyting connected
      /sbin/iptables -A INPUT   -m state --state ESTABLISHED,RELATED -j
ACCEPT

      # localhost and ethernet.
      /sbin/iptables -A INPUT -i lo -j ACCEPT
      /sbin/iptables -A INPUT -i $GREEN_DEV -j ACCEPT

      if [ "$RED_DEV" != "" -a "$RED_TYPE" = "DHCP" ]; then
            /sbin/iptables -A input -p tcp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
            /sbin/iptables -A input -p udp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
      fi
      if [ "$PROTOCOL" = "RFC1483" -a "$METHOD" = "DHCP" ]; then
            /sbin/iptables -A input -p tcp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
            /sbin/iptables -A input -p udp --source-port 67 --
destination-port 68 -i $IFACE -j ACCEPT
      fi

      /sbin/iptables -A INPUT   -m limit --limit 10/minute -j LOG --
log-prefix "INPUT "
      /sbin/iptables -A FORWARD -m limit --limit 10/minute -j LOG --
log-prefix "OUTPUT "
        ;;
  reload)
      iptables_red
      ;;
  restart)
      $0 stop
      $0 start
      ;;
  *)
        echo "Usage: $0 {start|stop|reload|restart}"
        exit 1
      ;;
esac

exit 0
```

© SANS Institute 2003, Author retains full rights.