



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 permitted without express written permission.

Table of Contents	1
Vince_Kornacki_GCFW.doc	2

© SANS Institute 2000 - 2002, Author retains full rights.

Security Architecture

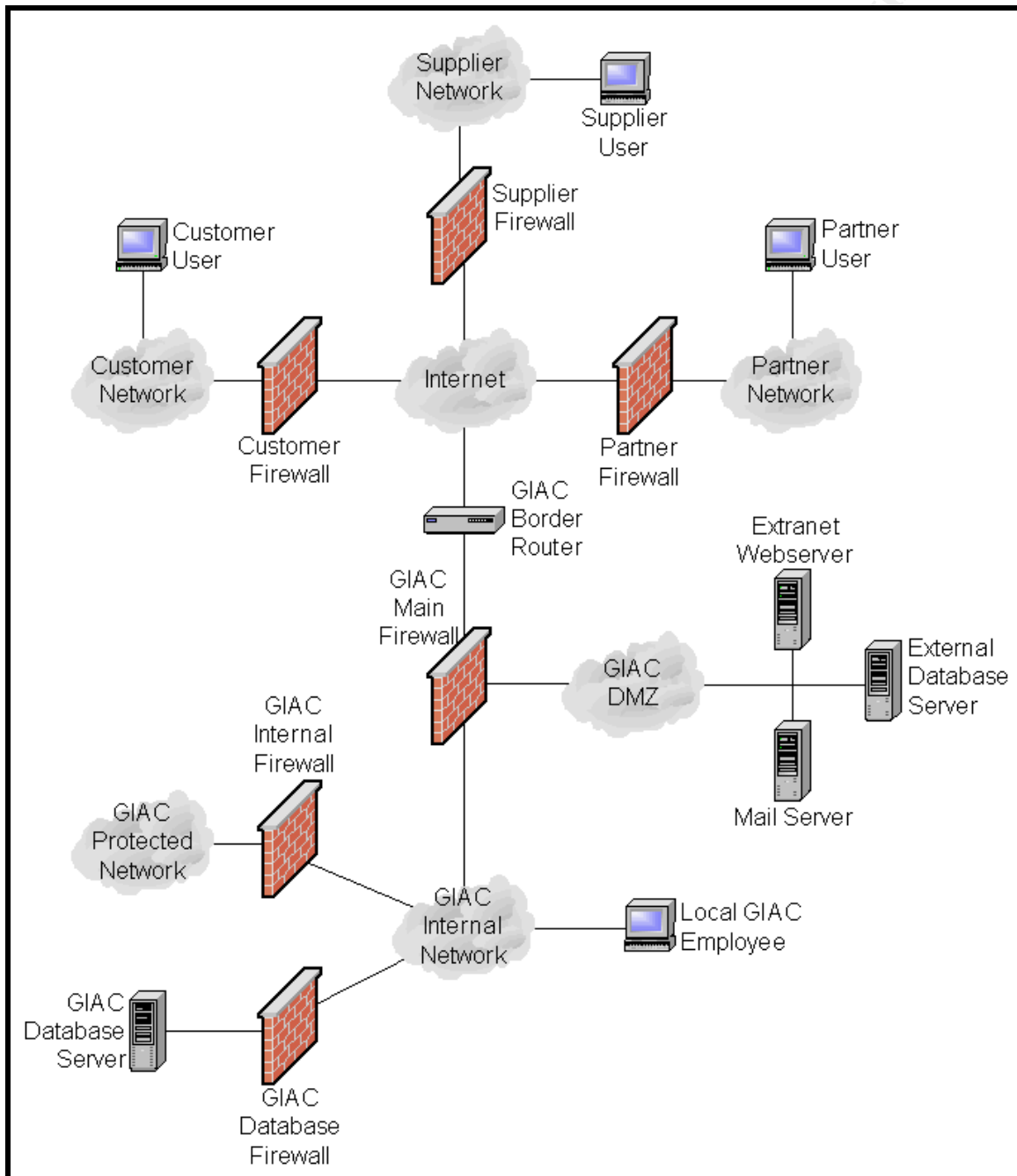
This section defines the security architecture of GIAC Enterprises (henceforth referred to as "GIAC"), an e-business that sells fortune cookie sayings online. The security architecture is specified through a list of security architecture policies. These security architecture policies define access control specifications for customers, suppliers, partners, local GIAC employees, and remote GIAC employees. To prevent confusion, each group is explicitly defined here:

- Customers
Companies that purchase fortune cookie sayings from GIAC
- Suppliers
Companies that sell fortune cookie sayings to GIAC
- Partners
International companies that translate and resell fortune cookie sayings for GIAC
- Local GIAC Users
GIAC Enterprises employees located on the GIAC Internal Network (the GIAC Internal Network will be defined later in this section)
- Remote GIAC Users
GIAC Enterprises employees not located on the GIAC Internal Network (the GIAC Internal Network will be defined later in this section)

First, a network diagram depicting the GIAC security architecture will be displayed. Next, the major security components of the diagram will be further discussed. Finally, the security architecture policies will be defined. The security architecture policies will include discussions of what protocols and applications will be allowed, and what outbound access will be allowed.

Security Architecture Diagram

This section displays the security architecture diagram, which highlights important security devices throughout the GIAC network. It is important to note that not all devices are represented in the diagram, only devices that are significant *with regard to security*. The diagram follows:



Major Security Architecture Components

This section will detail the major security architecture components of the security architecture diagram:

- **GIAC Border Router**
The GIAC Border Router is a Cisco 3600 router running Internetwork Operating System (IOS) 12. The GIAC Border Router is located between the Internet and the GIAC Main Firewall. In addition to routing, the GIAC Router performs rudimentary network traffic filtering. In order to boost performance, however, the GIAC Border Router does not implement Access Control Lists (ACLs), leaving the majority of traffic filtering to the GIAC Main Firewall.
- **GIAC Main Firewall**
The GIAC Main Firewall is a Check Point FireWall-1 4.1 firewall running on a Nokia IP440 firewall appliance. The GIAC Main Firewall is the central access control device in the GIAC network, implementing a rulebase that filters traffic by service. In addition, the GIAC Main Firewall terminates site-to-site Virtual Private Networks (VPNs) to customer, supplier, and partner networks, and client-to-site VPNs to remote GIAC users.
- **GIAC Internal Network**
The GIAC Internal Network is the internal network protected by the GIAC Main Firewall. The GIAC Internal Network is the home of local GIAC users. Even though the GIAC Internal Network is protected by the GIAC Main Firewall, it is still not considered a totally secure network.
- **GIAC Internal Firewall**
The GIAC Internal Firewall is a Check Point FireWall-1 4.1 firewall running on a Nokia IP440 firewall appliance. The GIAC Internal Firewall is a second-tier firewall that protects the GIAC Protected Network. The GIAC Protected Network contains servers that store sensitive information, such as Human Resources (HR) and Accounting servers. Consequently, another layer of protection is needed for the GIAC Protected Network. The GIAC Internal Firewall provides this additional layer of protection, enforcing a strict rulebase that filters traffic by service.
- **GIAC Protected Network**
The GIAC Protected Network is an internal network that is protected by both the GIAC Main Firewall and the GIAC Internal Firewall. The GIAC Protected Network contains HR and Accounting servers, which both store sensitive information. Consequently, the GIAC Internal Firewall is configured to provide an extra layer of protection, protecting sensitive information from both the Internet the GIAC Internal Network.

- **GIAC Database Firewall**
The GIAC Database Firewall is a Check Point FireWall-1 4.1 firewall running on a Nokia IP440 firewall appliance. The GIAC Database Firewall is a second-tier firewall that protects the GIAC Database Server. The GIAC Database Server stores all of the GIAC fortune cookie sayings, which are the lifeblood of the company. Consequently, another layer of protection is needed for the GIAC Database Server. The GIAC Database Firewall provides this additional layer of protection, enforcing a strict rulebase that filters traffic by service.
- **GIAC Database Server**
The GIAC Database Server is the internal repository for GIAC fortune cookie sayings. An interface to the fortune cookie sayings is provided by an HTTPS frontend to the database program. Only authenticated GIAC users are allowed to access the HTTPS interface. Authentication is provided by the HTTPS server, which implements strong authentication using RSA ACE/Server and SecurID tokens.
- **Extranet Webserver**
The GIAC Extranet Webserver is an HTTPS server that provides information to customer, supplier, and partner users, and to GIAC employees. Authentication is provided by the HTTPS server, which implements strong authentication using RSA ACE/Server and SecurID tokens. It is important to note that the Extranet Webserver *is not* the GIAC corporate webserver. The GIAC corporate webserver is hosted by an Internet Service Provider (ISP).
- **External Database Server**
The External Database Server is the external repository for GIAC fortune cookie sayings. An interface to the fortune cookie sayings is provided by an HTTPS frontend to the database program. Only authenticated customer, supplier, and partner users, and authenticated GIAC users, are allowed to access the HTTPS interface. Authentication is provided by the HTTPS server, which implements strong authentication using RSA ACE/Server and SecurID tokens.

Security Architecture Policies

This section will define the security architecture policies. The security architecture policies are a subset of the GIAC security policy, and define policies regarding the security architecture. Other matters covered by the GIAC security policy, such as Intrusion Detection Systems (IDS) and physical security, are out of the scope of the security architecture policies, and therefore are not defined here. The security architecture policies follow:

1. GIAC fortune cookie sayings will be stored on the GIAC Database Server. Authenticated local GIAC users will be allowed to access the GIAC Database Server through an HTTPS frontend that interfaces with the

database program. The HTTPS server will provide strong authentication using RSA ACE/Server and SecurID tokens. For enhanced security, remote GIAC users will not be allowed access to the GIAC Database Server.

2. All servers that need to be accessed by customer, supplier, and partner users will be located on the GIAC DMZ. Servers on the GIAC DMZ will only be accessible through VPNs, or from the GIAC Internal Network. For enhanced security, servers on the GIAC DMZ will not be translated with Network Address Translation (NAT), and, thus, will not be publicly accessible.
3. When fortune cookie sayings need to be transferred between GIAC and a customer, supplier, or partner, those fortune cookie sayings will be uploaded to the External Database Server. Authenticated customer, supplier, and partner users will be allowed to access the External Database Server through an HTTPS frontend that interfaces with the database program. The HTTPS server will provide strong authentication using RSA ACE/Server and SecurID tokens. For enhanced security, the External Database Server will not be translated with NAT, and, thus, will not be publicly accessible.
4. The GIAC Border Router will implement ACLs to perform rudimentary network traffic filtering. This rudimentary traffic filtering includes dropping:
 - Directed broadcasts
 - Source-routed packets
 - ICMP unreachable messages

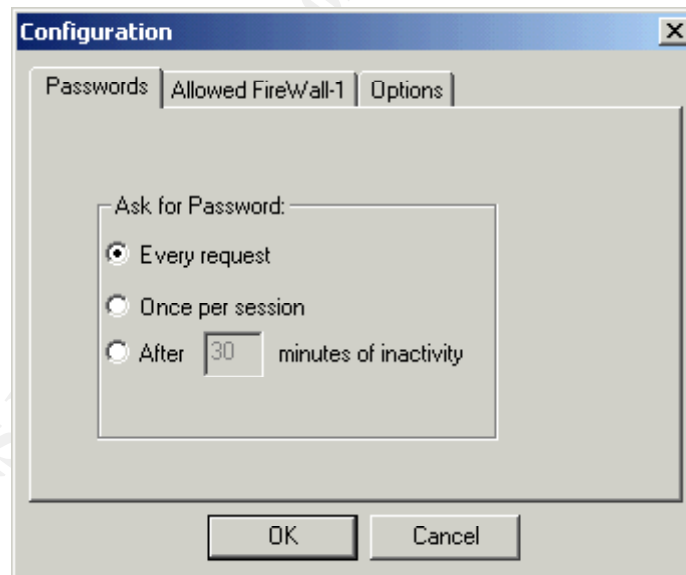
In addition, the following unnecessary services will be disabled on the router:

- TCP small servers (echo, discard, chargen, and daytime)
 - UDP small servers (echo, discard, and chargen)
 - Finger
 - Cisco Discovery Protocol (CDP)
 - Network Time Protocol (NTP)
 - HyperText Transfer Protocol (HTTP)
 - Simple Network Management Protocol (SNMP)
5. The GIAC Main Firewall should run a “hardened” version of Nokia IPSO that:
 - Runs Nokia Network Voyager over HTTPS only, not HTTP
 - Allows command-line access over SSH only, not Telnet

In addition, all other unnecessary services should be disabled. The GIAC Main Firewall will implement a rulebase that will:

- Terminate site-to-site VPNs that allow authenticated customer, supplier, and partner users limited access to the GIAC DMZ
- Terminate client-to-site VPNs that allow authenticated remote GIAC users limited access to the GIAC DMZ
- Allow authenticated local GIAC users limited access from the GIAC Internal Network to the GIAC DMZ
- Allow authenticated local GIAC users limited access from the GIAC Internal Network to the Internet

Access will be limited on a per-service basis. All traffic other than NetBIOS will be logged. Site-to-site VPN access will be authenticated with shared secrets. Client-to-site VPN access will be authenticated with RSA ACE/Server and SecurID tokens through the Check Point SecuRemote VPN client. All other authentication will be handled by the Check Point Session Authentication Agent, a lightweight program installed on GIAC workstations. The Session Authentication Agent has a simple, intuitive interface:



The Session Authentication Agent securely and seamlessly interfaces with FireWall-1 for efficient user authentication.

6. The GIAC Internal Firewall will implement a strict rulebase that will:
 - Allow authenticated GIAC HR users limited access to the HR servers on the GIAC Protected Network
 - Allow authenticated GIAC Accounting users limited access to the Accounting servers on the GIAC Protected Network

Access will be limited on a per-service basis. All traffic will be logged. Authentication will be provided by the Check Point Session Authentication agent, using RSA ACE/Server and SecurID tokens for strong authentication.

7. The GIAC Database Firewall will implement a strict rulebase that will:

- Allow limited access for authenticated database users to the GIAC Database Server

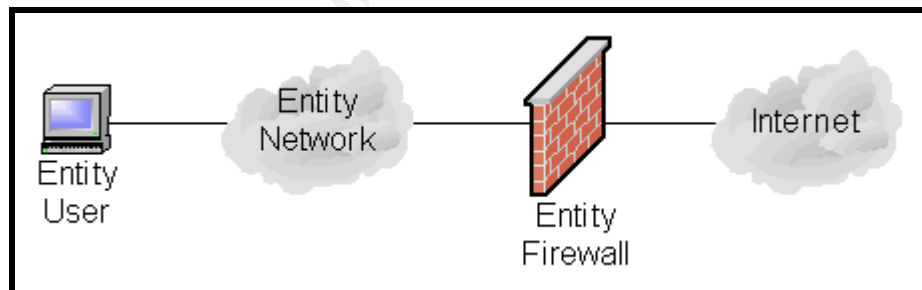
Access will be limited on a per-service basis. All traffic will be logged. Authentication will be provided by the Check Point Session Authentication agent, using RSA ACE/Server and SecurID tokens for strong authentication.

8. External connections will be allowed from the following entities:

- Customers
- Suppliers
- Partners

Each connection will take the form of a site-to-site VPN. The VPN will be terminated by the GIAC Main Firewall, and will only allow access to the GIAC DMZ. Furthermore, access will be restricted by service.

From the viewpoint of GIAC, the architecture of the customer, supplier, and partner networks is essentially the same:



The components are defined as follows:

- Entity Firewall
The Entity Firewall is the firewall that protects the Entity Network. In addition, the Entity Firewall terminates the site-to-site VPN to the GIAC DMZ. Because Entity Users will be allowed access to the GIAC network, it is important that the Entity Network is secure. In addition, it is important that the Entity Firewall securely terminates the site-to-site VPN.
- Entity Network
The Entity Network is an internal network protected by the Entity Firewall. The Entity Network provides a workplace for the Entity User, and is connected to the GIAC DMZ by the site-

to-site VPN.

© SANS Institute 2000 - 2002, Author retains full rights.

- Entity User

The Entity User is the actual end user that connects to servers on the GIAC DMZ through the site-to-site VPN.

For each entity, a separate site-to-site VPN will be established between the Entity Firewall and the GIAC Main Firewall. This VPN will allow Entity Users located on the Entity Network to securely access resources on the GIAC DMZ. Only a specific service will be allowed through the VPN:

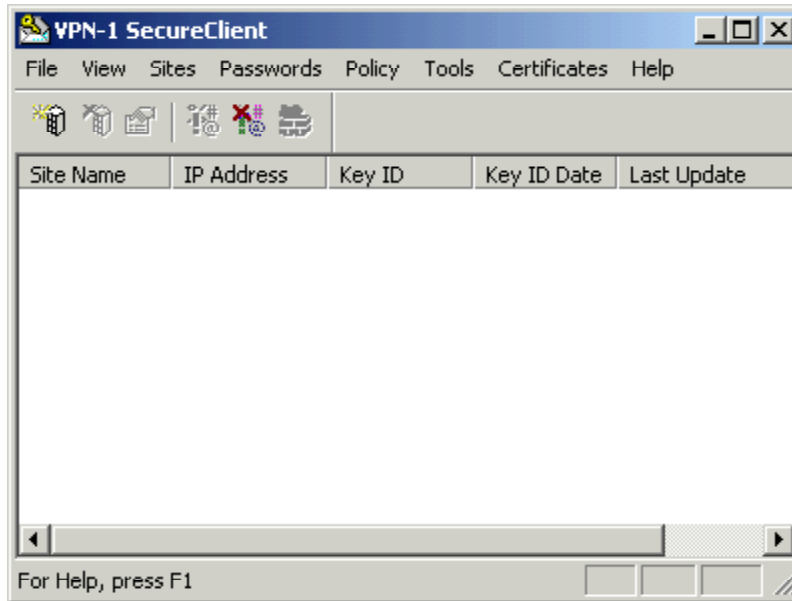
Service	Purpose
HTTPS	Allows entity users to securely access GIAC DMZ servers

Specifically, Entity Users will be allowed HTTPS access to the GIAC Extranet Webserver and External Database Server. Note that only HTTPS, not HTTP, will be allowed through the VPN. In addition to VPN authentication, entity users will be authenticated by the webserver or data server. RSA ACE/Server and SecurID tokens will be used for secure two-factor authentication. For the sake of accountability, each user will have a unique username. In addition, each entity will only be allowed to access their own data. Access will be controlled with HTTPS authentication and directory permissions. These mechanisms ensure the confidentiality of GIAC data.

9. External connections will also be allowed from remote GIAC users. Each connection will take the form of a client-to-site VPN. The VPN will be terminated by the GIAC Main Firewall, and will only allow access to the GIAC DMZ. Furthermore, access will be restricted by service. Specifically, only the following services will be allowed:

Service	Purpose
SMTP	Allows GIAC users to send email
POP3	Allows GIAC users to receive email
HTTPS	Allows entity users to securely access GIAC DMZ servers
SSH/SCP	Allows entity users to securely administer GIAC DMZ servers

Remote GIAC users will use the Check Point SecuRemote VPN client to access the VPN. SecuRemote has a simple, intuitive interface:



The client-to-site VPN access will be authenticated with RSA ACE/Server and SecurID tokens.

10. Only limited outbound access will be allowed. Specifically, only the following services will be allowed:

Service	Purpose
HTTP	Allows GIAC users to access Internet web servers
HTTPS	Allows GIAC users to access secure Internet web servers
FTP	Allows GIAC users to transfer files from Internet servers

In addition, local GIAC users will be allowed limited access to the DMZ for the following services:

Service	Purpose
SMTP	Allows GIAC users to send email
POP3	Allows GIAC users to receive email
HTTPS	Allows entity users to securely access GIAC DMZ servers
SSH/SCP	Allows entity users to securely administer GIAC DMZ servers

Note that access to the GIAC DMZ is restricted on a per server basis. For example, a firewall rule will only allow SMTP access to the Mail Server, not the Extranet Webserver.

Summary

This section displayed the security architecture diagram, discussed the main components of the diagram, and defined the security architecture policies. The security architecture detailed in this section is both technically reasonable and financially feasible. Technically, this security architecture implements the best

practices of the security industry. Financially, this security architecture provides an affordable, scalable solution that meets the needs of GIAC. While implementing this solution will cost a considerable amount of money, GIAC will be investing in the security of their data, which is after all the lifeblood of the company.

Security Policy and Tutorial

This section defines the security policy enforced on the security devices throughout the GIAC network. These security devices include:

- GIAC Border Router
- GIAC Main Firewall
- GIAC Internal Firewall
- GIAC Database Firewall

For each policy, each configuration command or rule will be explained in detail.

GIAC Border Router

The GIAC border router is the first line of defense against attackers. The GIAC Border Router is a Cisco 3600 router running IOS 12. The latest patches will be installed, and the router will be configured in a secure manner. While the GIAC Border Router does not enforce exhaustive ACLs, it does implement rudimentary network traffic filtering. The relevant portion of the GIAC Border Router configuration will be listed and detailed. Note that only the sections that deal specifically with security are covered. Routing functionality is not covered. In general, the ordering of router configuration commands is not important. The ordering of ACLs is very important, but the GIAC router configuration does not implement ACLs. The GIAC Border Router configuration follows, with lines numbered for easy reference:

1. interface serial 0
2. no service tcp-small-servers
3. no service udp-small-servers
4. no service finger
5. no cdp enable
6. no ntp enable
7. no ip directed-broadcast
8. no ip source-route
9. no ip unreachable
10. no http
11. no snmp
12. !
13. interface ethernet 0
14. no service tcp-small-servers
15. no service udp-small-servers
16. no service finger

```
17. no cdp enable
18. no ntp enable
19. no ip directed-broadcast
20. no ip source-route
21. no ip unreachable
22. no http
23. no snmp
24. !
25. ip route 10.0.0.0 0.255.255.255 null 0 255
26. ip route 172.16.0.0 0.31.255.255 null 0 255
27. ip route 192.168.0.0 0.0.255.255 null 0 255
28. ip route 127.0.0.0 0.255.255.255 null 0 255
```

An explanation of each configuration command follows:

Lines 1 & 13

The “`interface serial 0`” and “`interface ethernet 0`” commands place the router into interface configuration mode. Several commands will be applied to each interface, greatly enhancing the security of the router.

Lines 2 & 14

The “`no service tcp-small-servers`” command disables a variety of unnecessary TCP services (echo, discard, chargen, and daytime) that are vulnerable to Denial of Service (DoS) attacks.

Lines 3 & 15

The “`no service udp-small-servers`” command disables a variety of unnecessary UDP services (echo, discard, and chargen) that are vulnerable to DoS attacks.

Lines 4 & 16

The “`no service finger`” command disables the finger service, which can reveal sensitive router information.

Lines 5 & 17

The “`no cdp enable`” command disables the Cisco Discovering Protocol, which can reveal sensitive router information.

Lines 6 & 18

The “`no ntp enable`” command disables the Network Time Protocol, which is vulnerable to DoS attacks.

Lines 7 & 19

The “`no ip directed-broadcast`” command prevents attackers from using the router as a “smurf” amplifier. A smurf attack sends ICMP “echo-request” packets to a broadcast address, exponentially multiplying the number of “echo-reply” packets returned to the spoofed target.

Lines 8 & 20

The “`no ip source-route`” command prevents the router from accepting source-routed packets, which can be used to exploit trust relationships.

Lines 9 & 21

The “[no ip unreachable](#)” command prevents the router from sending ICMP unreachable messages, which can be used to map the network.

Lines 10 & 22

The “[no http](#)” command disables the webserver, which can reveal sensitive router information.

Lines 11 & 23

The “[no snmp](#)” command disables SNMP, which can reveal sensitive router information.

Lines 12 & 24

The “!” specifies a comment, which is not processed by the router.

Lines 25-28

The “[ip route](#)” commands are an alternative to ACLs that prevent the routing of packets destined for the private address ranges (10.0.0.0/8, 172.168.0.0/12, 192.168.0.0/16, and 127.0.0.0/8). For example, the command “[ip route 10.0.0.0 0.255.255.255 null 0 255](#)” will route all packets destined for the 10.0.0.0/8 network to the null interface, effectively dropping the packets. Using a route statement instead of an ACL, however, dramatically improves router performance.











For more information on enhancing Cisco router security, see “[Improving Security on Cisco Routers](#)” [1].

GIAC Main Firewall

The GIAC Main Firewall is the heart of the GIAC security architecture. The main firewall is the central access control device, and terminates both site-to-site and client-to-site VPNs. The GIAC Main Firewall is a Check Point Firewall-1 4.1 firewall running on a Nokia IP440 firewall appliance. The latest FireWall-1 Service Pack will be installed, and the IP440 firewall appliance will be configured in a secure manner. Specifically, the IP440 firewall appliance will:

- Run Nokia Network Voyager over HTTPS only, not HTTP
- Allow command-line access over SSH only, not Telnet

In addition, a rule in the Firewall-1 rulebase will allow Voyager and SSH access only from the Management Server. The complete rulebase follows:

No.	Source	Destination	Service	Action	Track
1	 Allowed_VPN_Devices  GIAC_Main_Firewall	 Allowed_VPN_Devices  GIAC_Main_Firewall	 IPSEC	 accept	 Long
2	 Customer_Network  GIAC_DMZ	 Customer_Network  GIAC_DMZ	 https	 Encrypt	 Long
3	 Supplier_Network  GIAC_DMZ	 Supplier_Network  GIAC_DMZ	 https	 Encrypt	 Long
4	 Partner_Network  GIAC_DMZ	 Partner_Network  GIAC_DMZ	 https	 Encrypt	 Long
5	 GIAC_Users@GIAC_Network	 GIAC_Extranet_Webserver	 https	 Session Auth	 Long
6	 GIAC_Users@GIAC_Network	 GIAC_Mail_Server	 smtp  pop-3	 Session Auth	 Long
7	 GIAC_Users@GIAC_Network	 GIAC_External_Database_Server	 https  ssh	 Session Auth	 Long
8	 Any	 GIAC_Main_Firewall	 FW1_topo  FW1_key  IPSEC	 accept	 Long
9	 GIAC_Main_Firewall	 Any	 IPSEC	 accept	 Long
10	 GIAC_Users@Any	 GIAC_Extranet_Webserver	 https	 Client Encrypt	 Long
11	 GIAC_Users@Any	 GIAC_Mail_Server	 smtp  pop-3	 Client Encrypt	 Long
12	 GIAC_Users@Any	 GIAC_External_Database_Server	 https	 Client Encrypt	 Long
13	 Management_Server	 GIAC_Main_Firewall	 https  ssh  FireWall1	 accept	 Long
14	 Any	 GIAC_Main_Firewall	 Any	 drop	 Long
15	 Any	 Any	 NBT	 drop	
16	 GIAC_Users@GIAC_Network	 GIAC_DMZ	 http  https  ftp  domain-udp	 Session Auth	 Long
17	 Any	 Any	 Any	 drop	 Long

In addition to the rulebase, several implied rules are automatically generated by the “policy properties” settings:

Properties Setup

Authentication | SYNDefender | LDAP | Encryption | ConnectControl
High Availability | IP Pool NAT | Access Lists | Desktop Security
Security Policy | Traffic Control | Services | Log and Alert | Security Servers

Apply Gateway Rules to Interface Direction: Inbound

TCP Session Timeout: 3600 Seconds

☒ Accept UDP Replies:

UDP Virtual Session Timeout: 40 Seconds

☒ Enable Decryption on Accept

Implied Rules

- ☐ Accept VPN-1 & FireWall-1 Control Connections: First
- ☐ Accept RIP: First
- ☐ Accept Domain Name Over UDP (Queries): First
- ☐ Accept Domain Name Over TCP (Zone Transfer): First
- ☐ Accept ICMP: Before Last
- ☐ Accept Outgoing Packets Originating From Gateway: Before Last

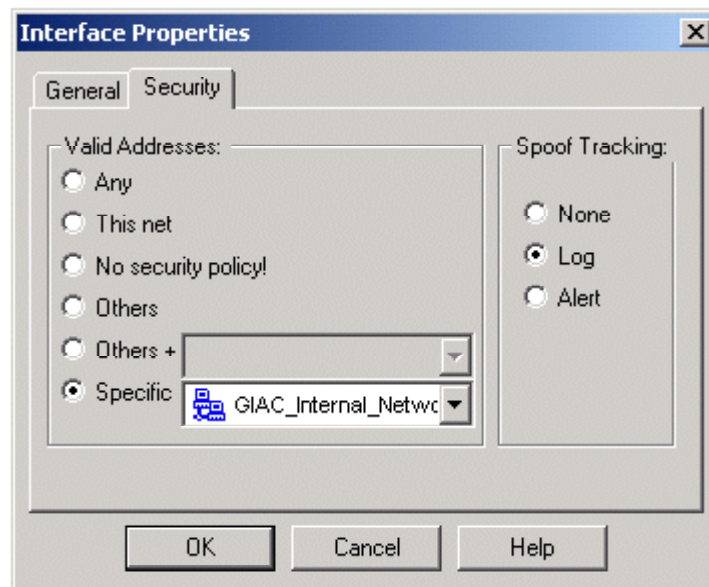
☒ Log Implied Rules

☐ Install Security Policy only if it can be successfully installed on ALL selected targets.

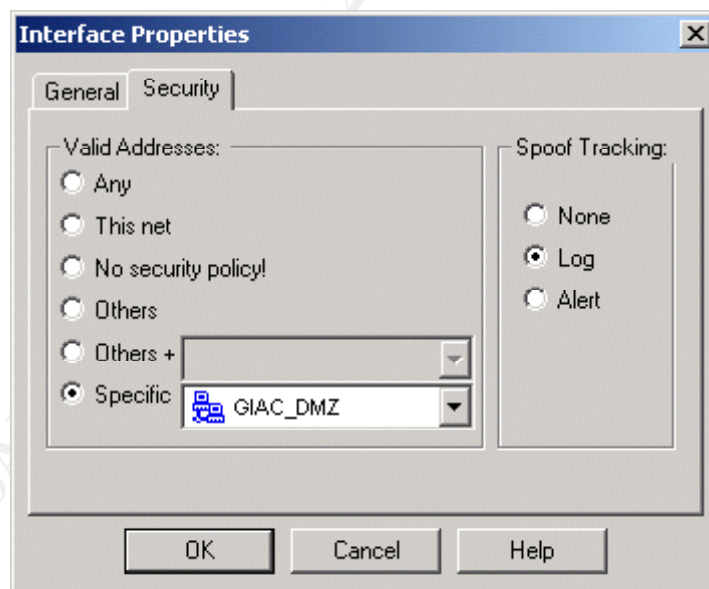
OK Cancel Help

In this case, all of the “implied rules” are disabled. Disabling the implied rules allows more granular control of the firewall policy. With the exception of the anti-spoofing policy, all of the rules are explicitly generated by the rulebase.

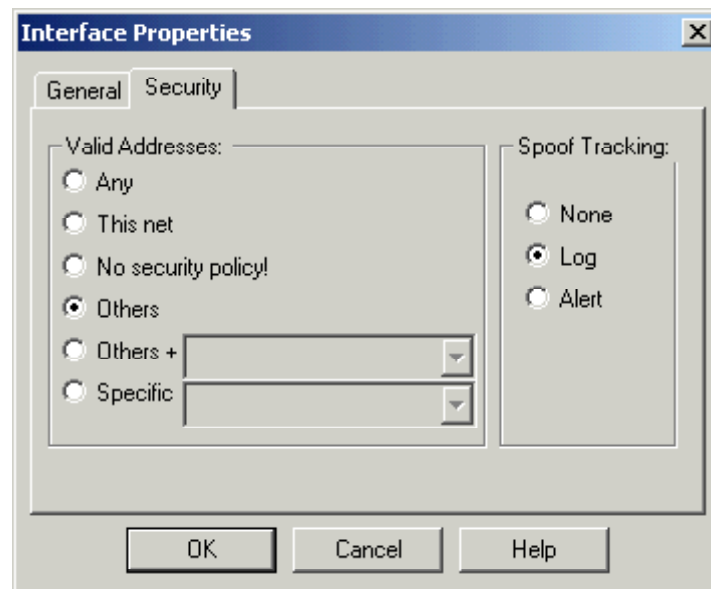
The anti-spoofing policy is configured on the firewall objects themselves. For example, the internal interface of the GIAC Main Firewall object is configured to only accept inbound packets from the GIAC Internal Network:



The DMZ interface is configured to only accept inbound packets from the GIAC DMZ:



Finally, the external interface is configured to only accept inbound packets with addresses *other* than those assigned to the other interfaces:



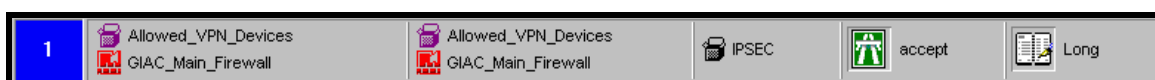
This configuration prevents attackers from spoofing internal addresses through the firewall. If the external interface receives an inbound packet with an address assigned to the GIAC Internal Network or GIAC DMZ, the firewall will know the packet is spoofed. The firewall will drop the packet and log the attempted spoof.

The order of the rules in the rulebase is extremely important. The following ordering guidelines were followed when creating the rulebase:

- Rules handling traffic that must directly access the firewall must come before the stealth rule (rule 14). This includes authentication rules (rules 5-7) and encryption rules (rules 1-4 and 8-12).
- All other rules should appear after the stealth rule (rule 14).
- The cleanup rule should be last (rule 17).
- Rules handling higher priority traffic, such as customer, supplier, and partner traffic (rules 2-4) should appear near the top of the rulebase.
- Rules handling lower priority traffic, such as Netbios (rule 15), should appear near the bottom of the rulebase.

A detailed description of each rule in the rulebase follows:

Rule1



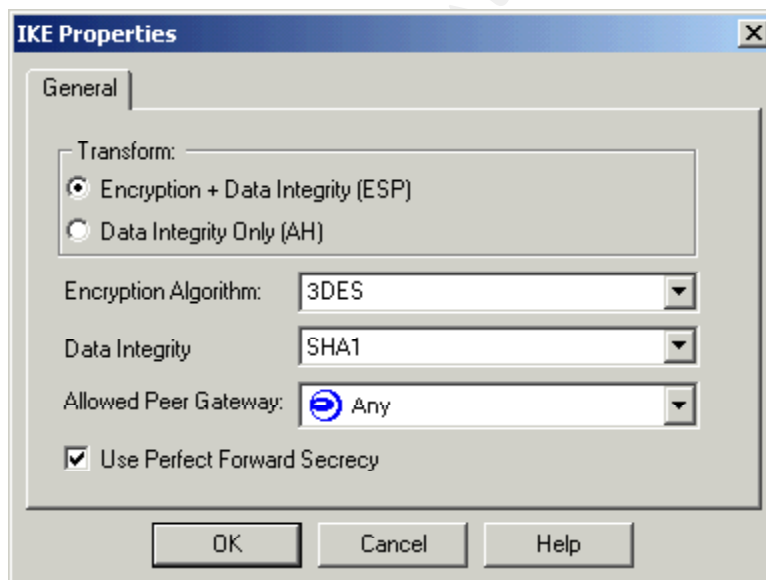
This rule allows the IPSEC services between the GIAC Main Firewall and the Allowed VPN Devices. This rule is necessary to establish site-to-site VPNs to

customer, supplier, and partner networks. The Allowed_VPN_Devices group contains all of the customer, supplier, and partner VPN devices. The IPSEC services group includes services such as AH (IP type 50), ESP (IP type 51), and IKE (UDP port 500).

Rule 2

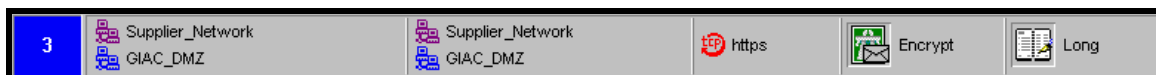


This rule creates a site-to-site VPN between the GIAC network and a customer network. Note that a separate rule will exist for each customer. As designated by the “Service” column, only the HTTPS protocol will be allowed through the VPN. The customer will use HTTPS to access the Extranet Webserver and External Database Server. For access control and auditing, the HTTPS server will require user authentication. This rule is important because customers need to access resources on the GIAC DMZ, but GIAC needs to ensure the security of those resources. If the GIAC External Database Server is breached, GIAC fortune cookie sayings could be stolen, which would cost GIAC millions of dollars in lost revenue. The VPN is established with 3DES encryption:



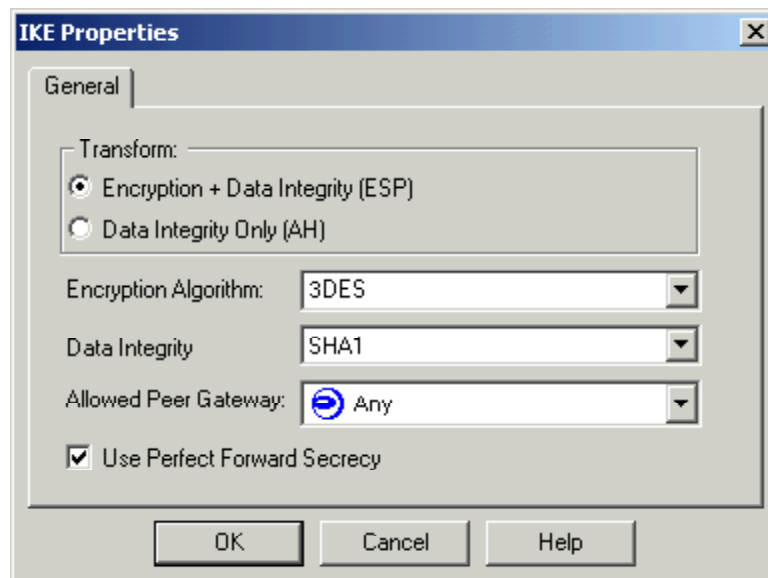
This strong encryption ensures the confidentiality of GIAC data.

Rule 3



This rule creates a site-to-site VPN between the GIAC network and a supplier network. Note that a separate rule will exist for each supplier. As designated by the “Service” column, only the HTTPS protocol will be allowed through the VPN. The supplier will use HTTPS to access the Extranet Webserver and External Database Server. For access control and auditing, the HTTPS server will require user authentication. This rule is important because suppliers need to access

resources on the GIAC DMZ, but GIAC needs to ensure the security of those resources. If the GIAC External Database Server is breached, GIAC fortune cookie sayings could be stolen, which would cost GIAC millions of dollars in lost revenue. The VPN is established with 3DES encryption:



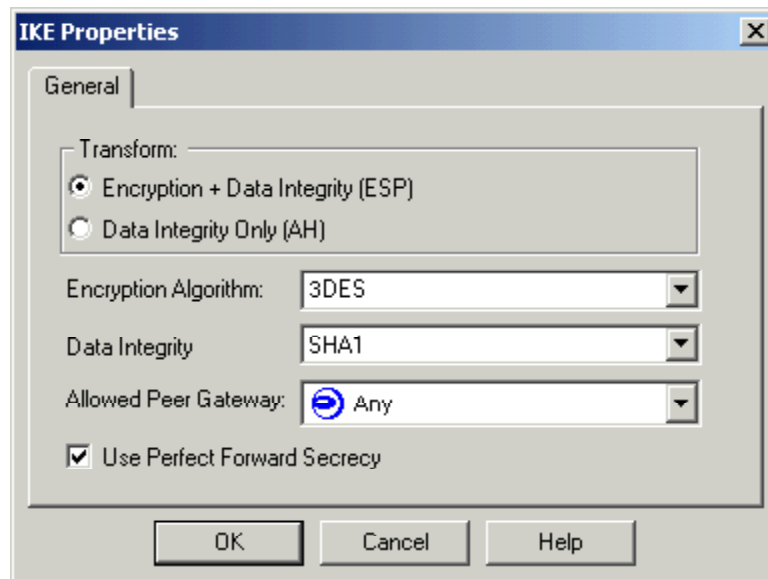
This strong encryption ensures the confidentiality of GIAC data.

Rule 4

4	Partner_Network GIAC_DMZ	Partner_Network GIAC_DMZ	https	Encrypt	Long
---	-----------------------------	-----------------------------	-------	---------	------

This rule creates a site-to-site VPN between the GIAC network and a partner network. Note that a separate rule will exist for each partner. As designated by the "Service" column, only the HTTPS protocol will be allowed through the VPN. The partner will use HTTPS to access the Extranet Webserver and External Database Server. For access control and auditing, the HTTPS server will require user authentication. This rule is important because partners need to access resources on the GIAC DMZ, but GIAC needs to ensure the security of those resources. If the GIAC External Database Server is breached, GIAC fortune cookie sayings could be stolen, which would cost GIAC millions of dollars in lost revenue.

The VPN is established with 3DES encryption:



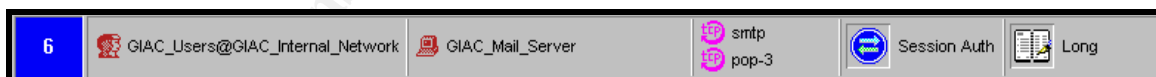
This strong encryption ensures the confidentiality of GIAC data.

Rule 5



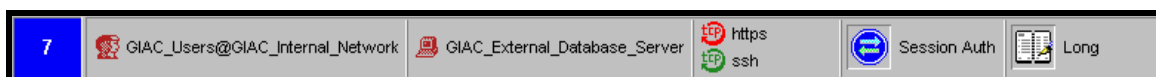
This rule allows authenticated local GIAC users access to the Extranet Webserver using the HTTPS service. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because authenticated local GIAC users need to securely access content on the Extranet Webserver.

Rule 6



This rule allows authenticated local GIAC users access to the Mail Server using the SMTP and POP3 services. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because authenticated local GIAC users need to securely send (SMTP) and receive (POP3) email.

Rule 7



This rule allows authenticated local GIAC users access to the External Database

Server using the HTTPS and SSH services. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because authenticated local GIAC users need to securely access the database server (HTTPS) and login for system administration (SSH).

Rule 8



This rule allows the firewall to accept the FW1_topo, FW1_key, and IPSEC services from any destination. These services are used to establish the client-to-site VPNs handled by rules 10-12. The source of this rule cannot be specified, because the addresses of the remote users are not known. The IPSEC service group includes services such as AH (IP type 50), ESP (IP type 51), and IKE (UDP port 500).

Rule 9



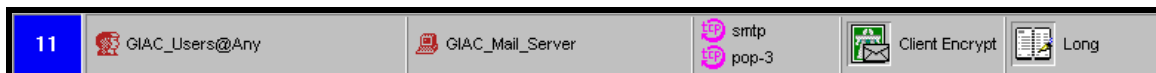
This rule allows the firewall to send IPSEC packets to any destination. This is necessary to establish the client-to-site VPNs handled by rules 10-12. The destination of this rule cannot be specified, because the addresses of the remote users are not known. The IPSEC service group includes services such as AH (IP type 50), ESP (IP type 51), and IKE (UDP port 500).

Rule 10



This rule allows authenticated remote GIAC users access to the Extranet Webserver using the HTTPS service. This access is encrypted by the client-to-site VPN using the SecuRemote client software. Authentication is performed by SecuRemote, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. Furthermore, the Extranet Webserver will also authenticate the users. This rule is important because authenticated remote GIAC users need to securely access the Extranet Webserver.

Rule 11



This rule allows authenticated remote GIAC users access to the Mail Server using the SMTP and POP3 services. This access is encrypted by the client-to-site VPN using the SecuRemote client software. Authentication is performed by

SecuRemote, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because authenticated remote GIAC users need to securely send (SMTP) and receive (POP3) email.

Rule 12



This rule allows authenticated remote GIAC users access to the External Database Server using the HTTPS service. This access is encrypted by the client-to-site VPN using the SecuRemote client software. Authentication is performed by SecuRemote, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. Furthermore, the External Database Server will also authenticate the users. This rule is important because authenticated remote GIAC users need to securely access the External Database Server.

Rule 13



This rule allows the Management Server to directly access the GIAC Main Firewall for the HTTPS, SSH, and FireWall-1 services. The HTTPS service is used for Voyager access, and the SSH service is used for secure command line access. Both of these protocols will perform user authentication using Nokia IPSO passwords. The FireWall-1 services group includes services such as FW, FW1_mgmt, and FW1_log, and is used for FireWall-1 control connections. This rule is important because, for proper management, the Management Server needs HTTPS, SSH, and FireWall-1 access to the GIAC Main Firewall.

Rule 14



This rule drops all other traffic destined for the firewall itself, and is commonly referred to as the “stealth” rule. This rule prevents attackers from directly accessing the firewall. This rule must appear after all rules that handle traffic destined for the firewall itself, which includes authentication and encryption rules. This rule is important because it prevents attacks against the firewall itself.

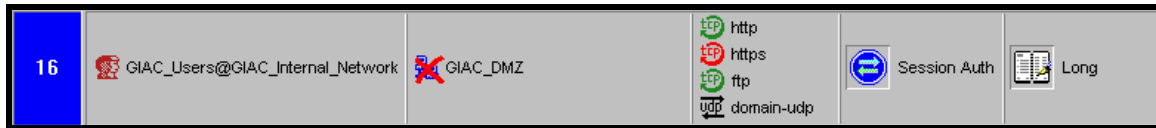
Rule 15



This rule drops all Netbios traffic, without logging it (notice that, unlike the other rules, the last column of the rule does not specify “Long Log”). The Netbios protocol generates massive amounts of traffic. Logging all of this traffic can

quickly fill the FireWall-1 logs. Consequently, this rule specifies that Netbios traffic is not to be logged.

Rule 16



This rule allows authenticated local GIAC users limited outbound access. The negated GIAC DMZ object in the Destination of the rule specifies that users can access any destinations not in the GIAC DMZ. Access to the GIAC DMZ is handled by rules 5-7. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. Authenticated users can use the HTTP, HTTPS, and FTP services. These protocols are used to search for new fortune cookie sayings. In addition, the DOMAIN-UDP service is allowed for name resolution. This rule is important because, to efficiently do their jobs, GIAC employees need outbound access.

Rule 17



This rule drops and logs all other traffic, and is commonly referred to as the “cleanup” rule. This rule is the implementation of the “deny that which is not explicitly allowed” security policy. Even without the cleanup rule, however, the “implicit drop” rule would drop packets not matched by other rules in the rulebase. The implicit drop rule, however, would not log these packets. Implementing the cleanup rule ensures that all other traffic will be dropped and logged. This rule must be the last rule in the rulebase, because it will catch all remaining traffic.

GIAC Internal Firewall

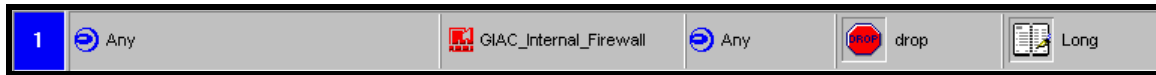
The GIAC Internal Firewall protects servers on the GIAC Protected Network, which includes HR and Accounting servers. These servers store sensitive information, so a second layer of protection is necessary. The complete rulebase follows:

No.	Source	Destination	Service	Action	Track
1	 Any	 GIAC_Internal_Firewall	 Any	 drop	 Long
2	 HR_Users@GIAC_Network	 GIAC_HR_Servers	 https	 Session Auth	 Long
3	 Accounting_Users@GIAC_Network	 GIAC_Accounting_Servers	 https	 Session Auth	 Long
4	 Management_Server	 GIAC_Internal_Firewall	 https  ssh  FireWall1	 accept	 Long
5	 Any	 Any	 Any	 drop	 Long

© SANS Institute 2000 - 2002, Author retains full rights.

A detailed description of each rule follows:

Rule1



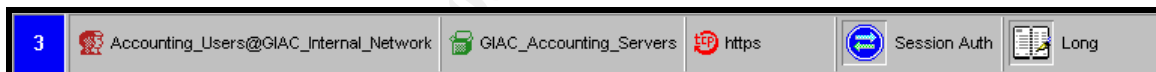
This rule drops all traffic destined for the firewall itself, and is commonly referred to as the “stealth” rule. This rule prevents attackers from directly accessing the firewall. This rule must appear after all rules that handle traffic destined for the firewall itself, which includes authentication and encryption rules. In this case, the GIAC Internal Firewall does not implement any authentication or encryption rules, so the stealth rule appears first. The stealth rule is important because it prevents attacks against the firewall itself.

Rule 2



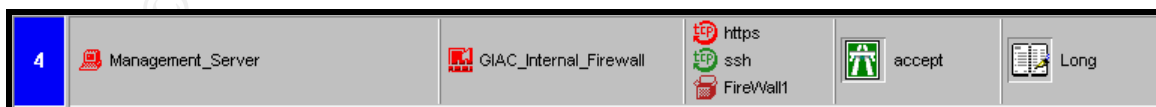
This rule allows authenticated local GIAC HR users access to the GIAC HR servers using the HTTPS service. Note that HR users can only access the HR servers on the GIAC Protected Network, not the Accounting servers. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because HR users need to securely access the HR servers.

Rule 3



This rule allows authenticated local GIAC Accounting users access to the GIAC Accounting servers using the HTTPS service. Note that Accounting users can only access the Accounting servers on the GIAC Protected Network, not the HR servers. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because Accounting users need to securely access the Accounting servers.

Rule 4



This rule allows the Management Server to directly access the GIAC Internal Firewall for the HTTPS, SSH, and FireWall-1 services. The HTTPS service is used for Voyager access, and the SSH service is used for secure command line access. Both of these protocols will perform user authentication using Nokia IPSO passwords. The FireWall-1 services group includes services such as FW, FW1_mgmt, and FW1_log, and is used for FireWall-1 control connections. This

rule is important because, for proper management, the Management Server needs HTTPS, SSH, and FireWall-1 access to the GIAC Internal Firewall.

Rule 5



This rule drops and logs all other traffic, and is commonly referred to as the “cleanup” rule. This rule is the implementation of the “deny that which is not explicitly allowed” security policy. Even without the cleanup rule, however, the “implicit drop” rule would drop packets not matched by other rules in the rulebase. The implicit drop rule, however, would not log these packets. Implementing the cleanup rule ensures that all other traffic will be dropped and logged. This rule must be the last rule in the rulebase, because it will catch all remaining traffic.

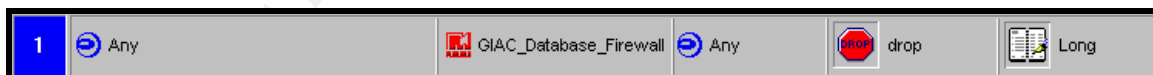
GIAC Database Firewall

The GIAC Database Firewall protects the GIAC Database Server. This server stores all of the GIAC fortune cookie sayings, so a second layer of protection is necessary. The complete rulebase follows:

No.	Source	Destination	Service	Action	Track
1	Any	GIAC_Database_Firewall	Any	drop	Long
2	Database_Users@GIAC_Internal_Network	GIAC_Database_Server	https ssh	Session Auth	Long
3	Management_Server	GIAC_Database_Firewall	https ssh FireWall1	accept	Long
4	Any	Any	Any	drop	Long

A detailed description of each rule follows:

Rule1



This rule drops all other traffic destined for the firewall itself, and is commonly referred to as the “stealth” rule. This rule prevents attackers from directly accessing the firewall. This rule must appear after all rules that handle traffic destined for the firewall itself, which includes authentication and encryption rules. In this case, the GIAC Database Firewall does not implement any authentication or encryption rules, so the stealth rule appears first. The stealth rule is important because it prevents attacks against the firewall itself.

Rule 2



This rule allows authenticated local GIAC database users access to the GIAC Database Servers using the HTTPS and SSH services. Session Authentication is performed by the FireWall-1 Session Authentication Agent, using RSA ACE/Server and SecurID tokens for secure two-factor authentication. This rule is important because local database users need to securely access the GIAC Database Server.

Rule 3



This rule allows the Management Server to directly access the GIAC Database Firewall for the HTTPS, SSH, and FireWall-1 services. The HTTPS service is used for Voyager access, and the SSH service is used for secure command line access. Both of these protocols will perform user authentication using Nokia IPSO passwords. The FireWall-1 services group includes services such as FW, FW1_mgmt, and FW1_log, and is used for FireWall-1 control connections. This rule is important because, for proper management, the Management Server needs HTTPS, SSH, and FireWall-1 access to the GIAC Database Firewall.

Rule 4



This rule drops and logs all other traffic, and is commonly referred to as the “cleanup” rule. This rule is the implementation of the “deny that which is not explicitly allowed” security policy. Even without the cleanup rule, however, the “implicit drop” rule would drop packets not matched by other rules in the rulebase. The implicit drop rule, however, would not log these packets. Implementing the cleanup rule ensures that all other traffic will be dropped and logged. This rule must be the last rule in the rulebase, because it will catch all remaining traffic.

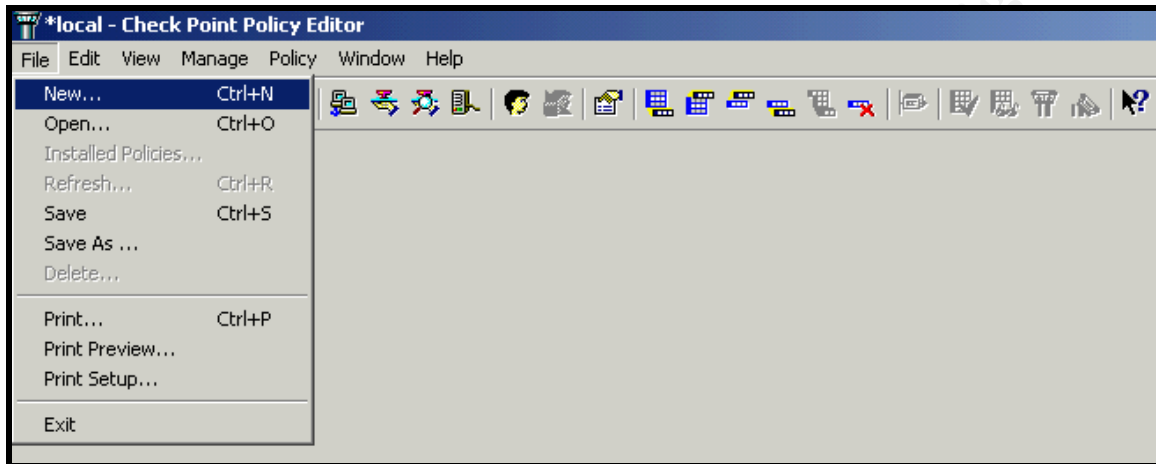
Check Point FireWall-1 Tutorial

While the previous sections displayed completed FireWall-1 rulebases, this section presents a tutorial detailing *how* to create a FireWall-1 rulebase. This section assumes that both the FireWall-1 Management Server and Enforcement Module have been successfully installed, and that the “fw putkey” commands have been properly configured for bi-directional FireWall-1 communication. In addition, this section assumes that the GUI is installed, and that the user has successfully logged into the Management Server. This is a high-level tutorial,

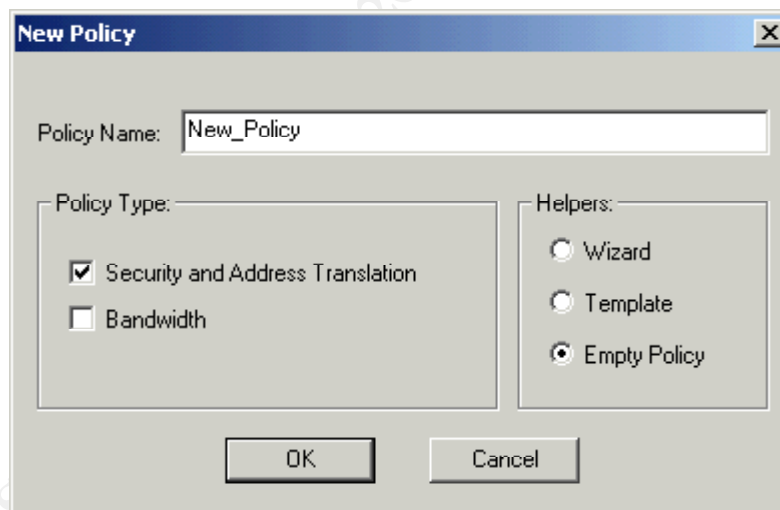
and is not designed to be a comprehensive guide to FireWall-1 installation or configuration. For more detailed information regarding FireWall-1 installation and configuration, see the [Check Point Support Services](#) website [2].

Creating A New Policy

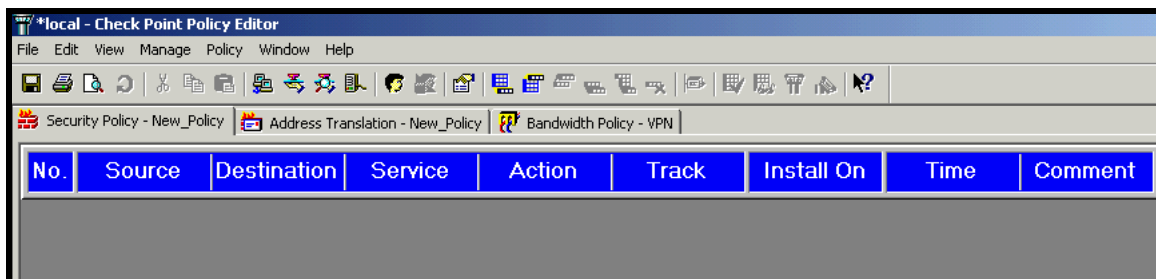
First, select “File | New” to create a new policy:



When prompted, enter the desired policy name, and select “Security and Address Translation” and “Empty Policy”:



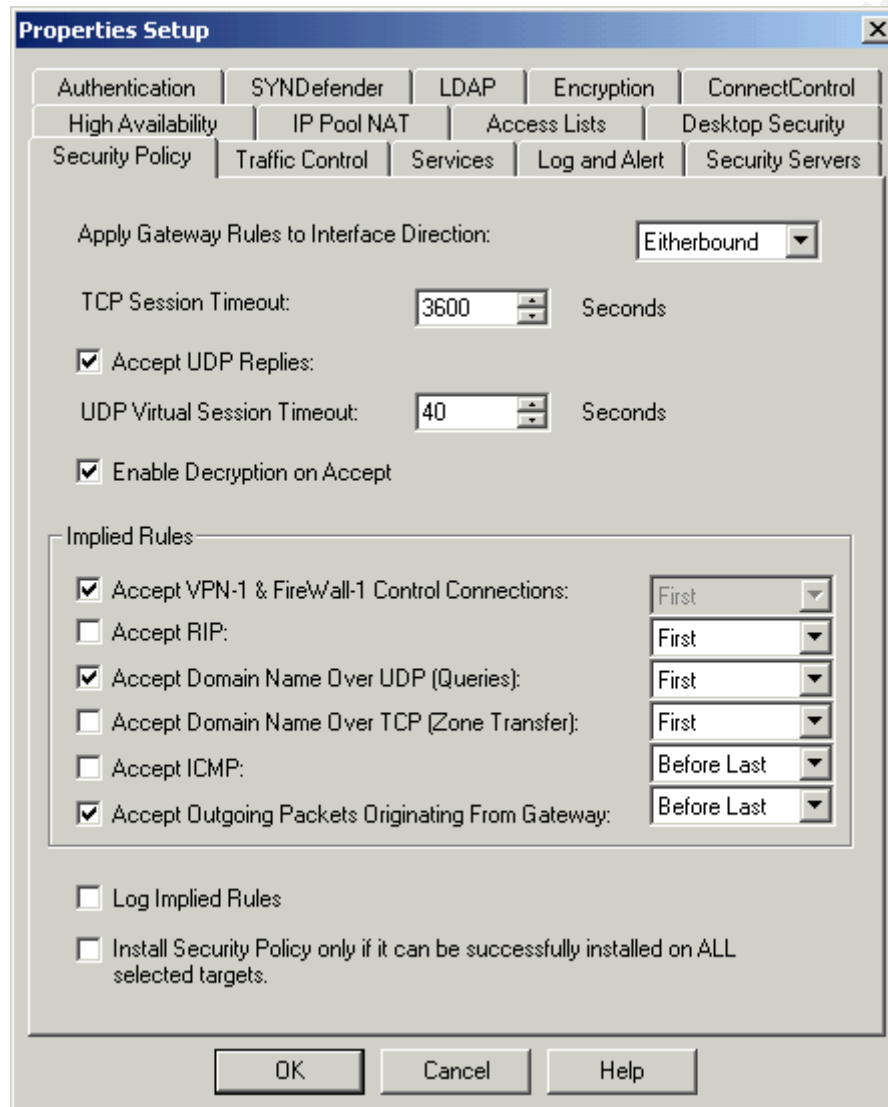
A new policy is created:



The new policy is now ready for configuration.

Configuring Policy Properties

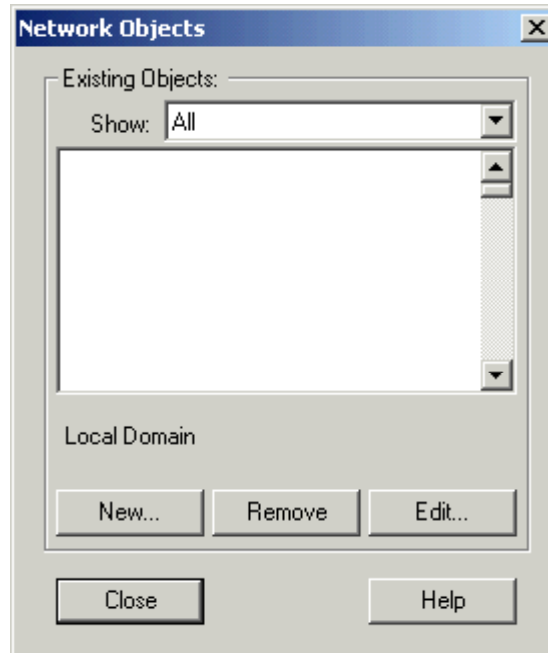
The next step is to configure the policy properties by selecting “Policy | Properties”:



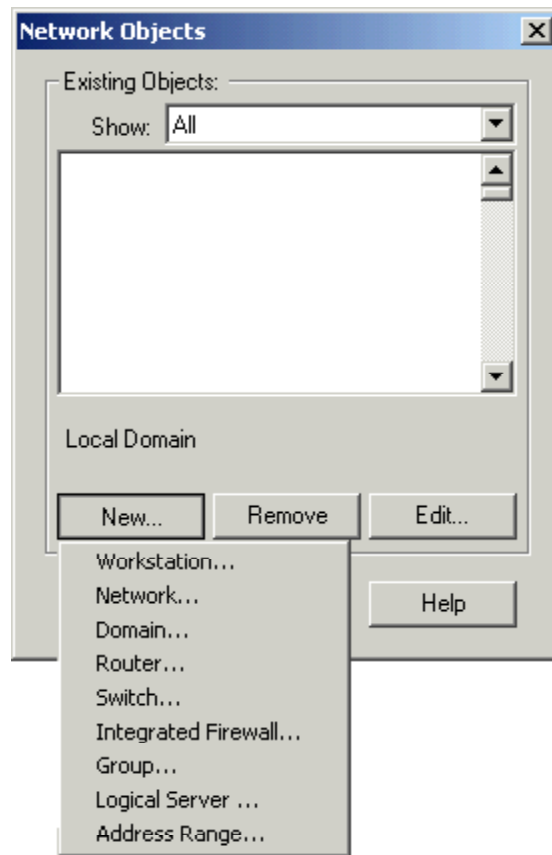
The policy properties are used to quickly generate “implied rules” that commonly appear in rulebases. Select the desired properties. It is important to note that several properties are enabled by default, and these properties will create implied rules in every rulebase. For the sake of security, it is a good practice to disable all of the policy properties, instead creating explicit rules in the rulebase.

Creating Network Objects

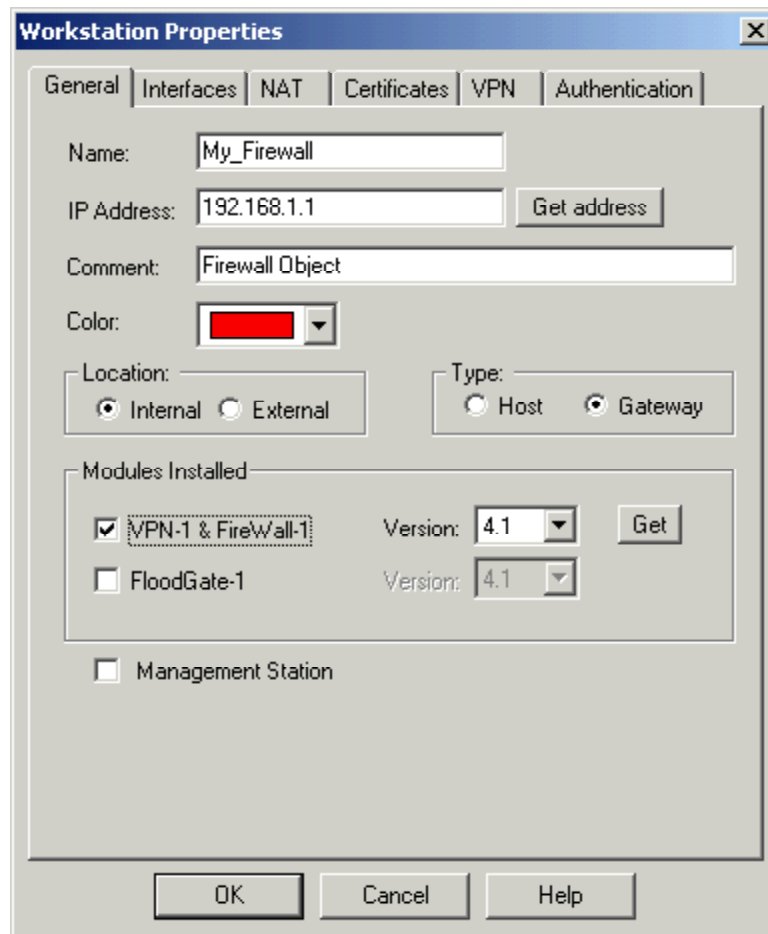
The next step is to create network objects. A network object must be created for every object that appears in the rulebase. To create a network object, select “Manage | Network Objects” to display the “Network Objects” window:



Next, select “New” and choose the type of network object you would like to create:



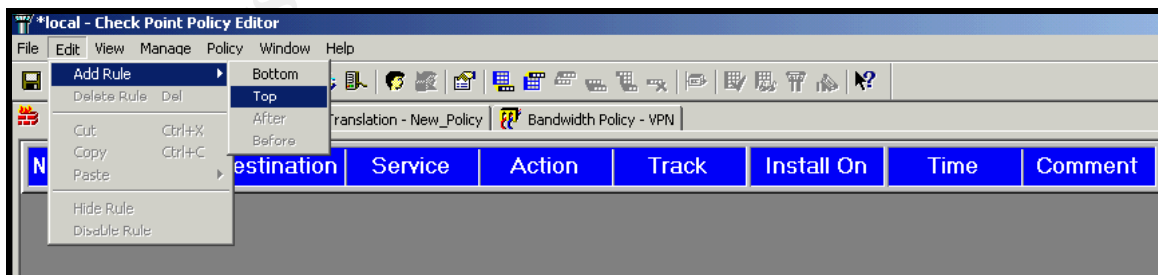
For example, you can create a “Workstation” object for the firewall:



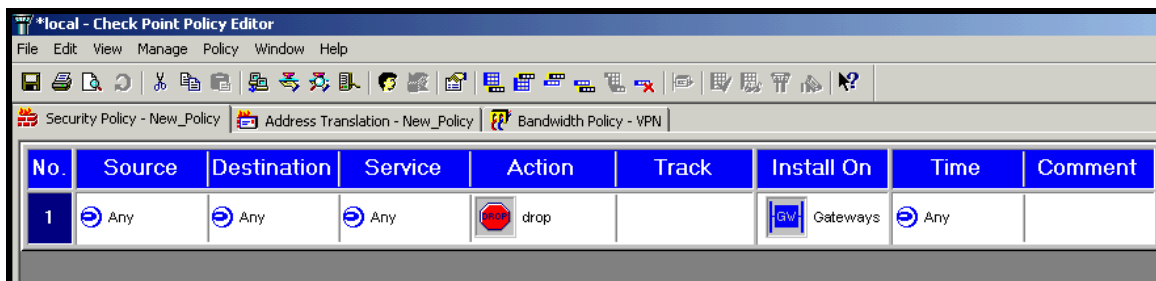
Once you have created all of your network objects, you are ready to create rules.

Creating Rules

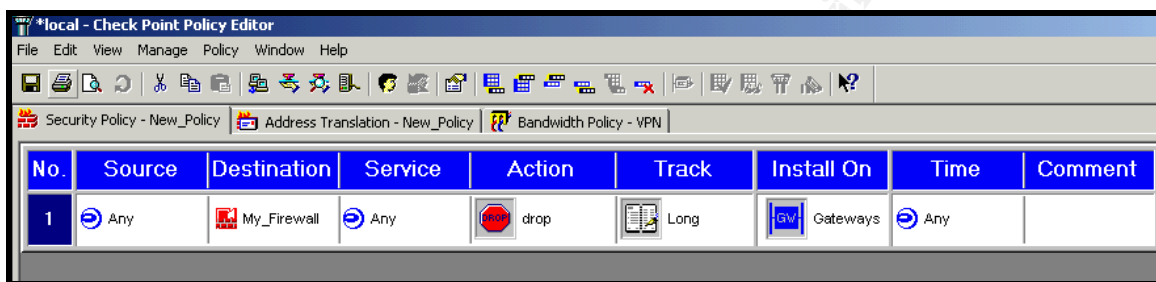
To create a rule, select “Edit | Add Rule” and choose where you want to add the rule:



A new rule is created:



Next, configure the rule by right clicking in each field and selecting the desired options. For example, create the “stealth” rule that prevents direct communication to the firewall:



Once you have created all of your rules, you are ready to push the policy.

Pushing The Policy

To push the policy, select “Policy | Install” and select the desired firewalls to install the policy on. Once you click “OK”, your firewall will be operational! For more information regarding FireWall-1 configuration, see the [Check Point Support Services](#) website [2]. For excellent FireWall-1 troubleshooting information see [Phoneboy's FireWall-1 FAQ](#) [3].

Verify the Firewall Policy

This section details an audit of the implemented security architecture. The freeware network auditing tool “Nmap” is used for the audit. Nmap is the king of port scanners. Nmap is highly flexible, and can scan both TCP and UDP ports. In addition, Nmap supports several different scanning methods, performs ping sweeps, and provides OS detection. Nmap is run from the command line, and has several powerful options. For more information regarding Nmap, see the [Nmap Homepage](#) [4].

Here the “-P0” option specifies not to ping the host before the scan, “-sS” specifies a stealth scan, and “-p 1-1024” specifies to scan TCP ports 1-1024. During a stealth scan, the three-way TCP handshake is intentionally not completed, causing most operating systems to not log the connection. The command performs the port scan and reports what ports are open:

```
root@attacker $ nmap -P0 -sS -p 1-1024 www.giac.com
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on www.giac.com (10.1.1.1):
```

(The 1022 ports scanned but not shown below are in state: closed)

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

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

As you can see, Nmap reports that ports 80 (HTTP) and 443 (HTTPS) are open, while all other ports are closed.

Planning The Audit

For the firewall audit, Nmap will be used to audit the security of several different servers from several different networks. This method of scanning will ensure the security of the firewall from multiple angles. Since the audit will not be intrusive, it can be conducted during business hours. In addition, the audit will not be overly costly or time consuming. This is good, since the audit should be repeated on a regular basis. In fact, the audit can be scripted to automatically run on a regular schedule. The following scans will be conducted:

- The GIAC Main Firewall from the Internet
This scan will ensure that the GIAC Main Firewall is not running any dangerous services, although a few FireWall-1 ports are expected to be open.
- The Extranet Web Server from the GIAC Internal Network
This scan will ensure that only the HTTPS service is accessible on the Extranet Web Server. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.
- The External Database Server from the GIAC Internal Network
This scan will ensure that only the HTTPS service is accessible on the External Database Server. The HTTPS service is the frontend to the database program. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.
- The GIAC Mail Server from the GIAC Internal Network
This scan will ensure that only the SMTP and POP3 services are accessible on the Mail Server. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.
- The GIAC Database Server from the GIAC Internal Network
This scan will ensure that only the HTTPS service is accessible on the GIAC Database Server. The HTTPS service is the frontend to the database program. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.

- An HR Server from the GIAC Internal Network
This scan will ensure that only the HTTPS service is accessible on an HR server, which is located on the GIAC Protected Network. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.
- An Accounting Server from the GIAC Internal Network
This scan will ensure that only the HTTPS service is accessible on an Accounting server, which is located on the GIAC Protected Network. This scan assumes that the user has already authenticated to FireWall-1 using the Session Authentication Agent.

The IP addresses of the GIAC security architecture components are as follows:

Server	IP Address
GIAC Main Firewall (external address)	192.168.0.1
Extranet Web Server	10.1.0.1
External Database Server	10.1.0.2
GIAC Mail Server	10.1.0.3
GIAC Database Server	10.2.0.1
GIAC Accounting Server	10.3.0.1
GIAC HR Server	10.3.0.2

Conducting The Audit

Each scan is now conducted, including a discussion of the results:

The GIAC Main Firewall from the GIAC Internal Network

For this scan, we expect TCP ports 264 and 265 to be open. These ports are used for SecuRemote client-to-site VPN establishment. The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 192.168.0.1
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 192.168.0.1 (192.168.0.1):
(The 1022 ports scanned but not shown below are in state: closed)
```

Port	State	Service
264/tcp	open	http
265/tcp	open	https

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

As we can see, TCP ports 264 and 265 are indeed open. While this indicates to attackers that this machine is running FireWall-1, little can be done to hide these ports. They must be open for SecuRemote to function properly. Other than these ports, the stealth rule ensures that no other ports are accessible. It is still a good idea, however, to manually disable other services that may be running on the firewall.

The Extranet Web Server from the GIAC Internal Network

For this scan, we expect TCP port 443 (HTTPS) to be open. This port is used by the secure webserver. Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed. The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.1.0.1
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.1.0.1 (10.1.0.1):
(The 1023 ports scanned but not shown below are in state: filtered)
```

Port	State	Service
443/tcp	open	https

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

As we can see, TCP port 443 is indeed open. In addition, note that the other ports are all “filtered”. In other words, nmap can detect the GIAC Main Firewall. Specifically, filtered means that “a firewall, filter, or other network obstacle is covering the port and preventing nmap from determining whether the port is open” [5]. As we can see, Nmap provides extremely useful information.

If we had attempted the scan before authenticating, the results would have been different:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.1.0.1
```

```
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
All 1024 scanned ports on (10.1.0.1) are: filtered
```

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

In this case, because the user has not authenticated, all ports appear to be filtered.

The External Database Server from the GIAC Internal Network

For this scan, we expect TCP ports 22 (SSH) and 443 (HTTPS) to be open. These ports are used to administer the server (SSH), and to access the database frontend (HTTPS). Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed.

The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.1.0.2
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.1.0.2 (10.1.0.2):
(The 1022 ports scanned but not shown below are in state: filtered)
```

Port	State	Service
22/tcp	open	ssh
443/tcp	open	https

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

As we can see, TCP ports 22 and 443 are indeed open. All other ports are all filtered. This is exactly what we expected to see.

The GIAC Mail Server from the GIAC Internal Network

For this scan, we expect TCP ports 25 (SMTP) and 110 (POP3) to be open. These ports are used to send (SMTP) and receive (POP3) email. Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed. The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.1.0.3
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.1.0.3 (10.1.0.3):
(The 1022 ports scanned but not shown below are in state: filtered)
```

Port	State	Service
25/tcp	open	smtp
110/tcp	open	pop3

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

As we can see, TCP ports 25 and 110 are indeed open. All other ports are all filtered. This is exactly what we expected to see.

The GIAC Database Server from the GIAC Internal Network

For this scan, we expect TCP port 22 (SSH) and 443 (HTTPS) to be open. These ports are used to administer the server (SSH), and to access the database frontend (HTTPS). Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed.

The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.2.0.1
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.2.0.1 (10.2.0.1):
(The 1022 ports scanned but not shown below are in state: filtered)
```

Port	State	Service
22/tcp	open	ssh
443/tcp	open	https

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

As we can see, TCP ports 22 and 443 are indeed open. All other ports are all filtered. This is exactly what we expected to see.

HR Server from the GIAC Internal Network

For this scan, we expect TCP port 443 (HTTPS) to be open. This port is used by the secure webserver. Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed. The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.3.0.1
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.3.0.1 (10.3.0.1):
(The 1023 ports scanned but not shown below are in state: filtered)
```

Port	State	Service
443/tcp	open	https

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

As we can see, TCP port 443 is indeed open. All other ports are all filtered. This is exactly what we expected to see.

Accounting Server from the GIAC Internal Network

For this scan, we expect TCP port 443 (HTTPS) to be open. This port is used by the secure webserver. Again, we assume that the user has already authenticated to FireWall-1 using the Session Authentication Agent. Otherwise, the scan will timeout waiting for authentication to commence, and all scanned ports will register as closed.

The results of the scan follow:

```
root@attacker $ nmap -P0 -sS -p 1-1024 10.3.0.2
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )
Interesting ports on 10.3.0.2 (10.3.0.2):
(The 1023 ports scanned but not shown below are in state: filtered)
```

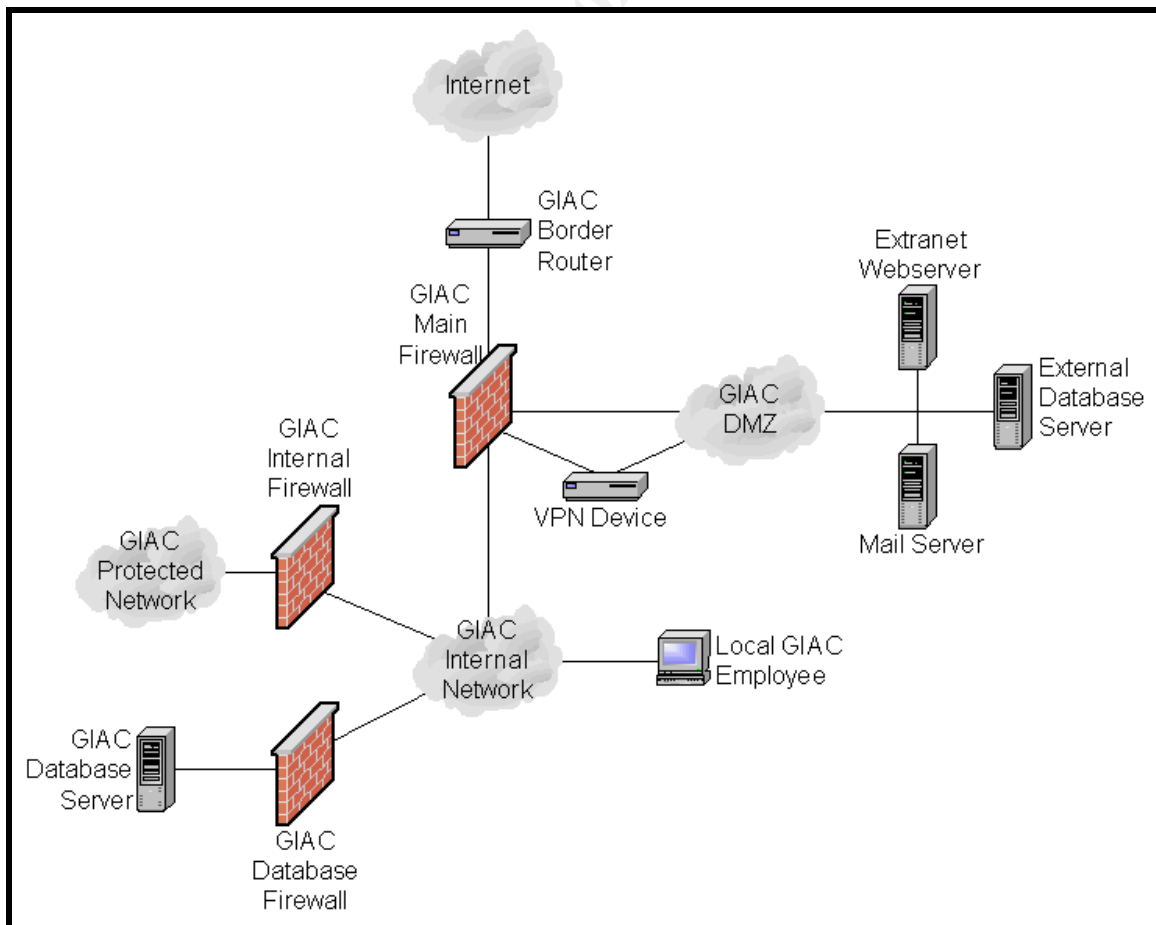
Port	State	Service
443/tcp	open	https

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

As we can see, TCP port 443 is indeed open. All other ports are all filtered. This is exactly what we expected to see.

Evaluating The Audit

As you can see, the GIAC network is currently quite secure. Only the ports that need to be accessible are open. All other ports are closed. One weakness of the security architecture, however, is that the GIAC Main Firewall is easily identified as a FireWall-1 firewall by the ports that are open (TCP ports 264 and 265). One possible improvement to the architecture would be to implement a dedicated VPN device to handle all VPN traffic:



Notice that the VPN device is placed between the firewall and the GIAC DMZ. This architecture offers several advantages:

- TCP ports 264 and 265 can be closed on GIAC Main Firewall, further hiding the firewall from attackers
- The VPN Device would handle the encryption and decryption of VPN traffic, greatly reducing the load on the firewall
- An encryption license would not have to be purchased for the GIAC Main Firewall, greatly reducing cost

If this improvement were implemented, an external scan of the firewall would produce the following results:

```
root@attacker $ nmap -P0 -sS -p 1-1024 192.168.0.1
```

```
Starting nmap V. 2.54BETA32 ( www.insecure.org/nmap/ )  
All 1024 scanned ports on (192.168.0.1) are: closed
```

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

As we can see, all ports on the GIAC Main Firewall are now closed. Even without this improvement, however, the GIAC network is quite secure. Just because the GIAC network is secure now, however, does not necessarily mean it will be secure in the future. Security is dynamic. Consequently, this audit should be repeated on a regular basis. As previously mentioned, the audit can be scripted and run on a regular schedule.

Design Under Fire

This section analyzes the security architecture of another GSFW practical. For my analysis, I chose Edmond Chiu's practical [6]. Edmund employs Check Point FireWall-1 to protect his network. If installed correctly, FireWall-1 is very secure. If older, unpatched versions of FireWall-1 are installed, however, FireWall-1 may be vulnerable to several exploits. The following sections describe three kinds of attacks against Firewall-1:

- An attack against the firewall itself
- A Denial of Service (DoS) attack
- An attack through the firewall

Each attack is described in detail, including links to appropriate tools. In addition, reconnaissance (what must be done before the attack) and detection (what will happen after the attack) will be discussed.

An Attack Against The Firewall Itself – Attacking FWN1 Authentication

This attack targets the firewall itself. Specifically, the internal authentication mechanisms of FireWall-1 are attacked. At the 2000 Blackhat Briefings, the paper “A Stateful Inspection of FireWall-1” was released. This paper details several vulnerabilities with FireWall-1 operation, including this authentication attack [7].

By default, FireWall-1 versions 4.0 and 4.1 use the FWN1 authentication mechanism for authentication between the Management Server and Enforcement Module. As described in the “A Stateful Inspection of FireWall-1” paper, FWN1 works as follows [7]:

1. The “fw putkey” command is used to establish the secret key, called K, on both the Enforcement Module and the Management Server
2. The Enforcement Module generates a random number, called R1
3. The Enforcement Module signs R1, so $S1 = \text{hash}(R1, K)$
4. The Enforcement Module sends R1 and S1 to the Management Server
5. The Management Server verifies S1 using the same hash() function
6. The Management Server generates a random number, called R2
7. The Management Server signs R2, so $S2 = \text{hash}(R2, K)$
8. The Management Server sends R2 and S2 to the firewall module

The FWN1 authentication scheme can be broken, however, with a replay attack. Instead of generating R2 and calculating the signature S2, an attacker could simply reuse the R1 and S1 values sent by the Enforcement Module. The attacker would be authenticated by the Enforcement Module, and could then unload the policy, or install a custom policy. An attacker’s custom policy might look something like this [7]:

No.	Source	Destination	Service	Action	Track
1	 Any	 Any	 Any	 accept	

This policy would accept all traffic, and would not perform any logging whatsoever. In response to this vulnerability (among several others), Check Point released FireWall-1 4.1 SP2, which patched all of the vulnerabilities detailed in the “A Stateful Inspection of FireWall-1” paper. Consequently, only versions of FireWall-1 older than 4.1 SP2 are vulnerable to this exploit. As a result, the attacker must find a firewall running an older version of FireWall-1.

Once the attacker has found an older version of FireWall-1, the FWN1 authentication vulnerability can be exploited with the “fw1fwn” program. This utility is included on the “A Stateful Inspection of FireWall-1” website. The

fw1fwn program simply unloads the firewall policy from the target firewall, but the source code can be modified to install a custom policy. Unless FireWall-1 is patched to version 4.1 SP 2, this attack will succeed, and the attacker will control the firewall. To run the exploit, simply compile and run fw1fwn with the IP addresses of the Enforcement Module and Management Server. Assuming the Enforcement Module is 192.168.0.1 and the Management Server is 10.1.0.10, the exploit would be executed as follows:

```
root@attacker $ ./fw1fwn 192.168.0.1 10.1.0.10
```

At this point, the attacker can install any desired policy on the firewall. In addition, the attacker can disable FireWall-1 logging. Depending on the previous rulebase and/or operating system configuration, the attack itself may or may not have been logged by FireWall-1 and/or the operating system. If the attack was logged, the attacker will not be able to modify or delete these logs without further exploiting the firewall. In addition, it is possible that an Intrusion Detection System (IDS) could recognize the attack, and send an alert. The IDS could be bypassed, however, by using packet fragmentation or other IDS evasion techniques. To prevent this attack altogether, FireWall-1 4.1 SP2 or later should be installed.

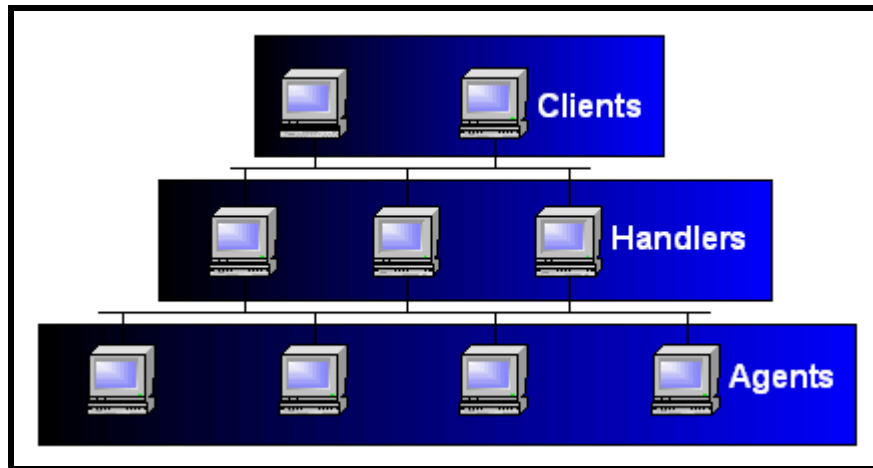
In addition to this vulnerability, the FWN1 authentication scheme does not provide encryption or data integrity. Theoretically, an attacker could also use a TCP hijacking tool such as “hunt” to compromise an authenticated connection between a Management Server and Enforcement Module. Hunt is a TCP hijacking tool that can be used not only to eavesdrop on connections, but also to take over connections. After the connection is hijacked, the attacker can inject arbitrary commands [8].

A DoS Attack – Stacheldraht

This attack is a DoS attack against the firewall and the networks that it protects. The tool used for this attack is the Distributed DoS (DDoS) program “stacheldraht”, which is German for “barbed wire”. Stacheldraht uses a distributed architecture to launch DoS attacks, composed of three layers [9]:

- Clients
The Clients control the Handlers
- Handlers
The Handlers are the “master” programs, and control the Agents
- Agents
The Agents are the “daemon” programs, and are controlled by the Handlers

The distributed architecture is as follows:



First, many systems are compromised using arbitrary vulnerabilities. Next, the stacheldraht Agent is installed on these compromised hosts. Finally, the Handlers instruct the many Agents to launch the actual DoS attacks against the target host. The target host is besieged by the massive amount of traffic generated by the agents, and quickly becomes overwhelmed.

The Client is executed using the “client” program:

```
root@attacker $ ./client 192.168.0.2
[*] stacheldraht [*]
(c) in 1999 by ...
trying to connect...
connection established.
-----
enter the passphrase :
```

After entering the passphrase, the client enters interactive mode. In interactive mode, commands can be issued to control Agents. This includes the “.mdos” command, which is used to actually launch the DoS attack. The Handler is executed using the “mserv” program, and the Agent is executed using the “td” program. Both programs have command line interfaces similar to the “client” program.

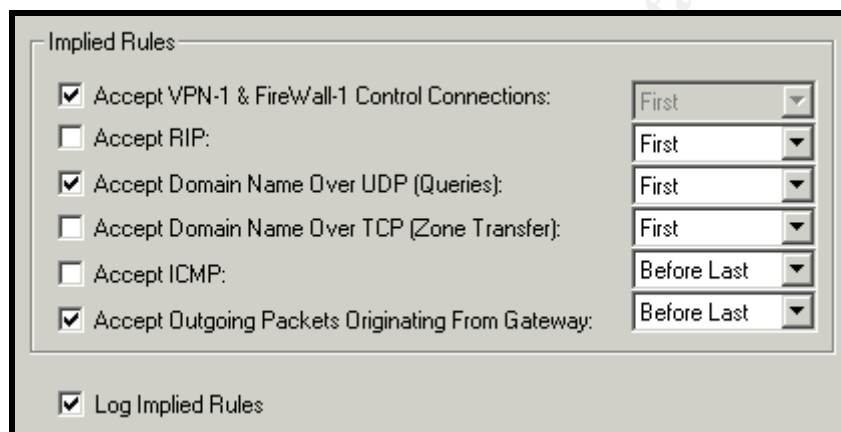
Very little reconnaissance is necessary before launching a DDoS attack. It would help to know the bandwidth of the firewall’s connections, but if enough Agents are deployed, the attack will most likely be successful regardless. When a DDoS attack such as stacheldraht is launched, intermediate routers and gateways will all log the attack, assuming they are logging traffic. The success of stacheldraht, however, is not dependent on stealthiness. Whether or not the attack is logged, it will most likely be successful. Intermediate IDS systems may recognize the attack, but that will not hinder stacheldraht’s effectiveness.

Edmond’s security architecture, like most, would most likely be susceptible to

the stacheldraht DDoS attack. It's a simple fact that, given enough traffic, any link can be saturated. There is no easy way to prevent DDoS attacks such as stacheldraht. One solution is to improve the security of servers in general, thereby making it more difficult to compromise those servers and install stacheldraht Agents. If a server administrator suspects that stacheldraht is running on their network, they can use the Perl script "gag" to determine whether or not their servers have been compromised [9].

An Attack Through The Firewall – Attacking DNS

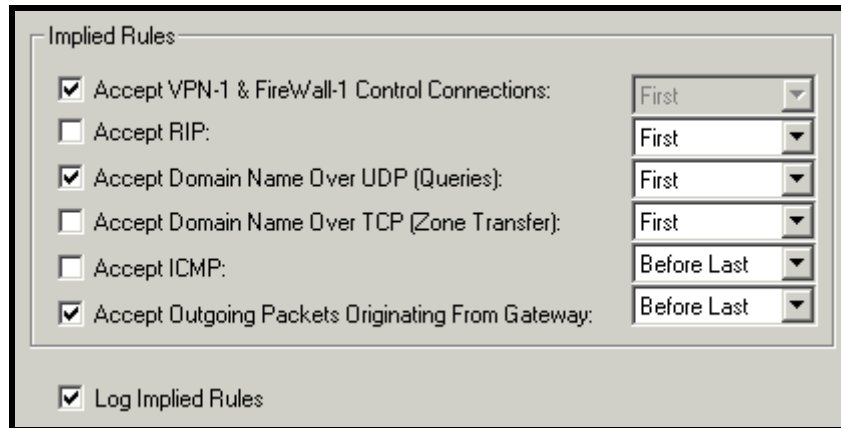
This attack targets another system through the firewall. Specifically, an internal system running DNS is attacked. By default, earlier versions of FireWall-1 (including some versions of 4.1) shipped with DNS lookups enabled in the implied rules configuration of the policy properties:



Notice that the "Accept Domain Name Over UDP (Queries)" property is enabled. This option is enabled to automatically accept client DNS requests, but has dire implications on the security of the firewall. This configuration accepts *all* DNS lookup traffic, *both* outbound and inbound. This allows attackers to pass DNS traffic through the firewall to any Internet accessible servers. If the internal network is publicly addressed, all servers and user workstations will be accessible. If the internal network is privately addressed, any servers or user workstations configured for static Network Address Translation (NAT) will be accessible. With this access to DNS lookups, it may be possible to exploit BIND, which has historically been plagued by security holes. Websites such as [Packet Storm](#) catalog a variety of BIND exploits [10]. And once one server has been compromised, it can be used as a stepping stone to launch attacks against other servers.

Before launching this attack, the attacker must locate a firewall that is running an older version of FireWall-1. By sending inbound DNS queries to known servers with a tool such as Nmap, the attacker should be able to discern if the "Accept Domain Name Over UDP (Queries)" property is checked. If it is, the attacker can then begin to search internal hosts for the DNS service. If a vulnerability is found, a corresponding exploit can usually be found at [Packet Storm](#) [10].

If an exploit is successful, it will only be logged by FireWall-1 if the “Log Implied Rules” property is enabled:



In this case, the exploit would be logged. In addition, the exploit may be logged by the target system. If the exploit is successful, however, the attacker will most likely edit the target system's logs, removing any evidence of the attack. To prevent this type of attack altogether, simply disable the “Accept Domain Name Over UDP (Queries)” property. In fact, it is a good practice to disable all of implied rules in the policy properties, instead creating explicit rules in the rulebase.

References

1. Various authors. "Improving Security on Cisco Routers." 1 May 2002.
<http://www.cisco.com/warp/public/707/21.html>.
2. Various authors. "Check Point Support Services." 8 April 2002.
<http://www.checkpoint.com/techsupport/index.html>.
3. Phoneboy. "Phoneboy's FireWall-1 FAQ." 17 May 2002.
<http://www.phoneboy.com/>.
4. Fyodor. "Nmap Network Security Scanner." 17 May 2002.
<http://www.insecure.org/nmap/>.
5. Fyodor. "Nmap Network Security Scanner Man Page." 17 May 2002.
http://www.insecure.org/nmap/nmap_manpage.html.
6. Chiu, Edmond. "GCFW Practical." 21 March 2002.
<http://www.giac.org/GCFW.php>.
7. Lopatic, Thomas, John McDonald, and Dug Song. "A Stateful Inspection of FireWall-1." 9 August 2000. <http://www.phoneboy.com/docs/bh2000/>.
8. Krauz, Pavel. "HUNT Project". 17 May 2000.
<http://lin.fsid.cvut.cz/~kra/index.html#HUNT>.
9. Dittrich, David. "The 'stacheldraht' Distributed Denial of Service Attack Tool." 31 December 1999. <http://www.sans.org/y2k/stacheldraht.htm>.
10. Various authors. "Packet Storm". 17 May 2000.
<http://packetstormsecurity.nl/>.