Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment
Version 1.6a (revised October 26, 2001)

SANS East Conference 2001, Washington DC November 2001

"Secure e-Fortunes"

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

January 28, 2002
Angela R. Latimer

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table of Content

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

I. Security Architecture (15 points)

Entity Communications.

GIAC Enterprises is an e-business which deals in the online sales of fortune cookie *sayings*. In this business, they have several "entities" to deal with and protect their infrastructure from:

- Their *customers* order and purchase bulk online fortune cookie sayings via their web browsers using SSL. SSL allows communications between the web browser and the "customer" web server to be encrypted. GIAC's customer web server has a trusted 128-bit server-side certificate from Verisign. By specifying this type of certificate, the customers' web browser must be able to support the 128-bit encryption, instead of the standard 40-bit encryption.
- Their *suppliers* are the authors of the fortune cookie sayings and require access to the "fortune cookie jar" i.e. database. Since direct database access is **not** needed and no other major communications is required between the entities, SSL will suffice for their connections. Their web browsers will connect to a specified "supplier" web server via a 128-bit SSL connection. *Client-side certificates*, issued by Verisign, will also be required for authentication for each supplier. After authentication is successful, they may submit their *sayings* and they will be sent to the backend database in the internal network. Verisign issued *Client-side certificates* are a GIAC requirement for all suppliers and potential suppliers. GIAC's supplier web server has a trusted 128-bit server-side certificate from Verisign.
- Their *partners* (both domestic and international) require access to translate and resell the fortune sayings. Business partners will have the ability to directly access the internal database. Additional internal resource access, including the exchange of sensitive information, may be required. To accommodate this need, a VPN tunnel through the Internet using IPSEC with ESP will be setup to allow encrypted communications between them.
- Their *employees* have access to restricted resources within their internal network based on their job function. Most employees are also able to access the Internet via http/https with content filtering on their requests. Telnet and FTP are not allowed to internal or external resources. SSH is used where these options are necessary by administrators only. POP3 mail is not allowed since each individual is issued an internal Lotus Notes account. Internet mail, i.e. Yahoo and Hotmail, is not allowed and filtered. Internal modems are not allowed on workstations or servers for remote administration.
- The *employees* that require *remote access* from various locations use a company-issued laptop with a VPN client utilizing IPSEC with split-tunneling **disabled.** Disabling split-tunneling helps prevent an ISP's Internet traffic from flowing through the VPN tunnel into GIAC's internal network. These users also have a personal firewall installed on their laptops.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Architecture Design.

GIAC's internal infrastructure design consists of filtering routers, firewalls, virtual private networks, and intrusion detection systems.

With this equipment, a layered architecture will be formed. The first layer will consist of a **Cisco (model 3640) border router running IOS 12.2** for packet filtering and protecting the entrance to the internal infrastructure from the Internet. (Nested filtering routers will also be used to help protect the internal network as well.) The second layer consists of a **Solaris 7 Checkpoint FW-1 v4.1 Service Pack 5** firewall for stateful packet filtering possibly missed by the Cisco border router. In addition to this, the firewall will also handle network address translation (NAT) functions and remote VPN clients, not including business partners. VPN connections to business partners will be setup in tunnel mode (gateway-to-gateway) between Cisco routers (one at GIAC and the other at the business partner). GIAC will use a separate **Cisco (model 3620) router running IOS 12.2** to handle all VPN connections separate from the Internet border router.

Other equipment used to secure the internal infrastructure includes:

- **Internal router (Cisco 2621 IOS 12.2)** to filter certain internal users from accessing unnecessary resources, i.e. financial information, etc.
- **Intrusion detection systems** utilizing **ISS RealSecure v6.01** (External) and **SNORT v1.8.3** (Internal), both Network IDSes (NIDS), will be used to alert when suspicious activity occurs at different points within the network infrastructure. The **ISS RealSecure NIDS** will be setup in "stealth mode" with **no** ip address on the monitoring interface for traffic to/from the Internet. A second interface will be connected to the internal network to communicate information back to the reporting console.
- **Content Filtering** will be handled by **Surf Control v3.0.3** to ensure *appropriate* websites are visited by internal users. All website traffic will be logged and inappropriate URL requests are redirected to GIAC's company "web policy" page.
- **Antivirus software** from **McAfee including GroupShield 5.0 and VirusScan 4.5** will be installed and frequently updated on mail servers and client workstations, respectively.
- GIAC is implementing a ***split* DNS** architecture with an Internal and External DNS Server that operate independently of each other. Both DNS servers are running **BIND v8.3.0**, http://www.isc.org/products/BIND/. Zone transfers are **not** allowed between the Internal and External DNS, so as not to reveal internal IP information to the Internet. Also, the Internal DNS will do lookups on behalf of the internal users and DMZ servers, with the exception of the External DNS Server itself, when necessary. The External DNS Server will not be able to resolve internal addresses.
- GIAC is implementing **Sendmail v8.12.1** on their External SMTP Server as advised by http://www.sendmail.org/. This server *only* relays mail for the GIAC domain; it is not an "open" relay for potential spamming.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Internal VPN Tunneling** is used between the Ecommerce DMZ Web Servers and WebSphere and also between WebSphere and MS SQL Server (Customer/Supplier Web Servers (IIS 5.0) <--->WebSphere v3.5.4<--->MS SQL Server 2000). IPSEC with ESP will be used to prevent credit card and other sensitive information from being sniffed while en route from the supplier or customer web server to the internal database server (transport mode – host to host). All of the above servers are running Windows 2000 Advanced Server with the latest Service Patch for the OS and the application it supports.

Device To IP Mapping:

Device/Interface:	**IP Address/Network Bits:**
Border Router (Cisco 3640)	
Ethernet 0/0 (To Internet)	30.x.x.1/29
Ethernet 0/1 (To Firewall)	30.x.x.9/29
Ethernet 0/2 (To VPN Gateway)	30.x.x.17/29
Firewall and NAT (Checkpoint FW-1)	
E0 (To Border Router)	30.x.x.10/29*
E1 (To DMZ)	30.x.x.33/28
E2 (To Ecommerce DMZ)	30.x.x.49/28
E3 (To VPN Gateway)	30.x.x.25/29
E4 (To Internal Router)	10.x.x.1/29
E5 (To Application DMZ)	10.x.x.9/29
VPN Gateway (Cisco 3620)	
Ethernet 0/0 (To Border Router)	30.x.x.18/29
Ethernet 0/1 (To Firewall)	30.x.x.26/29
Internal Router (Cisco 2621)	
Ethernet 1/1 (To Firewall)	10.x.x.2/29
Fast Ethernet 0/0 (To Internal Server Network)	10.x.x.17/28
Fast Ethernet 0/1 (To Internal User Network)	10.x.x.129/25
Ecommerce DMZ	
Supplier WWW **IIS 5.0**	30.x.x.50/28
Customer WWW **IIS 5.0**	30.x.x.51/28
Application DMZ	
WebSphere **v3.5.4**	10.x.x.10/29
DMZ	
External DNS **BIND v8.3.0**	30.x.x.34/28
External SMTP Server **Sendmail 8.12.1**	30.x.x.35/28
WWW Server **IIS 5.0**	30.x.x.36/28
Internal Server Network	
Internal DNS **BIND v8.3.0**	10.x.x.18/28
Lotus Notes Server **v5.0.3**	10.x.x.19/28
MS SQL Server **2000 SP2**	10.x.x.20/28
Syslog Server	10.x.x.21/28
Internal User Network	

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Administrator System 1	10.x.x.130/25
Administrator System 2	10.x.x.131/25
Business Partner VPN Gateway (Cisco 3620)	
External Interface	14.x.x.1/29
Business Partner Internal Network	12.x.x.x/24

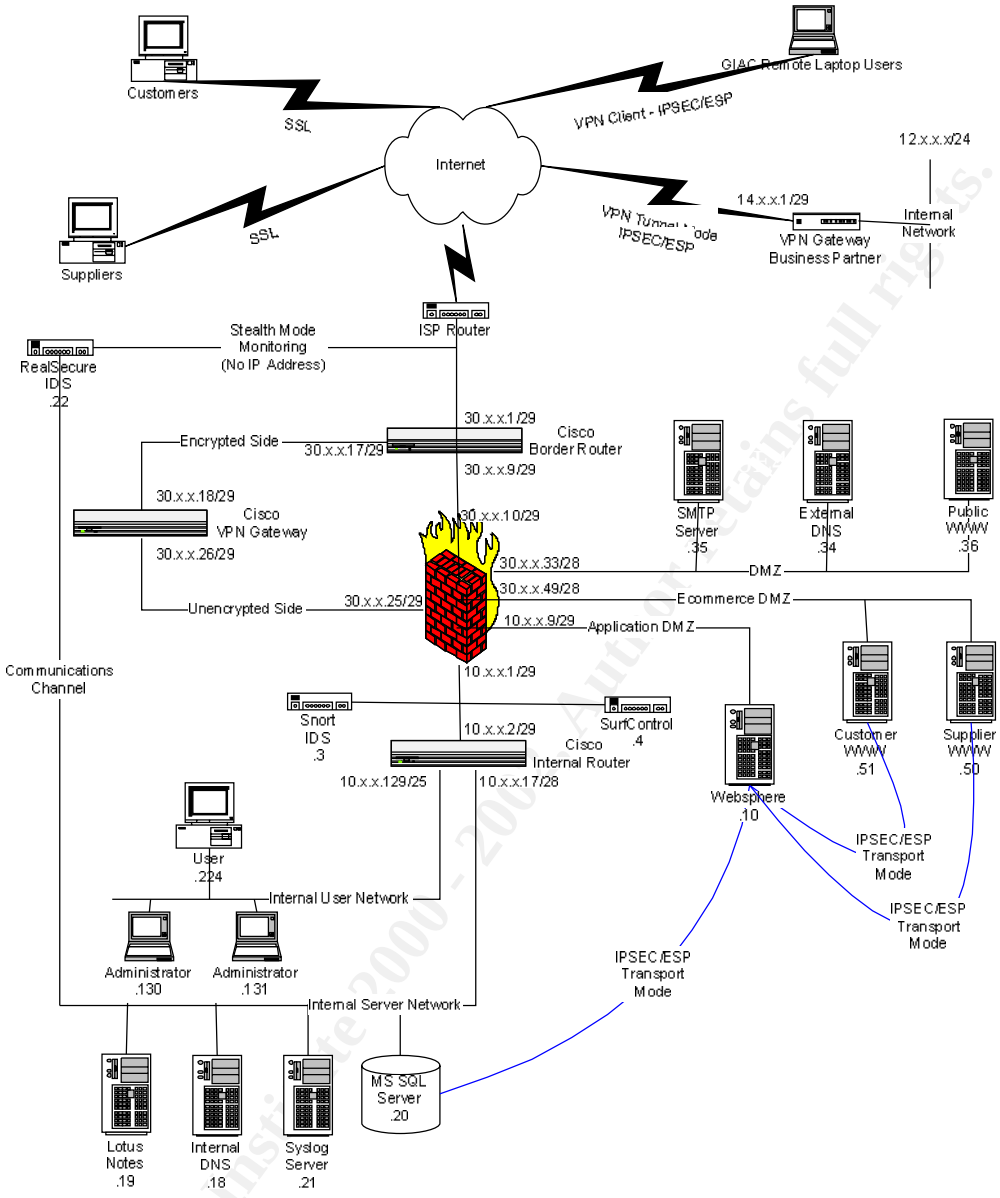
Note: *10.x.x.x addresses* are only used within the GIAC environment and not on *Partner* networks. Therefore, network address translation is not required for internal packets through the IPSEC tunnel. Proper (static) routing is in place to handle *Partner* to GIAC, and vice versa, VPN communications.
**10.x.x.x internal addresses* destined for the Internet will be natted to 30.x.x.10, which is the outside interface of the firewall.

Subnet Bits To # Useable Hosts Per Subnet

- 30 bits = 2 hosts
- 29 bits = 6 hosts
- 28 bits = 14 hosts
- 25 bits = 126 hosts
- 24 bits = 254 hosts

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

II. Security Policy (35 points)

Border Router Security Policy.

The border router selected to protect the entrance to GIAC's network is a **Cisco 3640 IOS 12.2**. This router will handle packet filtering at the *network* and *transport* layers. In addition to using *extended access control lists* (ACLs), there are some services that should be disabled to help *harden* the device against simple attacks.

Border Router Hardening:

In addition to checking the BUGTRAQ, CERT, CVE, etc. websites for the latest vulnerabilities and patches for our border router, there are some additional router hardening techniques that should be implemented. Below is a collection of commands that may be applied at the global configuration or interface level.

References:
http://www.sans.org/infosecFAQ/netdevices/disabling.htm
http://Pasadena.net/cisco/secure.html

- *CDP (Cisco Discovery Protocol)* Disable cisco discovery protocol to prevent additional router and neighboring router information from being revealed.
  - no cdp run
  - no cdp enable
- *TCP and UDP Small Services* Disable tcp and udp non-routable services typically used for diagnosis purposes, i.e. echo, chargen, which can be easily exploited for attack purposes.
  - no service tcp-small-servers
  - no service udp-small-servers
- *Finger* Disable this service to prevent an attacker from identifying who is currently accessing the router
  - no service finger
- *Bootp Server* Disable this service to prevent auto-configuration of network devices
  - no ip bootp server
- *IP Source Routing* Disable this protocol to help prevent spoofing of network paths
  - no ip source-route
- *Proxy ARP* Disable this service to prevent internal addresses from being revealed to an attacker
  - no ip proxy-arp
- *IP Directed Broadcast* Disable directed broadcasts to help prevent an amplification point via a DoS attack
  - no ip direct-broadcast
- *Classless Routing* Disable this protocol to prevent super-net routing
  - no ip classless
- *IP Unreachables* Disable this service to prevent the router from sending valuable ICMP information to an attacker.
  - no ip unreachables

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Redirects* Disable this service to prevent another path from being selected if the default path is not valid.
    - no ip redirects
- *NTP* Disable this service to prevent misuse by an attacker. This service is not needed.
    - ntp disable
- *SNMP* Disable this service to prevent releasing router specific information
    - no snmp-server
- *PAD-X.25* Disable this service because it is not needed
    - no service pad
- *Maintenance Operation Protocol (MOP)* Disable this service because it is not needed
    - no mop enabled
- *HTTP Server* Disable this service to prevent an attacker from accessing the router via a web browser
    - no ip http server
- *Encryption of the "Enable" password* The **service password-encryption** command is primarily useful for preventing unauthorized individuals from viewing your password *(in clear text)* in your configuration file. The **enable secret password** command allows the enable secret password to be stored using a non-reversible cryptographic function.
    - service password-encryption
    - enable secret password
- *Banner Warning* This is used to display GIAC's legal disclaimer for accessing their equipment
    - banner login # <message> #
    - banner incoming # <message> #
    - motd # <message> #
- *Logging to Syslog Server* This allows an external server to log important information pertaining to the router
    - logging 10.x.x.21
- *Setup SSH on VTY ports* This prevents non-SSH connections on the virtual terminal connections, non-SSH including telnets will be explicitly refused.
    - transport input ssh

Border Router Access Control List:

The border router will consist of 3 interface connections: [1]an Internet connection, [2]a Firewall connection and [3] a VPN connection *(encrypted traffic side)*. Each of these connections will have inbound *extended* access control lists. Proper routing is in place to differentiate between VPN traffic to business partners and traffic outbound to the Internet.

Reference:
http://www.cisco.com
SANS GCFW Training Material

[1]Internet Connection:
(Blocking of Absolutes, including but not limited to unnecessary traffic/noise)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

interface Ethernet 0/0
ip address 30.x.x.1 255.255.255.248
no ip direct-broadcast
no ip redirects
no ip proxy-arp
access-group 100 in

DENY:

!Anti-spoofing internal addresses:
access-list 100 deny ip 30.x.x.x 0.0.0.255 any log

!RFC-1918/IANA Source IP Addresses:
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.16.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log

!Historical loopback and loopback:
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log

!Link Local Networks (Used by Microsoft systems when DHCP fails)
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log

!Test-Net network
access-list 100 deny ip 192.0.2.0 0.0.0.255 any log

!Class D Multicast
access-list 100 deny ip 224.0.0.0 0.255.255.255 any log

!Class E Reserved
access-list 100 deny ip 240.0.0.0 0.255.255.255 any log

!Unallocated
access-list 100 deny ip 248.0.0.0 0.255.255.255 any log

!Broadcast
access-list 100 deny ip 255.255.255.255 0.0.0.0 any log

!Host without an IP Address
access-list 100 deny ip host 0.0.0.0 any log

!Explicitly Allowed Services
access-list 100 permit tcp any host 30.x.x.36 80 ! HTTP - Public Web Server
access-list 100 permit tcp any host 30.x.x.50 443 !HTTPS – Supplier Web Server
access-list 100 permit tcp any host 30.x.x.51 443 !HTTPS – Customer Web Server
access-list 100 permit tcp any host 30.x.x.50 80 !HTTP – Supplier Web Server
access-list 100 permit tcp any host 30.x.x.51 80 !HTTP – Customer Web Server
access-list 100 permit tcp any host 30.x.x.35 25 !SMTP

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

access-list 100 permit udp any host 30.x.x.34 53 !DNS

!Explicitly Denied Services
access-list 100 deny tcp any any range 23 log ! Telnet
access-list 100 deny udp any any range 23 log
access-list 100 deny tcp any any range 20 21 log ! FTP
access-list 100 deny udp any any range 20 21 log
access-list 100 deny tcp any any range 69 log ! TFTP
access-list 100 deny udp any any range 69 log
access-list 100 deny tcp any any range 512 514 log ! Syslog
access-list 100 deny udp any any range 512 514 log
access-list 100 deny tcp any any range 111 log !sunrpc
access-list 100 deny udp any any range 111
access-list 100 deny tcp any any range 161 162 log ! Snmp
access-list 100 deny udp any any range 161 162 log

!Deny connection directly to Border Router Interfaces:
access-list 100 deny ip any host 30.x.x.1 log
access-list 100 deny ip any host 30.x.x.9 log
access-list 100 deny ip any host 30.x.x.17 log

!Firewall Interfaces:
!Permit includes return traffic for natted addresses and VPN clients
access-list 100 permit ip any host 30.x.x.10 log !Border to Firewall
access-list 100 deny ip any host 30.x.x.33 log !DMZ to Firewall
access-list 100 deny ip any host 30.x.x.49 log !Ecommerce DMZ to Firewall
access-list 100 deny ip any host 30.x.x.25 log !VPN to Firewall
access-list 100 deny ip any host 30.x.x.57 log !IDS to Firewall
access-list 100 deny ip any host 10.x.x.1 log !Internal to Firewall
access-list 100 deny ip any host 10.x.x.9 log !Application DMZ to Firewall

!VPN Router Interfaces:
access-list 100 permit ip host 14.x.x.1 host 30.x.x.18 log !Allow Business Partner VPN
access-list 100 deny ip any host 30.x.x.18 log
access-list 100 deny ip any host 30.x.x.26 log

!Deny all other traffic

- access-list 100 deny any any

[2]Firewall Connection:
interface Ethernet 0/1
ip address 30.x.x.9 255.255.255.248
no ip direct-broadcast
no ip redirects
no ip proxy-arp
access-group 101 in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

!RFC-1918/IANA Source IP Addresses:
access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log

!Historical loopback and loopback:
access-list 101 deny ip 0.0.0.0 0.255.255.255 any log
access-list 101 deny ip 127.0.0.0 0.255.255.255 any log

!Link Local Networks (Used by Win98 systems when DHCP fails)
access-list 101 deny ip 169.254.0.0 0.0.255.255 any log

!Test-Net network
access-list 101 deny ip 192.0.2.0 0.0.0.255 any log

!Class D Multicast
access-list 101 deny ip 224.0.0.0 0.255.255.255 any log

!Class E Reserved
access-list 101 deny ip 240.0.0.0 0.255.255.255 any log

!Unallocated
access-list 101 deny ip 248.0.0.0 0.255.255.255 any log

!Permit all other traffic
access-list 101 permit any any

[3]VPN Connection:
interface Ethernet 0/2
ip address 30.x.x.17 255.255.255.248
no ip direct-broadcast
no ip redirects
no ip proxy-arp
access-group 102 in

!Allow only tunnel mode VPN traffic through
!Add similar ACLs for additional business partners
access-list 102 permit ip host 30.x.x.18 host 14.x.x.1 log ! includes IKE negotiation
access-list 102 deny any any

Primary Firewall Security Policy.

The primary firewall will be based on a **Solaris 7 SPARC** platform with the latest patches and with **Checkpoint FW-1 version 4.1 SP5** running on top of it. Before installing and applying the Checkpoint Security Policy, some unnecessary services need to be disabled in the underlying OS. The firewall will filter traffic to/from the border router, the VPN, the DMZ, and the internal network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Firewall Hardening:

References:
http://www.yassp.org/after.html,
http://www.usenix.org/sage/sysadmins/solaris/index.html#host,
http://www.enteract.com/~lspitz/papers.html,
http://www.geocities.com/sabernet_net/papers/Solaris.html,
http://sunsolve.sun.com/pub-cgi/show.pl
http://www.phoneboy.com

Referencing Lance Spitzner's white paper – *Armoring Solaris* *http://www.enteract.com/~lspitz/armoring.html*, the proper steps will be taken to harden the OS level of the firewall. This includes, but is not limited to, disabling unnecessary services (i.e. inetd file), using TCPWrappers where appropriate, ensuring the latest patches have been tested and properly applied, running a *hardening utility* against the OS (i.e. YASSP), installing and configuring Tripwire (comes with YASSP) for integrity checks on important system files, making a CD back-up copy of key utilities in the event of a system file breach, and so on. OpenSSH will also be installed to allow SSH connections from administrators. Based on these techniques, the OS level is assumed to be hardened and stable.

Checkpoint Firewall Security Policy and Tutorial:

Business Security Policy

- Internal users can access the Internet (http/https) for business purposes only. Content filtering will be performed on all Internet requests to help prevent access to inappropriate material.
- Remote users can use their company issued laptops to access the internal network via cable modem/DSL with Checkpoint's SecureClient/SecureRemoteVPN Client. Split tunneling will be **disabled** to prevent ISP-traffic from flowing through the internal network. All laptops will have a personal firewall installed on them. Dial-up connections are not supported with the VPN software, only high speed connections are supported.
- POP3, Internet mail, Telnet, and FTP are not allowed. Telnet and FTP are not allowed internally or externally.
- SSH will be utilized to perform all remote administration functions.
- Only Business Partners and Remote users can access internal resources using IPSEC tunneling.

Administering Checkpoint FW-1

Start the Checkpoint FW-1 *Policy Editor* GUI client and authenticate to the management server by entering the proper username, password, and management server name.

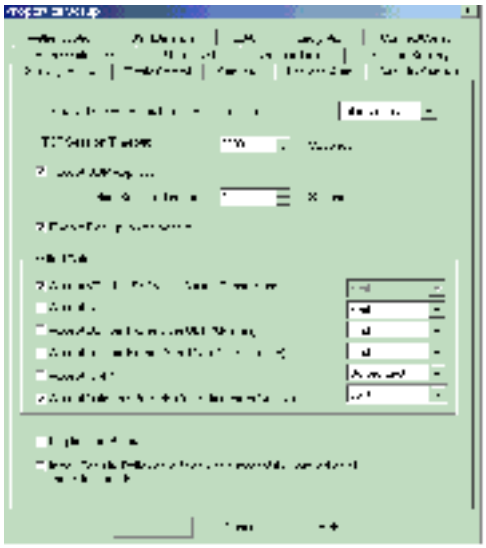
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Before:
Before building the rulebase, the *implied* rules set up should be investigated. By default these rules are not logged. These rules can be viewed by selecting *View -> Implied Rules* within the **Policy Editor**.

Source	Destination	Service	Action	Track	Install On	Time	Comment

The implied rules settings are controlled by the *Property Settings*, which can be found by selecting the *Policy->Properties…*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



After:

For the purposes of GIAC's rulebase, all unnecessary services/protocols will be disabled (unchecked) and explicitly defined in the rulebase, with logging, if needed. This will remove the implied rules that were viewed above.

Rulebase Setup:

Before creating a rulebase, the appropriate objects representing the network, i.e. servers, networks, undefined services, etc., must be created. These can be created by selecting:

- For Network Objects select *Manage->Network Objects…*
  Used for specific types of network components, i.e. workstations, networks, etc.
- For Services select *Manage ->Services…*
  Used to define unlisted services
- For Servers select *Manage ->Servers…*
  Used to create specific types of servers, i.e. RADIUS, Policy, etc.
- For Users select *Manage->Users…*

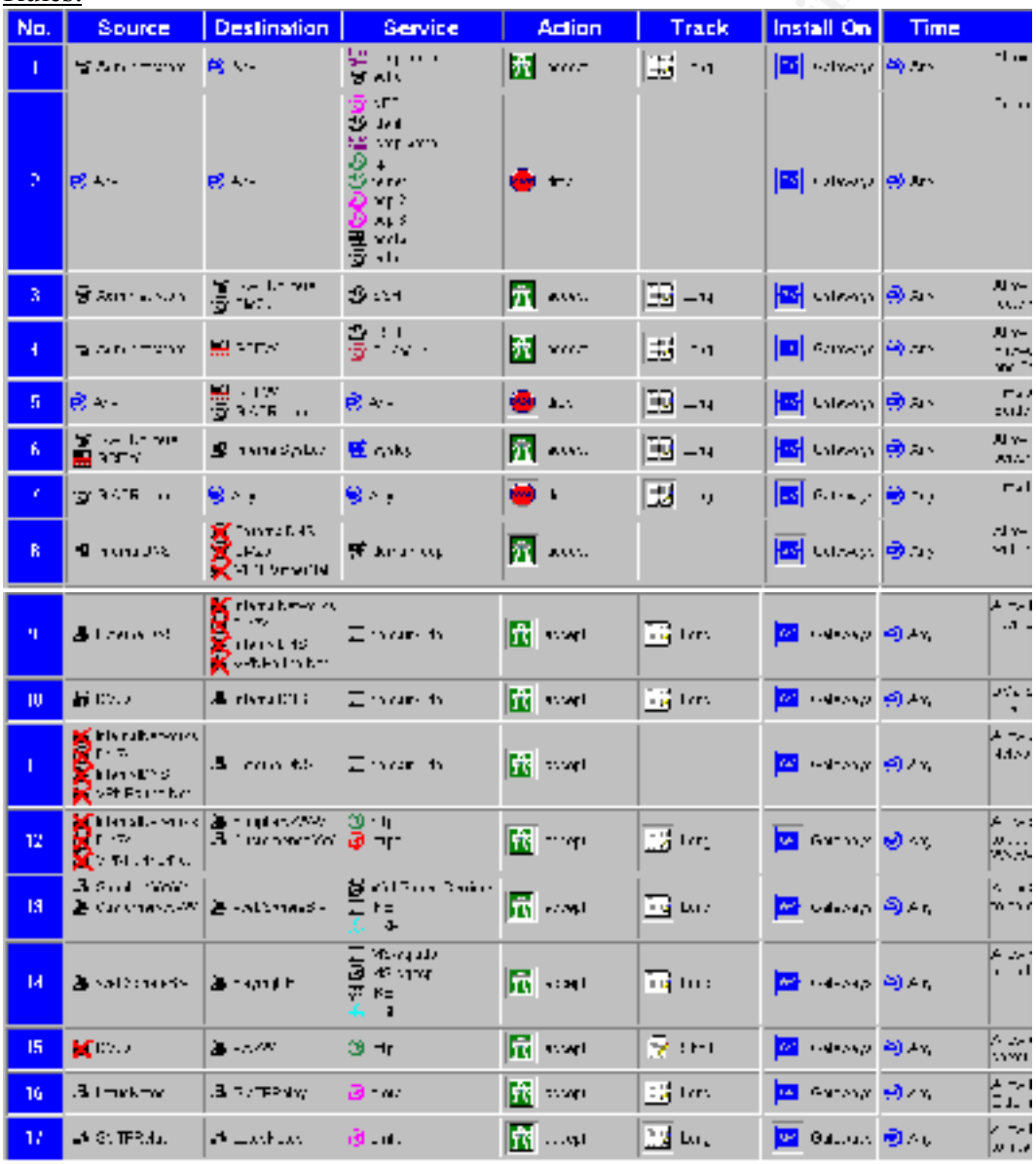
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Used to create specific users to authenticate and/or encrypt their communications
Once all the necessary objects have been created, the rulebase can be created to implement the security policy. Rules are added by selecting *Edit->Add Rule* followed by one of the following options:

- *Top* – inserts rule at the top of the rulebase
- *Bottom* – inserts rule at the bottom of the rulebase
- *After* – inserts rule after the highlighted rule
- *Before* – inserts rule before the highlighted rule

Once a rule has been added, right click in each cell to change the appropriate properties to accurately reflect the desired policy. Properties can be modified for *Source, Destination, Service, Action, Track, Install On, Time, and Comment*.

Rules:



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Allow administrators to troubleshoot via the ICMP and echo protocols. Allow the administrators to troubleshoot any internal/external destination's connectivity issues via ICMP or TCP echo. ICMP can be used as a tunneling protocol, i.e. TFN or TFN2K, to cause a denial of service via ICMP floods, therefore we are restricting who can actually utilize this protocol. To ensure that this rule is working properly, the administrators will initiate ICMP "ping" tests from their workstations to devices outside the firewall and ensure they get a return.

2. Drop chatty and restricted protocols. If a service is not needed then it should be explicitly dropped to help avoid exploitation. The security policy states the non-use of ftp, telnet, and pop3 mail. Other services that can be easily exploited and should not cross the firewall, include NetBIOS, ICMP, ident and bootp. As other services/protocols are evaluated and not required, they can be added to this rule. This rule must be placed after *Rule #1* to allow the administrators access to ICMP and TCP echo for troubleshooting purposes. To ensure that no one, with the exception of the administrators, can access these protocols, the administrators could generate traffic using any source that would pass through the firewall utilizing the explicitly denied protocols. The administrators would not be able to use their own machines for the icmp/echo tests because they have explicit rights to use this protocol via *Rule #1*.

3. Allow administrators to access the DMZ servers or routers via SSH. Only the administrators may directly access the routers and servers via SSH. Telnet is **not** allowed within this environment. TCP 22 – ssh is more secure because it encrypts communications between the source and destination. Therefore, passwords or other sensitive information are not sent in the clear like using Telnet. Administrators will use the SecureCRT client v4.3, SSH v2, to verify connections to the SSH server which is active on the routers and DMZ devices.

4. Allow administrators to access the firewall via SSH and Checkpoint protocols. Only the administrators may directly access the OS or Checkpoint firewall via SSH and the Checkpoint management protocols, respectively. Telnet is **not** allowed within this environment. TCP 22 - SSH is more secure because it encrypts communications between the source and destination. Therefore, passwords or other sensitive information are not

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

sent in the clear as with Telnet. OpenSSH is the server component loaded on the firewall and what administrators' SecureCRT 4.3 SSH client will connect to.

5. Drop accesses directly to the firewall and routers using any service. No one, with the exception of the administrators, is allowed to access the firewall or routers directly regardless of the protocol. This rule will help cut down on direct attacks against the firewall and routers. This rule must be placed after *Rules # 3 & 4* to allow the administrators access to the firewall and routers. Administrators can use any device but their own to ensure that the routers and firewall are inaccessible using any protocol.

6. Allow GIAC firewall and routers to send syslog information to the Internal Syslog server via syslog service. The firewall and routers log key information about traffic that is either allowed or blocked. This information will be stored and can be reviewed on the Syslog server which helps offload some of the firewall's and routers' work. UDP 514 - syslog is the only protocol allowed to communicate between the Syslog server and the router/firewall. This prevents other traffic from being initiated from the firewall or routers. The routers are setup to log directly to the Syslog server and the logs from the firewall are scheduled to offload logs to the Syslog server every four hours. The administrators will check the Syslog server to ensure that logs are transferred properly.

7. Drop communications initiating from any of the GIAC routers using any service. Traffic should not be initiated, regardless of the service/protocol, from the routers. If this does happen, it will be immediately dropped. This could be a sign that someone has taken over the router and attempting to exploit other devices. This must follow *Rule #6* to properly allow router/firewall communications to the Syslog server. Administrators can test this by consoling directly into the routers or using their SSH clients to connect to the routers and initiate that will cross the firewall.

8. Allow Internal DNS to query Internet DNS Servers (not External DNS) via DNS. If a user requests information that is not cached in the Internal DNS, the Internal DNS is allowed to query the Internet DNS Server(s) for an answer. UDP 53 will be used to obtain name resolution information. To prevent the Internal DNS from exposing internal information to the Internet DNS Servers, zone transfers are **not** allowed from the internal network. Valuable reconnaissance information could be gained by an attacker if this was allowed. The proof of concept for this rule is for a user to go to a website that has not been cached by the internal DNS. One warning to be careful of is *DNS Poisoning* that can result from the transfer of bad/inaccurate information from an Internet DNS. Since the internal DNS initiated the conversation, responses from the Internet DNS will be allowed to pass through without an explicit rule in place. This demonstrates Checkpoint's *stateful inspection* functionality.

9. Allow External DNS to query Internet DNS Servers (not Internal network) via DNS. The External DNS will use itself for name resolution and not the Internal DNS Server. If the External DNS does not have information cached about a particular request, it will query the Internet DNS Server(s) utilizing UDP 53. Zone transfers are not allowed so TCP 53 is not necessary. One warning to be careful of is *DNS Poisoning* that can result from the transfer of bad/inaccurate information from an Internet DNS.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

10. Allow DMZ Servers to query the Internal DNS via DNS. Servers on the DMZ, in particular the SMTP Server, require name resolution services and will use the Internal DNS to perform this function. Instead of setting up static host files on the servers, which can be easily exploited, both internal and external name lookup requests will be forwarded to the Internal DNS via port UDP 53. This port prevents zone transfers from happening.

11. Allow Internet DNS Server(s) to query the External DNS via DNS. The reciprocal of *Rule #9* is to allow the "Internet" DNS Servers to query our External DNS for the addresses of our external servers. In order for the Internet community to know how to get to GIAC's servers, the "Internet" DNS servers must have the ability to initiate a connection and query GIAC's external DNS server to retrieve this information. UDP 53 – dns is the only protocol allowed to access the External DNS server to help prevent attacks via other services. A warning to be careful of is DNS poisoning that can happen as a result of bad/faulty information being passed to the External DNS.

12. Allow Internet (only) to access Customer and Supplier Web Server via HTTP and/or HTTPS. Only non-internal users, i.e. Internet, are allowed to access the Customer and Supplier web servers via TCP 80 - http and TCP 443 – https. These are the only services allowed to connect to the servers to prevent other attacks via other protocols/services. There is no need for the internal network to access these servers. To ensure that internal users, with the exception of the administrators, can not access these servers, the administrators can attempt to do so from a user's workstation. To verify that the Internet community can get there, the administrators can work with their suppliers and verify access as well as use their Internet test account via AOL to access these sites.

13. Allow Customer and Supplier Web Servers to communicate with WebSphere Server via WebSphere Services. Information submitted to the Customer and Supplier web servers is actually processed by the WebSphere (application) Server. The Customer and Supplier web servers serve as a *Presentation* layer. The WebSphere server is not accessible via the Internet *only* through the Customer and Supplier Web Servers, which has some WebSphere code loaded on them to allow them to interconnect. Specific ports have been setup to allow communications between the *Presentation Servers (Customer/Supplier WWW)* and the *Application Server (WebSphere)*. IPSEC is also used to encrypt communications of sensitive data using transport mode, IKE and ESP.

14. Allow WebSphere Server to communicate with the Internal MS SQL Server database via 1433. WebSphere submits all information to the Internal MS SQL Server database via TCP/UDP 1433 – ms-sql. *Transport mode* IPSEC with ESP is used to encrypt communications between these two servers. This will help protect customer/supplier sensitive information. IKE will be used to setup IPSEC between these two devices, therefore UDP 500 – IKE needs to be allowed through the firewall as well. Using *transport mode*, the host IP addresses will remain in tact. Whereas with *tunnel mode,* the host IP addresses are encapsulated within another IP packet which uses the outside address of the gateway, usually a VPN router. **Special Note:** *MS SQL Server is setup*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

with a password for the system administrator (sa) in response to "Kaiten" exploit on port 1433 from CERT, http://www.cert.org/incident_notes/IN-2001-13.html.

15. Allow anyone, except DMZs, to access the public web server via HTTP. Everyone (internal and Internet) is allowed to connect to the public web server via TCP 80 – http. This is all public information and contains no sensitive information. GIAC will need to be careful that an attacker does not try to deface the website by *hardening* the web server OS and IIS 5.0 by keeping current with the latest patches, service packs, etc. Anyone internally and externally, with the exception of DMZ, should be able to access the public web server via http only, since there is not a server-side certificate installed.

16. Allow Internal Lotus Notes Server to access the External SMTP Server via SMTP. Internal mail destined for the Internet must first be *relayed* through the External SMTP server. Therefore, the Internal Lotus Notes Server is allowed to send mail to the External SMTP server. Only TCP 25 – smtp is allowed to communicate between these servers. Mail servers are protected by McAfee's GroupShield from viruses and other forms of malware sent via email. Mail rules will be tested by sending a "harmless" virus as an attachment and ensuring that it is properly detected and cleaned before reaching the end user.

17. Allow External SMTP Server to access Internal Lotus Notes Server via SMTP. Internet mail destined for the Internal network must first go through the External SMTP server. Therefore, communications on port 25 are allowed from the External SMTP server to the Internal Lotus Notes server. Mail servers are protected by McAfee's GroupShield from viruses and other forms of malware sent via email. Mail rules will be tested by sending a "harmless" virus as an attachment and ensuring that it is properly detected and cleaned before reaching the end user.

18. Allow Internet-only access to the External SMTP Server via SMTP. Internet mail is received by the External SMTP server before being passed to the Internal Lotus Notes server. To allow this communication, only TCP 25 – smtp is allowed for the Internet mail servers to communicate with the External SMTP server. Mail servers are protected by McAfee's GroupShield from viruses and other forms of malware sent via email. Mail rules will be tested by sending a "harmless" virus as an attachment and ensuring that it is properly detected and cleaned before reaching the end user. Please note that the SMTP Server only relays mail for the GIAC domain and cannot be used for SPAM mail.

19. Allow External SMTP Server to send mail to the Internet via SMTP. After Internal mail has been sent to the External SMTP server, it must be sent to the Internet. Therefore, communications on port 25 are allowed from the External SMTP server to the Internet (non-Internal) is allowed. Mail servers are protected by McAfee's GroupShield from viruses and other forms of malware sent via email. Mail rules will be tested by sending a "harmless" virus as an attachment and ensuring that it is properly detected and cleaned before reaching the end user.

20. Allow remote users using VPN Client to access Internal network using any service. GIAC's remote users are required to use Checkpoint's SecuRemote/SecureClient VPN

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

client. Communications between the remote users through the Internet to the Internal network will be encrypted. This will prevent an attacker from intercepting sensitive information. It should also be noted that split-tunneling will be **disabled** on the remote users' laptops to prevent ISP-traffic from tunneling through to GIAC's internal network. Since any service is allowed, GIAC security analyst will need to closely monitor this to ensure no holes can be exploited.

21. Drop traffic originating from the DMZ to the Internal Network or other DMZs using any service. Servers on the DMZs will not be able to initiate a connection to the internal network or other DMZs, regardless of the service. Once a device has been compromised within the DMZ, the attacker will then attempt to access and exploit devices in the internal network. To prevent this type of attack, we are blocking any traffic that originates from the DMZ and attempts to send traffic to the Internal Network. This rule must come after *Rule #14* to allow the WebSphere to communicate with the internal MS SQL Server. GIAC also wants to prevent a compromised device from getting to another DMZ device(s), basically limiting the scope of further penetration. The rule must also come after *Rule #10, 13 & 17*, to allow the DMZ devices to do name resolution via the Internal DNS, to allow the Supplier and Customer WWW to communicate with WebSphere and the SMTP Server to communicate with the Lotus Notes Server, respectively. GIAC analysts will be alerted on this rule because of a possible penetration attack.

22. Drop traffic originating from the Internal Network to the DMZ using any service. Internal network users should not be sending any type of information, regardless of protocol, directly to the DMZs. *Rules #1, 3, 4, 15, and 16* must all come before this rule to allow these internally initiated connections to specific devices on the DMZs.

23. Internal users to access the Internet via HTTP and/or HTTPS. This rule will allow internal users to access the Internet via TCP 80 - http and TCP 443 - https only. All other services, i.e. FTP and Telnet, will be dropped. This rule must follow *Rule #21* to prevent internal users from accessing DMZ devices via http/https.

24. Allow business partners to access specified internal resources i.e. MS SQL Server database. Business partners will use IPSEC *transport* mode with ESP between the partner machine and the SQL Server, *Sayings* database. This will help keep communications secure even while on GIAC's Internal Network. IPSEC *tunnel* mode with ESP is utilized between the VPN gateways (GIAC and Business Partner). IPSEC configurations will need to be setup on both the source (Business Partner) and destination (SQL Server) machines. As access to other internal resources is needed, GIAC will setup additional rules for the Business Partners.

25. Allow internal network/users to access the business partner(s) resources via VPN tunnel. Please note that the business partner(s) is responsible for restricting access to their resources from GIAC's Internal network. Initial traffic sent from the internal network to GIAC's VPN gateway is not encrypted, unless specified by the business partner. Once it leaves GIAC's VPN gateway and crosses the Internet destined for the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

business partner site, all traffic is encrypted using *tunnel* mode IPSEC utilizing the ESP protocol.

26. Drop All Rule. Checkpoint implicitly drops all traffic that does not meet any of the explicitly stated rules, but **does not** log them. By explicitly setting up this rule, traffic that is not explicitly allowed will be dropped (regardless of source, destination, and service) *and* logged. This should always be the last rule.

After the Checkpoint FW-1 rulebase matches the Business Security Policy, the firewall policy can be *installed and activated* by selecting *Policy->Install.*

VPN Security Policy.

The VPN gateway selected to handle business partner communications is a **Cisco 3640 IOS 12.2 router**. In addition to the *access control lists* (ACLs), there are some services that should be disabled to help prevent simple attacks.

VPN Gateway Hardening:

VPN gateway hardening will follow the same process as the ***Border Router Hardening*** section above.

VPN Gateway Policy:

Reference:
http://www.cisco.com/warp/public/779/largeent/vpne/vpndocs/vpnsw.html#iosdocset

For each business partner, a separate pre-shared key will be used to authenticate the gateways.

Configuration on GIAC VPN Gateway
IKE Requirements:
!Pre-share keys, IKE with 3DES, SHA, Diffie-Hellman Group 2 (1024 bit)

```
!IKE SA
crypto isakmp policy 1
authentication pre-share
encryption 3des
group 2
lifetime 3600
crypto isakmp key bp@4tune$ address 14.x.x.1
```

IPSEC Requirements:
!ESP, 3DES and SHA, Tunnel Mode **ONLY**

```
! IPSEC SA
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac

! Regular Crypto Map
crypto map bponly 1 ipsec-isakmp
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
set peer 14.x.x.1
set transform-set 3dessha
match address 101

! Apply the crypto map to an interface
interface Ethernet 0/0
ip address 30.x.x.18 255.255.255.248
access-group 102 in
crypto map bponly

!Access List for IPSEC SA – permit = "encrypt" and deny = "unencrypted"
access-list 101 permit ip 10.x.x.0 0.0.0.255 12.x.x.0 0.0.0.255
access-list 101 deny ip 10.x.x.0 0.0.0.255 any log

!Access List for traffic coming into the encrypted side of GIAC VPN Gateway
access-list 102 permit ip 14.x.x.1 0.0.0.0 30.x.x.18 0.0.0.0 log

!Deny all other traffic
access-list 102 deny any any

interface Ethernet 0/1
ip address 30.x.x.26 255.255.255.248
access-group 103 in

!Allow internal users to access business partner subnet – clear side of VPN
access-list 103 permit ip 10.x.x.0 0.0.0.255 12.x.x.0 0.0.0.255

!Allow internal administrators to access the router via SSH
access-list 103 permit tcp 10.x.x.130 0.0.0.0 30.x.x.26 0.0.0.0 22
access-list 103 permit tcp 10.x.x.130 0.0.0.0 30.x.x.18 0.0.0.0 22
access-list 103 permit tcp 10.x.x.131 0.0.0.0 30.x.x.26 0.0.0.0 22
access-list 103 permit tcp 10.x.x.131 0.0.0.0 30.x.x.18 0.0.0.0 22

!Deny all other traffic
access-list 103 deny any any
```

Configuration on Business Partner VPN Gateway
Note: *They are responsible for their own access lists, this only demonstrates how IPSEC should be set up.*

IKE Requirements:
!Pre-share keys, IKE with 3DES, SHA, Diffie-Hellman Group 2 (1024 bit)

```
!IKE SA
crypto isakmp policy 1
authentication pre-share
encryption 3des
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

group 2
lifetime 3600
crypto isakmp key bp@4tune$ address 30.x.x.18

IPSEC Requirements:
!ESP, 3DES and SHA, Tunnel Mode **ONLY**

! IPSEC SA
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac

! Regular Crypto Map
crypto map GIAC 1 ipsec-isakmp
set peer 30.x.x.18
set transform-set 3dessha
match address 101

! Apply the crypto map to an interface
interface Ethernet 0/0
ip address 14.x.x.1 255.255.255.248
crypto map GIAC

! Access List for IPSEC SA – permit = "encrypt" and deny = "unencrypted"
access-list 101 permit ip 12.x.x.0 0.0.0.255 10.x.x.0 0.0.0.255
access-list 101 deny ip 12.x.x.0 0.0.0.255 any log

III. Audit Your Security Architecture (25 points)

Audit Plan.

Referencing Lance Spitzner's White Paper – *Auditing Checkpoint Firewall Setup* http://www.enteract.com/~lspitz/audit.html, the analysts planned their audit strategy. After completing GIAC's network security architecture, an audit of the primary firewall was conducted to ensure there were no "leaks" to/from the internal network. In addition to checking the log files on a routine basis, the overall audit plan included internal and external penetration tests against and through the firewall using Internet-accessible scanner tools. Specifically, this audit sought to explore vulnerabilities in the firewall rulebase presented above and address them accordingly.

Audit Checklist - Two Step Audit:

1. *OS Audit*
   - Prior to audit perform a network "baseline" for future comparisons
   - Validate latest patches and upgrades
   - Test and validate "listening" services
   - Review logs for discrepancies and unexpected entries
2. *Checkpoint FW-1 Audit*
   - Validate latest patches and upgrades

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- *Manual*: Test and evaluate the validity of rules in firewall security policy (have business rules changed?, etc.)
- *Automated*: Use scanner tool to ensure unknown protocols/services are **not** "leaking" through the firewall.

Resources:
- 1 Senior Security Analyst and 1 Junior Security Analyst
- 1 Senior Network Analyst and 1 Junior Network Analyst

Senior analysts will perform audit testing functions with input from the junior analysts. The junior analysts will be utilized for on-the-job training (OJT) for future audit work.

Work Phase Approach:
- *Data Capture Phase* – use manual and automated techniques to capture data as input to Analysis Phase. This will be captured at different points during the day and work week to provide a good sample of information.
- *Analysis Phase* – review output from *Data Capture Phase* comparing results to Business Security Policy and ensuring other services are not exposed.
- *Documentation Phase* – management and technical documentation of processes, procedures, and analysis for baseline purposes, improvement(s) justification, etc.

Time Frame:
The anticipated total time to complete the audit is approximate five 5-hour days for a total of 25 hours. ***Note:*** *This will allow the analysts to be available to handle other troubleshooting calls outside of the audit.* This will encompass all 3 phases of work and ensure that accurate documentation is presented to upper management.

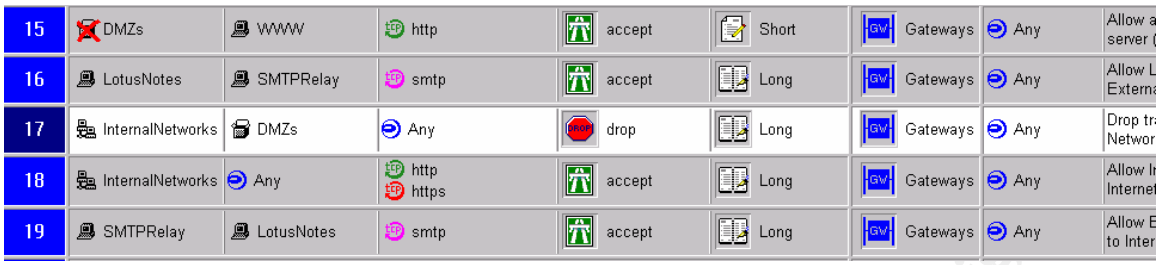
Costs:
The 4 individuals will be full-time GIAC employees conducting the firewall audit and will cost ~$9000 for the week. GIAC already has a development lab which is a semi-replica of the production network and includes similar types of network and security equipment.

Conducting the Audit.

Network Baseline

By conducting a baseline of the network and analyzing the firewall logs, the analysts learned that a large portion of their traffic was due to internal users accessing the Internet (http/https). They reviewed the security policy to determine if the associated rules (*Rules #22 and 23)* could be moved to improve Internet access performance. Increased performance would result from not having to check as many rules before being allowed access to the Internet. Their conclusion was that *Rules #22 and 23* could be moved just after *Rules #16* without affecting the other rules.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



15	DMZs	WWW	http	accept	Short	Gateways	Any	Allow a server (
16	LotusNotes	SMTPRelay	smtp	accept	Long	Gateways	Any	Allow L Externa
17	InternalNetworks	DMZs	Any	drop	Long	Gateways	Any	Drop tr Networ
18	InternalNetworks	Any	http https	accept	Long	Gateways	Any	Allow In Internet
19	SMTPRelay	LotusNotes	smtp	accept	Long	Gateways	Any	Allow E to Inter

Verify latest patch levels and vulnerabilities for OS and Checkpoint FW-1
The analysts split the load of verifying OS and Checkpoint FW-1 patch levels. After visiting Sun's website at http://sunsolve.sun.com/pub-cgi/show.pl, the analysts realized there was a new security patch released to handle a *login* security problem (4516885). This addressed a buffer overflow that could occur during login. The patch was tested and monitored in the development lab then released into the production environment.

Solaris 7:
Reference:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?patchid=112300&collection=fpatches

Patch-ID# 112300-01
Keywords: security login buffer overflow
Synopsis: SunOS 5.7: usr/bin/login Patch
Date: Dec/13/2001
Solaris Release: 7
SunOS Release: 5.7
Unbundled Release:
Xref: This patch available for x86 as patch 112301
Topic: SunOS 5.7: **usr/bin/login Patch**

Checkpoint FW-1 SP5:
Reference:
http://www.checkpoint.com/techsupport/downloads/html/securemote/sr-4-1/srsc_release_notes_41_sp5.pdf

They also found a new SecuRemote/SecureClient Service Pack and RDP hotfix for Checkpoint's software that was tested and applied into the production environment.
November 7, 2001
New Service Pack Release: VPN-1 SecuRemote/SecureClient 4.1 SP5 is now available for download for Win 9x, Win ME, Win NT, Win 2000 and Win XP.
Summary:
This new service pack provides new features and updates to the VPN-1 SecuRemote/SecureClient.

Reference:
http://www.checkpoint.com/techsupport/alerts/rdp.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

October 25, 2001
New Hotfix Release: VPN-1/FireWall-1 4.1 SP5 RDP Hotfix. This hotfix applies to management stations and not firewall modules.
Summary:
This hotfix addresses RDP communications and blocks it by **default**, unless explicitly passed via UDP port 259. Previously, VPN-1/FireWall-1 allowed RDP packets to traverse firewall gateways in order to simplify encryption setup.
Issue:
Packets with RDP headers could be constructed and utilized to establish a covert communication channel.

Test and Validate "listening" services
Nmap scan against OS:
Using a Windows 2000 machine, the analysts executed a TCP and UDP port (1 – 65535) scan against the firewall to determine what ports are "listening".

Nmap Commands and Screendumps:
ISS Realsecure picked up the scan attempts, but this could be easily masked (from being detected as an *nmap* scan utility) by changing the nmap command parameters to spoof the source address **and** not ping the host beforehand. The ping of the host is an indication of the utility being used is nmap.

TCP Port Scan:
>nmapnt -v -P0 -p1-65535 <fwmachine-name>

UDP Port Scan:
>nmapnt -v –sU –P0 -p1-65535 <fwmachine-name>

These scans revealed what the analysts anticipated; only 1 TCP (SSH-tcp 22) and no UDP services listening on the firewall. ISS Realsecure network IDS (NIDS) alerted, via email to the analysts, on the TCP/UDP scan attempts which was a good indication that this utility was also working properly. The analysts further investigated the SSH protocol to ensure that any vulnerabilities found were appropriately addressed by visiting, http://www.cert.org/current/current_activity.html#scans.

Review of Syslogs
The syslog server was filled with valuable data, but none of the analysts had taken time to setup scripts that would properly parse the data into a useable format. If an attack were to happen, they would spend hours sifting through the data to find anything relevant. The junior analysts were utilized at this point to develop scripts to properly parse the information received from the routers and firewall. These scripts were tested in development and then implemented in the production environment.

Tripwire (File Integrity) Review
A limited version of **Tripwire v1.2** was installed as part of the YASSP *hardening* utility. Tripwire is used to ensure the integrity of system files by generating a security hash and storing that information in a database for future comparisons. This database is not stored

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

on the firewall itself, to help further ensure that a "would-be" attacker could not change its contents.

Tripwire initialization:
The following command was used to initialize the Tripwire database when the operating system was first installed.

./tripwire –i 2 –c tw.config

Only the SHA1 and MD5 algorithms were used and not the *snerfu* algorithm. After this database was created it was burned to a CD and also copied to another server within the internal network. The original database was then deleted from the firewall. This was done in the event that the firewall was compromised and files were changed, the attacker would believe that there are no file integrity checks in place because of the absence of the integrity database.

Tripwire Comparison:
The Tripwire database is checked on a weekly basis and updated each time a system update occurs due to patch upgrades, hot fixes, etc. The command used for weekly checks is the same as was used to create the initial database.

./tripwire –i 2 –c tw.config

The command used to indicate that changes to certain files or directories are acceptable is:

./tripwire –update [/file1 /file2 … /filen]

The analysts determined that none of the files had been tampered with and considered the system to still be in a stable state.

Checkpoint Review
(Please note that screenshots of logs from the firewall and SurfControl could not be included in this paper because they contained company-specific information)

Manual Review:
The senior analysts spoke with upper management to determine if any of the business security policy statements had changed. From their interview, management was concerned with the Internet accesses of employees and asked that they be tightly monitored to ensure no company liabilities or exposures. Given this information, the junior analysts reviewed the **Surf Control** logs and discovered that users were spending too much time on the Internet. To better control accesses to the Internet on a time basis, the senior analysts implemented a time period of 11:30am – 1:30pm (typical lunch period) for Internet access. If anyone needed access to the Internet outside of these times, management approval would have to be granted and a special rule for these users would be setup in the firewall for 8:00am – 5:00pm access.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

17	InternalNetworks	DMZs	Any	drop	Long	Gateways	Any
18	SpecialInternetAccess	Any	http https	accept	Long	Gateways	business_h
19	InternalNetworks	Any	http https	accept	Long	Gateways	lunchtime
20	SMTPRelay	LotusNotes	smtp	accept	Long	Gateways	Any

Automated Review:
In addition to the manual review of the firewall rules and logs, the senior analysts also subjected the firewall policy to several scan tests. A Windows 2000 machine running nmapNT was utilized to perform these tasks. Their key concern was ensuring that if a device on either of the DMZs were compromised, that it could not access the internal network.
A sniffer and target workstation were setup between the firewall and internal router to act as endpoints. The target workstation had various ports open including both restricted and unrestricted, i.e. DNS – 53, Telnet – 23, Mail – 25, SSH – 22, FTP – 20 & 21, SNMP – 161 & 162, NetBIOS – 135 – 139, http/https – 80 & 443, and other "interesting ports". The objective was to determine if a machine on the DMZ could go through the firewall and reach the target machine on any of the open ports.

Reference:
http://www.insecure.org/nmap/nmap_manpage.html by Fyodor

The following nmap commands were used to conduct the firewall rulebase audit:
Ping Scan/Sweep: Determine what machines are "UP" on a given network
nmapnt –v –sP <target network>

TCP Scan: Determine what TCP ports are open
nmapnt -v -P0 –O –sT -p1-65535 <target machine>

UDP Scan: Determine what UDP ports are open
nmapnt -v -P0 –sU -p1-65535 <target machine>

RPC Scan: Determine if any RPC programs are running on the TCP/UDP ports
nmapnt -v -P0 –sT –sU –sR -p1-65535 <target machine>

Identd Scan: Determines who the owner is of a TCP service
nmapnt -v -P0 -sT –I -p1-65535 <target machine>

After testing was completed, the target machine was **immediately** taken offline. The results of the scans were as follows: *(Please refer to the new Firewall Rulebase for all rule number references)*

- *Ping Scan* – the ping scan was not able to penetrate the firewall because of *Rule #2*, which explicitly blocks the ICMP protocol and the TCP echoes. Therefore, this rule was determined to be working properly.
- *TCP Scan* – the tcp scan was not able to penetrate the firewall because of a combination of *Rules #2 and #24*. *Rule #2* drops explicit services like ftp – 20/21,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

telnet – 23, etc. *Rule #24* drops connections from the DMZ to the internal network.

- *UDP Scan* – the udp scan was not able to penetrate the firewall because of a combination of *Rules #2 and #24*. *Rule #2* drops explicit services like ftp – 20/21, telnet – 23, etc. *Rule #24* drops connections from the DMZ to the internal network.
- *RPC Scan* – the rpc scan was run in conjuction with both the TCP and UDP scan to determine if any of the open services had rpc programs associated with them. Since devices from the DMZ, *Rule #2 and 24,* are not allowed to initiate connections, this traffic was dropped.
- *Identd Scan* – the identd scan was run in conjunction with the TCP scan to determine if the owner of an open service could be released. Since devices from the DMZ, *Rule #2 and 24,* are not allowed to initiate connections, this traffic was dropped.

Evaluate the Audit.

After conducting the above audit, the analysts concluded that the current infrastructure is reasonably stable from an architectural perspective. From a technical perspective, they concluded that more or newer equipment was not necessarily the answer for improvement, but rather properly tuning what was already in place. As more updates and patches became available for their equipment, they need to do a better job of testing and deploying them into the production environment. Action items resulting from the audit and presented to management are as follows:

- Develop a checklist to disable all unnecessary *services* on all devices, not just perimeter devices. This will help prevent simple attacks on open *listening* ports.
- Develop a process to:
    - review the latest updates/patches/hotfixes for the *OS* and *Checkpoint FW-1*
    - download and test in the development environment
    - deploy into production after acceptable testing in the development environment
    - re-baseline and compare network traffic after the introduction of changes into the production environment
- Ensure IDS signatures are tuned appropriately and alerting security analyst when certain thresholds are reached
- Monitor logs on Syslog server, SurfControl and firewall more accurately, i.e. weekly graphical charts for analysts and management.
- Develop a process to validate integrity of key files and system tools after package installs on the firewall. Better review of Tripwire utility that was installed as part of the YASSP utility.
- Determine usage and need of Tripwire and host-based IDS (HIDS) on other *critical* systems.
- Setup quarterly meeting with upper management to review Business Security Policy Statements.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Conduct quarterly audits/penetration tests **and** when new equipment is deployed beyond the firewall, i.e. DMZs, and/or when major changes are made to the firewall rulebase.
- New Firewall rulebase after audit:

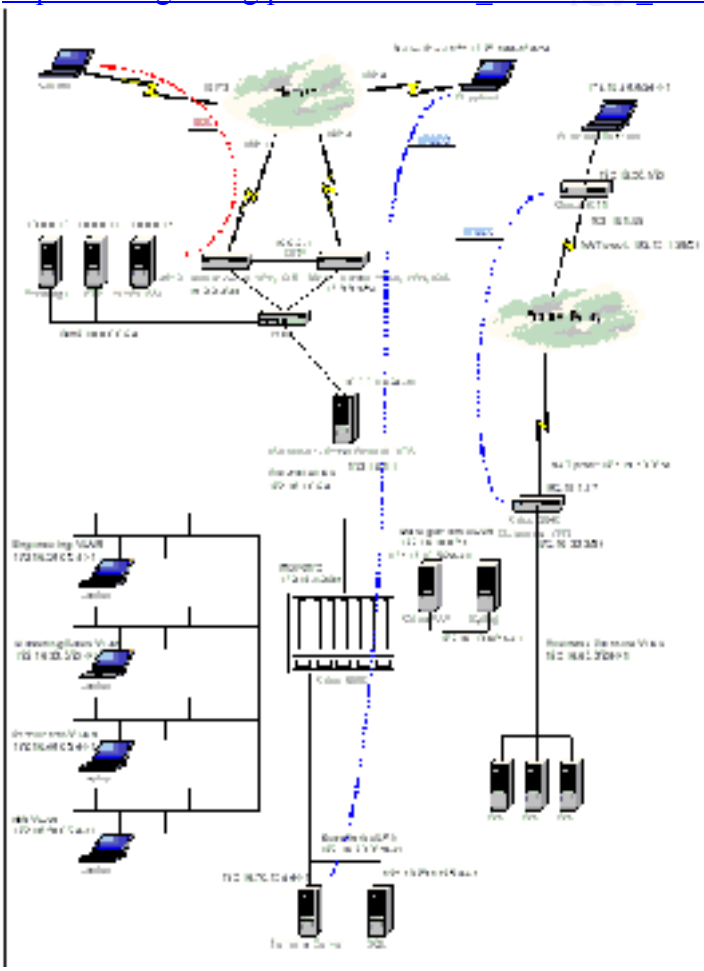
No.	Source	Destination	Service	Action	Track	Install On	Time
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

IV. Design Under Fire (25 points)

Background:

I have chosen to attack the Network Security Architecture setup by **Arkadi Karetnikov** (0174) which can be found at
http://www.giac.org/practical/Arkadi_Karetnikov_GCFW.zip



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Attack Against Firewall:

Vulnerability #1:

References:
http://www.securityfocus.com
http://cve.mitre.org/
http://www.cert.org/

This vulnerability is a Denial of Service (DoS) against the ISA server that results from sending a URL request with a long pathname. The URL request would consist of sending an extremely long pathname that in turn causes an access violation in *w3proxy.exe*. The final result is the termination of the service which presents a DoS. For more details, please read the following information below from BugTraq.

Options for exploiting this vulnerability:

- Issue the following command to a known ISA Server - http://<isa server>/aaa [3000+ occurences of "a"]
- Generate an HTML message with an IMG tag with a SRC value URL containing the above link
- Generate an HTML message containing Java- or VBScript which generates a URL request as stated above to an individual within the protected network

Pre-attack Tasks:

Option #1

- A "would-be" attacker would need to first ensure that a company is using an ISA server for their firewall. Social engineering could be used to accomplish this task by calling the "techies" and pretending to be a salesperson gathering, for example, statistical information about the type and version of border routers and firewalls used by e-commerce companies.
- By determining the border router type, the attacker can determine how to break-in to it and if necessary use the border router as a lauchpad for the attack against the firewall.

Option #2

- Another option would be to send an email to several internal users in hopes that they would be "curious" enough to click on the link and cause the DoS.

To prevent detection, the attacker could simply spoof the source address of the request.

How to mitigate vulnerability:

- Apply hotfix issued by Microsoft
- Perform some content filtering on URL requests
- Prevent web browser from executing Java- or VBScript in a web browser

Vulnerability #1 Reference:
http://www.securityfocus.com/archive/1/177160

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To:	BugTraq
Subject:	[SX-20010320-2b] - Followup re. Microsoft ISA Server Denial of Service
Date:	Apr 17 2001 12:02PM
Author:	SecureXpert DIRECT Bulletin Service <sxdirect@securexpert.com>
Message-ID:	<200104171602.MAA70968@mountain.fscinternet.com>

```
FSC Internet Corp. / SecureXpert Labs Advisory [SX-20010320-2b]

This is a follow-up to:
[SX-20010320-2] Denial of Service in Microsoft ISA server v1.0

Several individuals have pointed out an easier exploit scenario for
this vulnerability, which additionally does NOT require the Web
Publishing feature of ISA server to be active.

The new exploit consists simply of sending an HTML email message
containing an IMG tag with a SRC value URL of the form described in
[SX-20010320-2] to a recipient within the protected network.

When this message is read, the recipient's web browser will generate an
HTTP request which will trigger the W3PROXY.EXE access violation and
therefore the denial of service.

Another variation involves sending an HTML email message containing
Javascript or VBScript which generates such a URL request to a
recipient within the protected network.  However, some web browsers may
be configured not to execute Javascript VBScript within the context of
an email message.

Status
Microsoft Corp. was informed of this additional exploit scenario on
April 17,2001.  The hotfix issued by Microsoft on April 16, 2001
already provides a solution for this additional scenario.

Credits
Richard Reiner, SecureXpert Labs
Graham Wiseman, SecureXpert Labs
Matthew Siemens, SecureXpert Labs
Kent Nicolson, SecureXpert Labs
Hank Leininger <hlein@progressive-comp.com>

About SecureXpert DIRECT

SecureXpert DIRECT is an advance security advisory service provided to
qualified subscribers by SecureXpert Labs.  Subscriptions are free of
charge and may be obtained at http://www.securexpert.com/services.html.
```

http://www.securityfocus.com/archive/1/177216

To:	BugTraq
Subject:	Re: [SX-20010320-2] - Microsoft ISA Server Denial of Service
Date:	Apr 17 2001 7:32AM
Author:	Richard M. Smith <rms@privacyfoundation.org>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Message-ID: <ONEILKPECNHHJLENAGFMEELFEJAA.rms@privacyfoundation.org>
In-Reply-To: <20010416233023.N8227@securityfocus.com>

```
Hello,

   >>> Microsoft ISA server includes a web proxy component
   >>> (W3PROXY.EXE) that is used for both the "publishing"
   >>> of internal web servers to the external network
   >>> and for proxying of internal requests to external web servers.
   >>> Sending a URL with a long pathname component to this proxy
   >>> will cause it to terminate with an access violation error.
   >>> For example, sending the (valid) HTTP request:
   >>>  GET http://hostname/aaa[3000 more occurences of 'a']
HTTP/1.0\n\n
   >>> to port 80 on the ISA Server's external interface will cause
   >>> W3PROXY.EXE to terminate with an access violation.

I don't have access to an ISA server for testing, but this DoS attack
might also be exploitable from an HTML email message by
an outsider using the following <IMG> tag embedded in
a message:

  <img src=http://hostname/aaa[3000 more occurences of 'a']>

Another method of generating the DoS attack would be to
use JavaScript to create the long URL and then setting
the "src" property of an Image object.  This code could
also be embedded in an HTML email message.

Richard
```

Vulnerability #2:

This security bulletin lists 3 issues within ISA Server in which two services, H.323 Gatekeeper and Winsock Proxy, can cause a memory leak that result in a DoS. The other issue is with cross-site scripting. Please review the Microsoft bulletin for more details.

Vulnerability #2 Reference:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-045.asp

Microsoft Security Bulletin MS01-045 Print

ISA Server H.323 Gatekeeper Service Contains Memory Leak

Originally posted: *August 16, 2001*

Summary

Who should read this bulletin: System administrators running Microsoft® Internet Security and Acceleration (ISA) Server 2000.

Impact of vulnerability: Denial of service; cross-site scripting

Recommendation: System administrators should consider installing the patch.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Affected Software:

- Microsoft ISA Server 2000

Technical details

Technical description:

This bulletin discusses three security vulnerabilities that are unrelated except in the sense that both affect ISA Server 2000:

- A denial of service vulnerability involving the H.323 Gatekeeper Service, a service that supports the transmission of voice-over-IP traffic through the firewall. The service contains a memory leak that is triggered by a particular type of malformed H.323 data. Each time such data is received, the memory available on the server is depleted by a small amount; if an attacker repeatedly sent such data, the performance of the server could deteriorate to the point where it would effectively disrupt all communications across the firewall. A server administrator could restore normal service by cycling the H.323 service.
- A denial of service vulnerability in the in the Winsock Proxy service. Like the vulnerability above, this one is caused by a memory leak, and could be used to degrade the performance of the server to point where is disrupted communcations.
- A cross-site scripting vulnerability affecting the error page that ISA Server 2000 generates in response to a failed request for a web page. An attacker could exploit the vulnerability by tricking a user into submitting to ISA Server 2000 an URL that has the following characteristics: (a) it references a valid web site; (b)it requests a page within that site that can't be retrieved – that is, a non-existent page or one that generates an error; and (c) it contains script within the URL. The error page generated by ISA Server 2000 would contain the embedded script commands, which would execute when the page was displayed in the user's browser. The script would run in the security domain of the web site referenced in the URL, and would be able to access any cookies that site has written to the user's machine.

Mitigating factors:

H.323 Denial of service vulnerability:

- The vulnerability could only be exploited if the H.323 Gatekeeper Service was installed. It is only installed by default if "Full Installation" is chosen; if "Typical Installation" is selected, it is not installed.
- The vulnerability would not enable an attacker to gain any privileges on an affected server or add any traffic to an existing voice-over-IP session. It is strictly a denial of service vulnerability.

Winsock Proxy Service Denial of service vulnerability:

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- The vulnerability could only be exploited by an internal user; it could not be exploited by an Internet user.
- The vulnerability would not enable an attacker to gain any privileges on an affected server or compromise any cached content on the server. It is strictly a denial of service vulnerability.

Cross-site scripting vulnerability:

- In order to run script in the security domain of a trusted site, the attacker would need to know which sites, if any, a user trusted. Most users use the default security settings for all web sites, which would effectively deny an attacker any gain in exploiting the vulnerability for the purposes of running script.
- An attacker who wished to read other sites' cookies on a user's machine would have no way to know which sites had placed cookies there. The attacker would need to exploit the vulnerability once for every web site whose cookies she wished to access.
- Even if the attacker correctly guessed which sites had placed cookies on a user's machine, there should be no sensitive information in the cookies, if best practices have been followed.

Vulnerability identifier:

- H.323 Denial of Service: CAN-2001-0546
- Winsock Proxy Service Denial of Service: CAN-2001-0547
- Cross-site scripting vulnerability: CAN-2001-0658

Tested Versions:
Microsoft tested ISA Server 2000 and Proxy Server 2.0 to assess whether they are affected by these vulnerabilities. Previous versions are no longer supported, and may or may not be affected by these vulnerabilities.

Vulnerability #3:

This vulnerability ties in with the "Event Log" that is native to Windows 2000. By default the Event Log is set **not** to overwrite the log file. If an attacker can generate enough Event Log failures by sending bogus information, the log will fill up and every subsequent failure will result in a new command window opening and eventually exhausting its available memory. The final result is a DoS situation.

Vulnerability #3 Reference:

http://www.securityfocus.com/archive/1/173326

To:	BugTraq
Subject:	def-2001-16: Internet & Acceleration Server Event DoS
Date:	Apr 2 2001 12:24PM
Author:	Peter Gründl <peter.grundl@defcom.com>
Message-ID:	<01b601c0bb5f$20754f20$71002d0a@dk.defcomsec.com>

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
=============================================================================
                    Defcom Labs Advisory def-2001-16

                Internet & Acceleration Server Event DoS

Authors: Peter Gründl <peter.grundl@defcom.com>
  Andreas Sandor <andreas.sandor@defcom.com>
Release Date: 2001-04-02
=============================================================================
------------------------=[Brief Description]=-------------------------
If an alert action has been chosen in the ISA server console, a
malicious attacker can cause a Denial of Service situation on the ISA
server.

------------------------=[Affected Systems]=--------------------------
- Internet & Acceleration Server for Windows 2000 Server

----------------------=[Detailed Description]=-----------------------
By default the log settings on the Windows 2000 server are not set to
overwrite the log files as needed, and since the installation of the
ISA server does not change these settings, this is also the case with
the ISA server. If you enable the "Event Log Failure" option in the
ISA console, an attacker can send in any kind of spoofed packets that
will trigger event logs and cause the ISA server to start spawning a
CMD.EXE for each event log failure. This will result in the server
running very slowly and consuming all available memory.

This will go on even after the ISA server is rebooted until the event
log is cleaned.

We used ISIC to create a flood of spoofed, random packets:
http://www.packetfactory.net/Projects/ISIC/

Whether you chalk this one up as a security vulnerability or not, it
is still a potential problem that should be given attention if you
set up an "Internet Security and Acceleration" Server.

---------------------------=[Workaround]=-----------------------------
Make sure your log file is either overwritten as needed or that you
have the "event log failure" option disabled in the ISA firewall.

The issue is now described in Q284800 by MSRC:
http://support.microsoft.com/support/kb/articles/q284/8/00.ASP

-------------------------=[Vendor Response]=--------------------------
This issue was brought to the vendor's attention on the 20th of
February, 2001. The vendor replied:

"There are two issues here: the particular alert action (i.e., opening
 the command prompt in response to the log becoming full), and the fact
 that the alert action recurs each time you boot.

 * Alert action.  By default, there is no alert action selected -- you
 have to have enabled alerts.  Once they're enabled, the default alert
 mechanism is to run a program.  This is usually used to run a program
 to, for instance, send a mail to the administrator.  If you want to,
 you can select a different alert mechanism.
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

```
 * Recurrence.  By default, ISA will continue to take the alert action
 each time the machine is booted, until the "log full" condition no
 longer applies.  Again, the idea here is that ISA will give the
 administrator a signal that he needs to tend to his logs.  You can
 reset the recurrence so that the alert action is only take at
 predefined intervals, or only after a manual reset of the event log."

Also:

"Thanks for letting me review the draft.  I don't see anything in it
 that's factually incorrect.  However, classifying this as a denial of
 service vulnerability seems excessive, don't you think?  There isn't
 a product flaw here -- the only issue is that if the user
 deliberately turns on a feature, but doesn't configure it correctly,
 he can hurt the performance of his machine.  That is, there isn't any
 way for a bad guy to force the admin to turn on the Event Log Failure
 option, nor is there any way for him to prevent the admin from
 properly configuring it.  It seems much more appropriate to discuss
 this as an issue of proper use of the product, rather than as a
 security vulnerability."

And finally:

"I agree that the right way to use the alert mechanism isn't intuitive,
 and that we need to get the word out so folks will use it
 appropriately."

=====================================================================
            This release was brought to you by Defcom Labs

              labs@defcom.com             www.defcom.com
=====================================================================
```

A Denial of Service Attack:

DoS Attack References:
http://www.cert.org/advisories/CA-1999-17.html
http://xforce.iss.net/alerts/advise43.php
http://packetstorm.decepticons.org/distributed/TFN2k_Analysis.htm
http://www.symantec.com/avcenter/security/Content/2000_02_10_a.html
http://www.securiteam.com/securitynews/5YP0G000FS.html

With 50 compromised cable modem/DSL systems, an ICMP, UDP, or TCP flood can be conducted fairly easily. Using the DDoS utility called *Tribal Flood Network 2000* **(TFN2K)**, this task is made easy.

TFN2K has two components: *client and daemon*. The *daemon* component would be installed on each of the 50 compromised cable modem/DSL systems and they would be centrally controlled by a single *client* system. Special characteristics to note about this attack tool are:

- Client to daemon communications are encrypted

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Client to daemon communications can utilize randomized TCP, UDP, and ICMP packets
- Client to daemon communications can utilize *decoy* packets
- The client can spoof its address to making tracing tasks more difficult

The client instructs the daemons to attack one or multiple victims. In our scenario, we are only attacking **Arkadi Karetnikov** design for GIAC Enterprises. As stated in http://packetstorm.decepticons.org/distributed/TFN2k_Analysis.htm, commands to the daemons are of the form "+<id>+<data>" where <id> is a single byte denoting a particular command and <data> represents the command's parameters.

TFN2K Options and Attack:
Below are the options that can be used to launch an attack against the *Karenikov's* GIAC Enterprise design. The commands will be launched from the client and received by the daemons (50 cable modem/DSL systems), which actually executes the attack against the target. TFN2K can launch TCP, UDP, and/or ICMP flood attacks. Therefore, I am choosing to do a mixture of these attacks to keep GIAC guessing at what is actually going on. Just when they think they have figured out that it is a TCP attack, it can change to UDP or ICMP flooding. I will also use spoofed packets to make tracing the source of the attack harder.

Reference:
TFN2K Client and Daemon Sections taken from
http://cert.uni-stuttgart.de/archive/bugtraq/2000/03/msg00127.html

TFN2K Client (tfn)
[1;34musage: %s <options>
[-P protocol]
[-S host/ip]
[-f hostlist]
[-h hostname]
[-i target string]
[-p port]
<-c command ID>
change spoof level to %d
change packet size to %d bytes
bind shell(s) to port %d
commence udp flood
commence syn flood, port: %s
commence icmp echo flood
commence icmp broadcast (smurf) flood
commence mix flood
commence targa3 attack
execute remote command

TFN2K Daemon (td)
tribe_cmd *

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

tfn-daemon **
tfn-child **

* Mixter wisely avoids embedding clear-text strings in the TFN2K daemon. However, tribe_cmd, the one function unique to the daemon, is clearly visible and can be detected with any standard grep utility.

** Because, this text is likely to be modified in many TFN2K installations, it may be problematic to definitively identify a TFN2K daemon by traditional virus-scanning means.

TFN2K Daemon and Client (tfn and td)
security_through_obscurity *
D4 40 FB 30 0B FF A0 9F **
64 64 64 64 ... ***
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
/dev/urandom
/dev/random
%d.%d.%d.%d
sh ****
ksh ****
command.exe *****
cmd.exe *****

* This is a function whose definition is generated at compile time. This is a strong (and probably unique) signature.

** This byte pattern is present in both client and daemon, and represents the first eight bytes in the CAST-256 encryption table (displayed in little-endian byte ordering here).

*** A contiguous 128-byte sequence of 0x64 values reveals the presence of the static table used in the Base 64 decoding algorithm.

**** Unix and Solaris systems only

***** Windows NT systems only

The TFN2K binaries may be stripped of clear-text method and variable names, making it difficult to definitively identify the daemon by conventional string-based scanners.

Countermeasures to a TFN2K flood ***(for the target/victim network)***:

- Setup an IDS between the border router and Internet connection to alert on the TFN2K signature that includes at least one trailing 'A' at the end of the packet. *See first bullet point below under* "Detection of TFN2K flood ***(for the target/victim network)"***

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Disallow unnecessary ICMP, TCP, and UDP traffic. Typically only ICMP type 3 (destination unreachable) packets should be allowed.
- If ICMP cannot be blocked, disallow unsolicited (or all) ICMP_ECHOREPLY packets.
- Disallow UDP and TCP, except on a specific list of ports.

Detection of TFN2K flood ***(for the target/victim network):***

- Examine incoming traffic for unsolicited ICMP_ECHOREPLY packets containing sequences of 0x41 in their trailing bytes. Additionally, verify that all other payload bytes are ASCII printable characters in the range of (2B, 2F-39, 0x41-0x5A, or 0x61-0x7A).
- Watch for a series of packets (possibly a mix of TCP, UDP, and ICMP) with identical payloads.
- The UDP packet length (as it appears in the UDP header) is three bytes longer than the actual length of the packet.
- The TCP header length (as it appears in the TCP header) is always zero. In legitimate TCP packets, this value should never be zero.
- The UDP and TCP checksums do not include the 12-byte pseudo-header, and are consequently incorrect in all TFN2K UDP and TCP packets.

DoS Reference:
http://www.securityfocus.com/archive/1/225183

To:	BugTraq
Subject:	RE: Microsoft ISA Server Fragmented Udp Flood Vulnerability
Date:	Nov 5 2001 9:48AM
Author:	Microsoft Security Response Center <secure@microsoft.com>
Message-ID:	<949915AAAC8CED4B823E2B1BBD0B3E7F9F91D0@red-msg-18.redmond.corp.microsoft.com>

```
-----BEGIN PGP SIGNED MESSAGE-----

Hi all,

Wanted to take a moment and clarify this issue that's been posted.

We investigated the issue when it was initially brought to us at
secure@microsoft.com, but this is strictly a flooding attack.  The
script simply sends a huge number of fragmented packets to the
server, and recombining the packets takes the server some finite
amount of work.  Send enough of them,quickly enough, and you can
monopolize the server.  But of course this is true for any server,
not just for ISA.  The attack requires a very high bandwidth between
the attack and the server, and normal processing resumes as soon as
the flooding stops.

ISA can be configured to drop fragmented packets and, if this is
done, it significantly helps protect the system against flooding
attacks like this.  However, even so, it's not a cure-all.  Even
inspecting and dropping packets takes some finite amount of work, and
once again if the attacker has sufficient bandwidth, he may be able
```


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to flood the server. Again, though, there isn't a flaw in ISA server - - - -- it's strictly a flooding attack.

Regards,
secure@microsoft.com

- - - -----Original Message-----
Subject: Microsoft ISA Server Fragmented Udp Flood Vulnerability

- - - - ----[Summary
A fragmented Udp attack through the microsoft isa server makes the system hampered by using the cpu at 100%. Meanwhile server uses processor power too much and therefore packet process ratio decreases.

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

V. References

Book, People and Web References:

SANS GCFW Training Material – by Chris Brenton

Co-worker and Friend, Tom Swint

Co-worker, Nancy Scott

Three Tiered DMZ's by Chris Mahn
http://rr.sans.org/firewall/3_tiered.php

Disabling Unneeded Features and Services on Cisco Internet Gateway Routers
by Toon Mordijck August 13, 2001
http://www.sans.org/infosecFAQ/netdevices/disabling.htm

Screening Router Access List by Frank Keeney
http://Pasadena.net/cisco/secure.html

YASSP Post installation steps by Seán Boran
(includes Tripwire information)
http://www.yassp.org/after.html

Securing Solaris Servers - A Checklist Approach
by Paul D. J. Vandenberg and Susan D. Wyess
http://www.usenix.org/sage/sysadmins/solaris/index.html#host

Lance's Security Papers by Lance Spitzner
http://www.enteract.com/~lspitz/papers.html,

Solaris Security Guide by jrr
http://www.geocities.com/sabernet_net/papers/Solaris.html

Recommended and Security Patches for Solaris from Sun Microsystems
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/xos-7&nav=pub-patches

Phoneboy's Firewall-1 FAQ by Dameon D. Welch-Abernathy
http://www.phoneboy.com

Security Focus
http://www.securityfocus.com

Common Vulnerabilities and Exposures
http://cve.mitre.org/cve/

CERT Coordination Center

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.cert.org/

Cisco Systems
http://www.cisco.com

Tripwire
http://www.tripwire.com

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

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.