

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.

Table of Contents 1
Ruth_Kizlyk_GCFW.doc 2

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

SANS GCFW –track 2

Practical Assignment

GIAC Enterprises

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

Ruth Kizlyk

30Sep2002
GCFW Practical Assignment
Version 1.7 (revised 8Apr2002)

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

Table of Contents

Disclaimer 3

Assignment 1 – security architecture 4

Perimeter Defense Components – Specific Brand and Version 7
GIAC Enterprises Network Design 9

Assignment 2 – security POLICY 15

ASSIGNMENT 2 – BORDER ROUTER 15
ASSIGNMENT 2 - Firewall Policy 17
ASSIGNMENT 2 – VPN Policy 21
ASSIGNMENT 2 – VPN TUTORIAL 22
ASSIGNMENT 2 - TIPS, TRICKS AND GOTCA'S 30

Assignment 3 – Verify the Firewall Policy 31

ASSIGNMENT 3 – AUDIT STRATEGY 31
ASSIGNMENT 3 – AUDIT EXECUTION 33
ASSIGNMENT 3 – AUDIT RECOMMENDATIONS 43

Assignment 4 – design under fire 46

ASSIGNMENT 4 –SELECT NETWORK DESIGN 46
ASSIGNMENT 4 –ATTACK AGAINST THE FIREWALL 47
ASSIGNMENT 4 –A DENIAL OF SERVICE ATTACK 49
ASSIGNMENT 4 –ATTACK PAST PERIMETER 52
Appendix A - Router Policies and Procedures 54
Appendix B - Audit tools 56
Appendix C – Check Point Alerts 58
Appendix D – Nmap Options 62
References and Acknowledgements 64

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

SUMMARY

If anyone out there thinks you can just rely on your Firewall to secure your perimeter, they are sorely mistaken. Today's attacks are directed at Firewalls as well as being designed to past through Firewalls. Solid network security is a combination of security solutions which complement the overall organizations security policies. The individual components contribute to the overall layering providing the best protect for today and tomorrow.

This paper will demonstrate one secure solution for a company with access requirements for their Customers, Suppliers, Partners and mobile staff. The network design and explanation of how access will be securely accomplished are included.

The security policy for the border router, primary Firewall and VPN solutions are detailed. A tutorial on Check Point FW-1 VPN-1 is included.

The third assignment provides an audit of my network design and the final element is attacking another student's network design.

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

Disclaimer

The information contained in this document including but not limited to text, graphics and/or source code is not intended to represent the actual configuration of any known network in use by any individual or corporation.

Products and company names mentioned herein may be the trademarks of their respective owners, and should not lead the reader to infer that the author endorses these products over others that may provide similar functionality.

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

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

Assignment 1 – security architecture

The following secure architecture was designed to support GIAC Enterprises' e-business which deals in the online sale of fortune cookie sayings. The secure architecture was designed to meet the access requirements (and restrictions) for the following groups.

Customers: Companies or individuals can purchase bulk online fortunes using the GIAC secure website. There is a business requirement for customers to be able to browse through company products and other information. Secure links to Business Partner sites provide customer access to additional products. Customers require access to create and update profiles. They require secure access to order company products and follow the order through to delivery. They need to be able to make secure payments for their purchases. Any technical, clerical or administrative support is provided through a help desk or through Internet email.

New customers can apply for an account through the public website. The account is activated after appropriate credit checks are completed. The customer will then authentication with unique username and strong password.

GIAC provides these services and allows communications to their Webserver. Customers will browse to the business site on http (tcp port 80). Customers will log-on with their unique ID and strong password to make purchases and subsequent payments. This is a secure connection using https (tcp port 443). Customers only have access to the WWW server in the DMZ. Email communications will be accepted through SMTP (tcp port 25). The SMTP mail server in the DMZ will forward legitimate mail to the internal mail server.

Customer Traffic Summary			
Business Requirement	Services	Connects To	Access Permitted
Normal web browsing	Http (tcp port 80)	208.18.40.19 (WWW)	208.18.40.20 (perimeter FW)
Secure web browsing	Https (tcp port 443)	208.18.40.19 (WWW)	208.18.40.20 (perimeter FW)
Internet Mail	SMTP (tcp port 25)	208.18.40.18 (SMTP)	208.18.40.20 (perimeter FW)
Secure Link to Partner Site	Https (tcp port 443)	Partner (WWW)	208.18.40.20 (perimeter FW)

Supplier: Companies supplying GIAC Enterprises with fortune cookie sayings need to be able to transfer fortune cookie sayings securely to GIAC. A secure method is required to send invoices and payments. They will have frequent communication with GIAC Accounting department and Operations department.

Suppliers communicate through email through SMTP (tcp port 25) and transfer files through FTP (tcp port 21 and 20) GIAC supplies a VPN tunnel for encrypted communications and transfer of fortune cookie sayings. This VPN connection is from supplier FW to GIAC's FW. The supplier FW is specified as the default Gateway and authorized communications are directed to GIAC. The suppliers

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

will have encrypted access to the Supplier Server in the Supplier VLAN. VPN will be supported by the Check Point FW. Traffic will be encrypted up to the Firewall then passed through eSafe Antivirus Gateway and Real Secure Intrusion Detection. Suppliers will use Secure-Remote ID tokens with one time passwords.

Suppliers Traffic Summary			
Business Requirement	Services	Connects To	Access Permitted
Internet Mail	SMTP (tcp port 25)	208.18.40.18	208.18.40.20 (perimeter FW)
File Transfers	FTP (tcp port 21) FTP-Data (tcp 20)	Supplier VLAN	208.18.40.20 (perimeter FW) and RSA Ace Server authentication and Switch authentication
VPN Connection	VPN-1 Encryption	FW to FW	208.18.40.20 (perimeter FW)
Token Authentication	SecurID (tcp)	RSA ACE Server	208.18.40.20 (perimeter FW)

Partners: GIAC's partners are located in several different countries. Their business is to translate and resell the fortune cookie sayings. All partners need to share products and information with GIAC Enterprises. GIAC Enterprises is the central repository and communications are primarily required between the individual partner and GIAC. Partners will be sending confidential corporate information. They have regular interaction with all departments and participate in Strategic Planning and Development.

Partners contribute transfer sayings through FTP (tcp port 20/21). They require access to Shared Corporate Data inside the network through NetBIOS (tcp/udp ports 135 -139, 445). Mail is confidential and sent by encrypted VPN tunnel using SMTP (tcp port 25). Access is provided through FW to FW VPN connections. VPN will be supported by the Check Point FW. Traffic will be encrypted up to the Firewall then passed through eSafe Antivirus Gateway and Real Secure Intrusion Detection. Partners will all use Secure-Remote ID tokens with one time passwords

Partner Traffic Summary			
Business Requirement	Services	Connects To	Access Permitted
Internet Mail	SMTP (tcp port 25)	208.18.40.18	208.18.40.20 (perimeter FW)
File Transfers	FTP (tcp port 21) FTP-Data (tcp 20)	Shared VLAN Shared VLAN	208.18.40.20 (perimeter FW) and RSA Ace Server authentication and Switch authentication
File Sharing	NetBIOS (tcp/udp 135-139, 445)	Shared VLAN	208.18.40.20 (perimeter FW) and RSA Ace Server authentication and Switch authentication
VPN Connection	VPN-1 Encryption	FW to FW	208.18.40.20 (perimeter FW)
Token Authentication	SecurID (tcp)	RSA ACE Server	208.18.40.20 (perimeter FW)

GIAC Enterprises employees: There are 400 employees that work on site at GIAC Enterprise's internal network. Most require full Internet access but some are restricted to a defined set of business sites. All employees will have internal mail and Internet mail to communicate with Partners, Suppliers and Customers.

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

In order to provide this communication GIAC will allow SMTP (tcp port 25) traffic to the outside world. Additionally the non-authoritative DNS server must communicate through Domain (udp port 53) to connect to the Authoritative DNS service of the ISP.

Employee Outbound Traffic Summary			
Business Requirement	Services	Connects To	Access Permitted
Internet Mail	SMTP (tcp port 25)	Exchange Server	208.18.40.20 (perimeter FW)
Restricted File Transfers/ Downloading	FTP (tcp port 21) FTP-Data (tcp 20)	Most external site	208.18.40.20 (perimeter FW) and Websense and ESafe antivirus and content filtering.
Restricted web browsing	Http (tcp port 80)	External Webservers	208.18.40.20 (perimeter FW) and Websense and ESafe. Critical Data VLAN also restricted by Internal FW.
Restricted Secure web browsing	Https (tcp port 443)	External Webservers	208.18.40.20 (perimeter FW) and Proxy Server and Websense and ESafe Critical Data VLAN also restricted by Internal FW.

Other Traffic Summary			
Business Requirement	Services	Connects	Access Permitted
Intrusion Detection Sensors	RS (tcp ports 902, 2998)	Proxy, SMTP, WWW to Real Secure Intrusion Detection Server	208.18.40.20 (perimeter FW)
Name Resolution	DNS (udp port 53)	ISP DNS Server	208.18.40.20 (perimeter FW)
Time Syncing	NTP (udp port 123)	External Time Server	208.18.40.20 (perimeter FW)
Content Scanning	Http (tcp port 80) Https (tcp port 443) Ftp (tcp port 21) Smtp (tcp port 25)	Websense and ESafe	208.18.40.20 (perimeter FW)

GIAC Enterprises Mobile Staff: There is a team of employees working remotely that require access to shared files and to their internal email. Policy states they won't have direct access to the highly secure Database VLAN. They will require dialup access from home or from client site. They will need access to their internal mail, their personal files and shared data.

This team of employees will use their laptops to connect to GIAC Enterprises through VPN connection. VPN will be supported by the Check Point FW. Traffic will be encrypted up to the Firewall then passed through eSafe Antivirus Gateway and Real Secure Intrusion Detection. Employees will all use Secure-Remote ID tokens with one time passwords. They will access the internal Exchange mail server and shared file servers on internal and files services which all included in the Shared VLAN. They will use SMTP (tcp port 25) and NetBIOS (ports 137-139, 445) for access to file shares on the Internal network. These services will communicate through the established secure VPN connection.

Mobile Staff Traffic Summary			
Business Requirement	Services	Connects To	Access Permitted
Internet Mail	SMTP (tcp port 25)	208.18.40.18	208.18.40.20 (perimeter FW)

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

File Transfers	FTP (tcp port 21) FTP-Data (tcp 20)	Shared VLAN Shared VLAN	208.18.40.20 (perimeter FW) and RSA Ace Server authentication and Switch authentication
File Sharing	NetBIOS (tcp/udp 135-139, 445)	Shared VLAN	208.18.40.20 (perimeter FW) and RSA Ace Server authentication and Switch authentication
VPN Connection	VPN-1 Encryption	FW to FW	208.18.40.20 (perimeter FW)
Token Authentication	SecurID (tcp)	RSA ACE Server	208.18.40.20 (perimeter FW)

GIAC Secure Infrastructure: This network design supports the business requirements of the Customers, Suppliers and International Partners, as well as GIAC security policies. GIAC had a Security Policy backed by senior management. They expect layered security, secure Internet access and protection of the Critical Data VLAN.

GIAC implemented a switched environment which supports several Virtual LANs (VLANs) which provides access and restrictions for different groups of resources and employees. The Critical Data VLAN had to be the most secure from viruses and loss of data. Employees that work primarily with this data have restricted Internet browsing access and only have access to a predetermined list of business sites. Secure https (tcp port 443) SSL sites included in the predetermined list are bridged by ISA Proxy Server so encrypted traffic is not allowed into this VLAN.

All VLANs have further browsing restrictions by Websense URL Filtering on adult sites. Check Point Firewall rules restricts FTP (tcp port 20 and 21) downloading to all employees. HTTP (tcp port 80) downloading is restricted by eSafe Gateway AntiVirus which scans and blocks extension such as .exe and .com. The ESafe Antivirus Gateway also blocks spamming using a list of "forbidden words". All employees can request downloads through a Centralized process. All employees have internet email which is to be used primarily for business purposes. This is specified in the Information Security and Computer Usage Policies.

Perimeter Defense Components – Specific Brand and Version

The Secure Architecture includes the following primary perimeter components:

- Cisco 3550 Filtering Router Version Enterprise Set Version 12.X
- Check Point Firewall Version 4.1 Build 4XXX, Service Pack 6
- VPN on Check Point Firewall Version VPN-1™ and FW-1 Version 4/10, Build 41514 VPN+DES+Strong

Additional security component on the diagram include

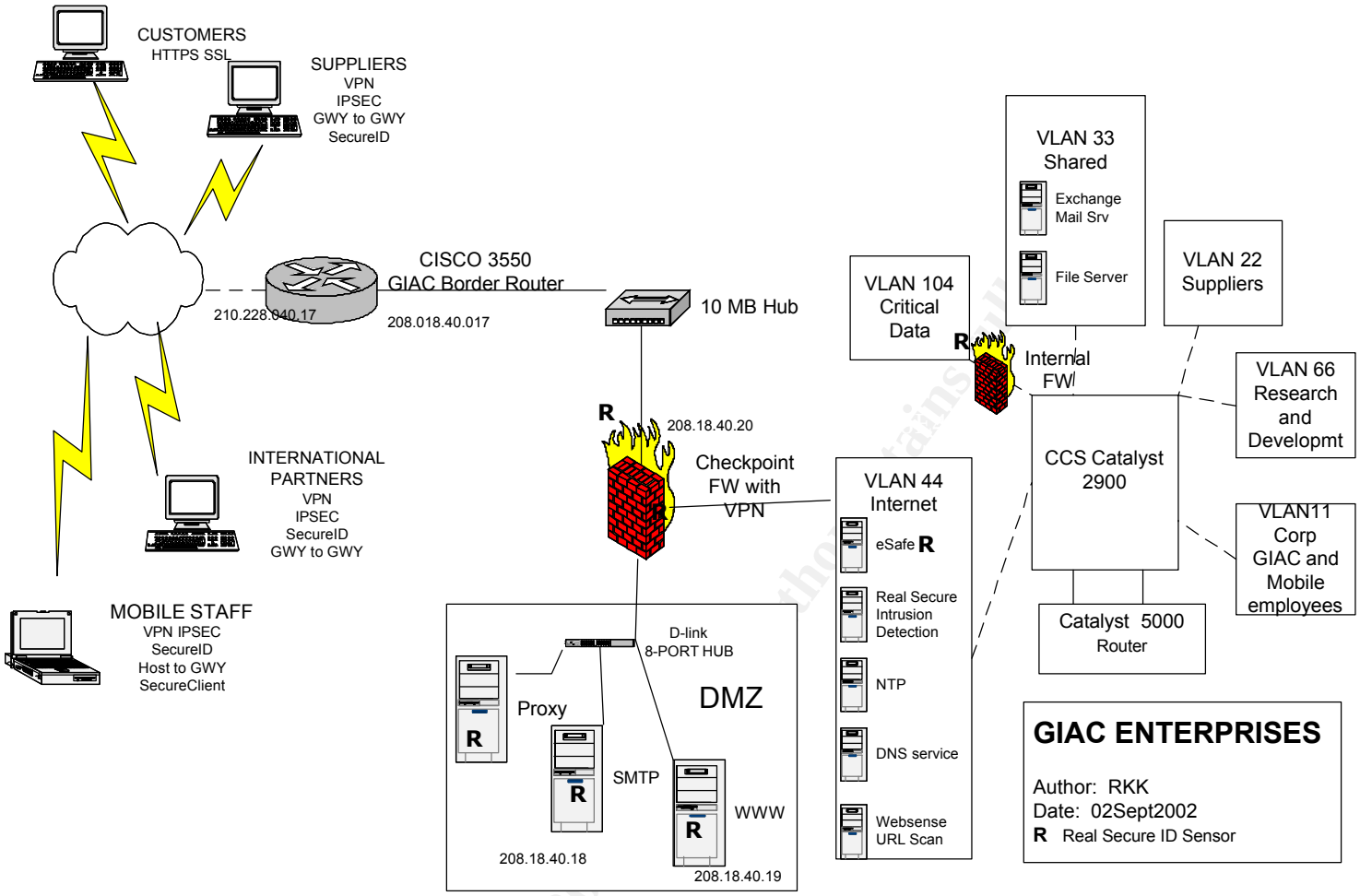
- Catalyst 2900 switch and Catalyst 5000 router CAT Version 5.4 (2) and CISCO OS 12.1

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

- Check Point Internal Firewall Version 4.1 Build 41506
- Real Secure Intrusion Detection System Version 6.6.2002.155, network sensor 7.0.2002.155.9, o/s sensor 6.5.2002.100 (SR3.3)
- Esafe Antivirus Gateway Version 3.1.96.8, eConsole 3.1.94.10
- Websense URL filter Version 4.3, Websense Reporter v6.2, Websense manager4.4.3, build 20001020

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

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



GIAC Enterprises Network Design

Each component in the above diagram plays a distinct security role and is placed to create layered security for GIAC Enterprises. The following explanations describe the purpose of each component, the security function or role it carries out, and how the placement of the component on the network allows it to fulfill this role.

- Cisco 3550 Filtering Router: The purpose of the perimeter router is to direct traffic to the Firewall. The security function is to provide the first layer of defence in blocking traffic according to the access control list. If the router is configured properly, some unwanted traffic is blocked at the router instead of the Firewall. This of course increases the efficiency of the Firewall. If the router prevents some unwanted traffic and directs appropriate traffic then its ACL is complimenting the FW policies and fulfilling its role.
- Check Point Firewall: The Check Point FW-1 4.1 is running on a Compaq machine running Windows 2000. The purpose of the Firewall is

Created on 9/26/2002 9:13 PM
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to provide a layer of protection between the trusted (inside) network and the untrusted (Internet). Additionally if specifies access policies in and out of the DMZ. Public access is only permitted to the SMTP Mail server and the Webserver. The security function is to provide ingress and egress filtering based on GIAC Enterprise polices. Any traffic not explicitly allowed or denied by Firewall rule is denied. Network Address translation (NAT) is performed to hide the private internal network addresses.
The Firewall is placed at the entrance to the network and DMZ to create a secure single-point of entry. A properly configured and maintained Firewall is an essential security component. Check Point Firewall was selected because it is OPSEC compliant. OPSEC (Open Platform for Secure Enterprise Connectivity) means FW supports other vender's products. Check Point provides stateful inspection, integrated VPN and authentication options like SecurID.

- VPN on Check Point Firewall: FW-1/VPN-1 solution enables VPN communication from Firewall to Firewall or from client to Firewall. It was chosen as a proven solution with encryption, authentication and access controls. The encrypted traffic is terminated at the Firewall to ensure content scanning by eSafe Gateway before traffic enters the network. SecurID (token authentication) is supported by Check Point Firewall. The RSA Ace authentication client is installed on the Firewall. This enforces two-factor authentication from the source of the VPN as well as another authentication to the resource on the inside network. Policy states any employee granted VPN access must run a personal Firewall. This provides another layer of protection for the Mobile User. SecureClient integrates a personal firewall with the VPN solution. The security administrator can verify personal Firewall settings are not changed, can correct changes or deny access if the settings are changed. This product is a proven technology. The VPN solution fulfils its role of ensuring authentication, secure transfer of data, access restrictions and requirement to filter inbound traffic through eSafe Gateway and other AV products.

- Catalyst 2900 and 5000 switch and router: Even with a strong perimeter router and Firewall in place it is still wise to restrict traffic further. This purpose of this switch is to provide an additional layer of security by creating virtual LANs (VLANS) which contain resources and workstations. Its security function is to control traffic into or out of VLANS based on switch access control lists. Access control lists are based on a combination of extended and reflexive access list which can include protocol, service or port or specific IP. All VLAN servers and workstations connecting to the Catalyst 2900 and 5000 access the switched network with designated port based on specific MAC address. A connection attempt by an unspecified MAC will shut down the port. The placement of this component inside the firewall is the net layer of

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

control for traffic which has passed through the perimeter Firewall.

- Check Point Internal Firewall: This Firewall provides an additional layer of protect to the mission critical servers within the Critical Data VLAN. All internal traffic to this VLAN must pass through this Firewall. Using a different product than the primary Firewall reduces risk of exploiting both using the same vulnerability. However in this case the same FW product was used. This Internal Firewall is another layer of protection for the Critical Data. This provides additionally policies to restrict traffic. These policies will match or compliment the ACL's on the switch providing double the protection in the event traffic slips past the first control. If malicious traffic finds its way into the network through a backdoor or through a virus the firewall blocks traffic from internal users and other VLANs. Additionally it provides another layer from the Suppliers and International Partners which have VPN access to network resources.

- Real Secure Intrusion Detection: This intrusion detection system is in place to provide real time alerts based on known signatures or changed host information. There is one network sensor and several host sensors which provide the security function of sending alerts to the console. The network sensor is placed outside the Firewall to get a flavor of all traffic knocking at the door. The host sensors provide alerts on the webserver, the critical Database server, SMTP, Proxy and the eSafe server. The placement of the sensors (some of which are in the DMZ) result in the necessity for traffic to pass to the console (inside the network). Firewall rules are created to allow this traffic. However, the monitoring of traffic on critical boxes in the DMZ is a necessary element of total network security. Note also that port scanning is required for ID to function in a switched environment.

- ESafe Antivirus (AV) Gateway: The AV product provides the main or first layer of AV protection. All traffic is directed by the Firewall to ESafe AV Gateway so it can fulfil its security role to scan content of incoming and outgoing traffic for known signatures. It can react to undesirable content by stripping attachments, quarantining mail or blocking file types. This is placed to work with the Firewall and provide egress and ingress content scanning. It provides the primary AV scanning. Desktop and server antivirus is implemented with different products. This provides AV defence in depth in case one product misses a signature that the next product may catch.

- Domain Name Service (DNS): DNS is the online distributed database system used by Internet to map names into IP addresses. DNS resolution is provided by the GIAC DNS server and GIAC's ISP. GIAC DNS server is non-authoritative meaning it only stores name resolution for previously cached or manually entered records. GIAC DNS server will forward lookup requests to the primary and backup ISP's DNS servers. The GIAC

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

DNS server also provides alternate DNS servers if both ISP's DNS servers are not available. This provides a secure method to do name resolution without the vulnerabilities of zone transfers. The firewall only allows Domain (udp port 53) traffic out to specified DNS servers. If the DNS server was listening on Domain (udp port 53) then it would be prudent for it to be placed in the DMZ.

- Websense: The purpose of Websense URL filter is to support the company policy of web access control. It achieves this security function by comparing browsing attempts against its URL database. This allows administrators to control access to undesirable or inappropriate sites. It will deny access to the sites specified. The Critical Data VLAN is restricted to a list of approved business sites. Only these sites can be accessed by employees or resources in this VLAN. Websense is placed to work with the Firewall. The firewall will check all web connection attempts against Websense.

- Network Address Translation (NAT) The purpose of NAT is to conceal internal IP addresses from the Internet. This protects private internal address from being known in the outside world and enables routing to final destination. The function is to replace the source IP address with an address from the Firewall NAT table. When a reply is sent back, the Firewall replaces the destination IP address with the original source IP. This ensures the reply is sent to the correct host.

- Network Time Protocol (NTP) The purpose of NTP is to synchronize network time for coordination of events and matching log entries. All secure gateways and primary servers will synchronize their system clocks to the NTP server. The NTP server synchronizes to the Navy time Server. The Firewall Policy allows this one box out to the time server on NTP (udp port 123). This security function is essential to correlate events between different logs and critical if legal evidence is required.

- DMZ Servers: (This may be more appropriately called the 'service network', however this paper will continue with calling it the DMZ). The purpose of placing boxes in the DMZ is to limit exposure to boxes which have high external traffic and could more likely be compromised. The Proxy (or SSL Bridging), SMTP (mail server) and the Webserver reside in the DMZ.

  The purpose of Proxy or ISA Server is to provide SSL Bridging for staff in the Critical Data VLAN. This security is required so encrypted HTTPS traffic is bridged to HTTP traffic and can be content scanned by eSafe Gateway. The Firewall directs traffic to the proxy and to eSafe to fulfil its role. Staff in the Critical Data VLAN must have their Proxy setting specified for this box.

  The purpose of the SMTP mail server is to relay valid SMTP (tcp port 25)

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

traffic to the internal mail server. The firewall policy allows this traffic and restricts to specific boxes. It works with eSafe AV Gateway to perform appropriate scanning of mail and attachments. The ISP provides mail services and forwards mail to the SMTP server. The SMTP is placed in the DMZ as another layer of protection. The box is monitored by host sensors and hardened to industry standards. Additional controls restrict the size of attachments to prevent intentional or unintentional large transfer of data. Other controls restrict the number of recipients in one mailing. This prevents possible spamming.

The Webserver's purpose is to provide web-based information to customers, suppliers and staff. The Webserver is the most visible server and first contact to most external traffic. This box is listening on http (tcp port 80) and https (tcp port 443) and will attract the most attention. Port 80 is consistently one of the top attacked ports. The security function is to perform its functionality without being attacked, defaced, compromised or brought down with a denial of service attack. It is essential that this box is hardened and maintained with the latest patches and service packs. The Firewall only allows http (tcp port 80) and https (tcp port 443) to this box.

Any traffic from the DMZ to the inside network is rejected and an alert is sent. The reverse is also alerted on. Any traffic from the Inside network to the DMZ is 'rejected'. All boxes in the DMZ are monitored with a host intrusion detection sensor.

Justification

Any network design can introduce risks in order to provide the functionality required. The trick is to mitigate those risks until they are acceptable to the Security Architect and the business owners. This solution offers layers of protection and meets the functional requirements of GIAC Enterprises. GIAC is leveraging the strengths of several different technologies. Layered security is accomplished with 'static packet' filtering at the border router and 'stateful inspection' at the Firewall. All servers are hardened according to policy. Continual monitoring and maintenance is required to keep the perimeter secure. Logs and alerts must be monitored. Service packs, patches and operating systems must be upgraded with the latest stable versions.

When designing this network there was considerable debate about allowing the Suppliers to the Internal network. However, based on the business requirement to provide access to this long=standing, established supplier and their limited access to one server, the decision was made to allow access. Management was not prepared to purchase another Firewall or introduce another DMZ at this time. The risks of allowing external parties into the network are mitigated by FW restrictions, VPN traffic, SecurID authentications and VLAN restrictions.

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

Some VPN connections allow any services. Access was restricted to just the services required. Another concern was allowing Mobile Staff VPN access from their laptops. Policy states Personal Firewalls will be installed prior to allowing VPN access. The additional use of SecurID enforces token authentication. SecureClient enforces a desktop policy to ensure that Internet browsing can not occur during a VPN connection.

External traffic of International Partners and Mobile Staff are also allowed into the internal network through an established VPN tunnel to the FW. Traffic is only allowed into the Shared VLAN. All resources are protected with antivirus software and traffic is contained within those VLANs.

GIAC has grown into this architecture. Initially the company struggled with development of Internet Security Architecture Policies. The policies were approved by senior management and discussed with external auditors. The architecture was then built to support the policies. Through each phase of implementation the security was analysed internally and by external auditors. Not all components of the proposed infrastructure were introduced at first. Intrusion detection systems, VPN access and internal Firewall followed original implementation as budget and resources became available. Additional elements will be added in the future including centralized logging and alerting server.

© SANS Institute 2000 - 2002 All rights reserved.

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

Assignment 2 – security POLICY

The following security polices for the border router, primary Firewall and VPN are based on the security architecture defined in Assignment 1.

ASSIGNMENT 2 – BORDER ROUTER

The border router is the first line of defence. The primary function is often basic routing functionality. However, as the first line of defence, the border router should also block explicitly denied traffic.
Some routers providing service to GIAC are owned or managed by third parties. All routers however follow GIAC policy. The router should be hardened and configured to follow GIAC Router Policy (Appendix A). The router will be running the latest stable operating system. Best practices are followed to ensure backups are available in event of a disaster. Change management procedures ensure router configurations are tested before being deployed and that security is not affected during the change. Strong passwords are kept in a vault along with the community string names. Physical access to routers is also restricted. Login banners are used on all routers.
Global configurations include the login banner, timestamps, restricting ftp access to least required access and log buffering. Source routing, tcp/udp small services and cdp run can also be blocked. These commands are necessary to block attacks or stop attempts to gain reconnaissance. The *Interface configurations* are unique for each interface. A border router should prevent ip directed broadcasts. SNMP is not used at GIAC due to recent vulnerabilities. The no snmp command is used to prevent SNMP from entering the network. The following commands will prevent attempted reconnaissance. No cdp enable, no ip unreachables, no ip redirects. *Access List*s can be standard, extended or reflective. Groups of access lists are identified by number and applied to specific interface as inbound or outbound.

Inbound rules for serial interface	General Purpose and importance
access-list 110 deny 10.0.0.0 0.255.255.255 log	blocks and logs all traffic from private address
access-list 110 deny 127.0.0.0 0.255.255.255 log	blocks and logs all traffic from the loop back address 127.*
access-list 110 deny 172.16.0.0 0.15.255.255 log	blocks and logs all traffic from the private addresses range
access-list 110 deny 192.168.0.0 0.0.255.255 log	blocks and logs all traffic from private address
access-list 110 deny 224.0.0.0 15.255.255.255 log	blocks and logs all traffic from multicast address range
access-list 110 deny 0.0.0.0 log	an invalid address and should be blocked and logged.
Access-list 110 deny tcp any any range ftp telnet log	Telnet passes user name and passwords in the clear and therefore should be denied and logged.
Access-list 110 deny udp any any eq sunrpc log Access-list 110 deny tcp any any eq sunrpc log Access-list 110 deny udp any any eq 2049 log Access-list 110 deny tcp any any eq 2049 log Access-list 110 deny udp any any eq 4045 log Access-list 110 deny tcp any any eq 4045 log	Remote Procedure Call (RPC) should be blocked so devices can not be used to execute programs on other devices.

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

Access-list 110 deny udp any any eq 135 log Access-list 110 deny tcp any any eq 135 log Access-list 110 deny udp any any range 137 Access-list 110 deny udp any any range 138 Access-list 110 deny tcp any eq 139 log Access-list 110 deny udp any any eq 445 log Access-list 110 deny tcp any any eq 445 log	These lines block NetBIOS services which are not considered secure due to numerable vulnerabilities. Win2000 servers listen on port 445.
Access-list 110 permit tcp any any established	This line permits inbound tcp packets that represent connections established by clients on the internal network.
Access-list 110 permit tcp any host 208.18.40.19 eq http log Access-list 110 permit tcp any host 208.18.40.19 eq https log Access-list 110 permit tcp any host 208.18.40.18 eq smtp log Access-list 110 deny ip any any log	Public access is only allowed to the SMTP mail server (208.18.40.18), and the webserver (208.18.40.19).
Order and other considerations Once an accept rule has been applied, denials are inherent. It is beneficial to add a final "Deny ip any any" as the last rule. By adding in the rule, the number of entries matching that rule can be attained. The rule can also be modified to "log" denied entries. The log is also helpful for investigation.	

Access List for Internal Ethernet interface	General Purpose and importance
access-list 100 permit ip 208.18.40.20 0.0.0.255 any access-list 100 deny ip any any	Allows internal network addresses to go to the Internet. Efficiency is gained by apply these rules to the internal interface and sharing the traffic load between the route interfaces.
ip access-group 100 in no snmp no ip directed-broadcasts no ip unreachables no ip redirects no cdp enable	Secure by preventing reconnaissance through snmp and ip directed broadcasts. Prevent return of message by turning off response of ip unreachables, and router reconnaissance through cdp.

Your router can be verified using the Router Audit Tool (RAT). Follow this link for information on how the free product works and to see output from the audit tool. http://ncat.sourceforge.net/

© SANS Institute 2000 - 2002

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

ASSIGNMENT 2 - Firewall Policy

The following Firewall security policy is based on the security architecture defined in Assignment 1. The specific rule set reflects GIAC business requirements and provides secure access for customer, suppliers, partners, remote staff and internal staff.

The Firewall plays an important role in the security of GIAC and therefore is subject to appropriate change controls. The philosophy is that all access is denied until there is a business requirement and it can be securely implemented. The FW rules are based on GIAC policies as determined by the governing security body called the GIAC Security Team (GST). The Firewall log is monitored daily. The rules can only be changed in the presence of two authorized staff. Additional ports can not be opened without the approval of the GST.

The box used for the Firewall was hardened to industry standard and the latest stable patches and service packs were applied. Patches are applied for any specific Check Point vulnerabilities.

RULES	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	General Purpose and Importance Order and Other Considerations
Rule 0	IMPLIED RULES					Check Point default allows specific port traffic through without logging or restriction. Review the settings in Properties and deselect all except the settings which match your policies. GIAC has deselected all default settings.
Rule 1	Any	www.giac.ca	http, https	Accept	Long	Rule accepts all http (tcp port 80) and https (tcp port 443) connections from any source including internal sources.
Rule 2	Authorized Download Group Only	Any	http ->blocked sites from websense ftp, http, smtp	Reject	Long	Websense is checked to see if the site is blocked and will send a blocked message.
Rule 3	Authorized Download Group Only	Any	http (tcp port 80), https (tcp port 443) and Ftp (tcp 21)	Accept	Long	If the download is performed from an authorized download box (identified by static IP) it will be scanned by ESafe and then accepted.
Rule 4	DNS service	ISP DNS Server 1 ISP DNS Server 2 Alternate DNS servers	Domain-udp port 53	Accept	Long	This rule accepts domain (udp port 53) connections forwarded from GIAC non-authoritative DNS service to the ISP's authoritative DNS servers. There are no zone transfers.
Rule 5	Internal NTP Server	External NTP Server	NTP	Accept	Long	Allow internal NTP server to sync to specified external Time server on NTP (udp port 123)
Rule 6	HTTPS Scan	Any	http URI Scan	Accept	Long	Esafe content scanning before being passed to the Proxy for SSL Bridging.
Rule 7	Proxy or ISA Server	Any	https, http	Accept	Long	Allows SSL bridged traffic to final destinations.
Rule 8	Inside Networks	Any	Http Blocked File Sites	Reject	Alert	Websense http URL filtering of adult sites.
Rule 9	Critical Data Vlan	Any	Https Blocked Sites	Reject	Long	This rule blocks encrypted HTTPS traffic into the Critical Data VLAN. The traffic must be proxied with SSL bridging...
Rule 10	Inside Networks	Any	Http Blocked sites scan	Accept	Long	ESafe HTTP content filtering. M-Sat 7-6:00.

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

Rule 11	Inside Network	Any	Ftp -> Scan content	Accept	Long	ESafe FTP content filtering M-Sat 7-6:00
Rule 12	Partner FW Supplier FW GIAC FW	Partner FW Supplier FW GIAC FW	IPSEC	Accept	Long	This rule allows IPSec traffic between Firewall to Firewall for International Partners, Suppliers and Mobile Staff.
Rule 13	Supplier Staff	Supplier VLAN	ftp, smtp	Client Encrypt	Long	Allows ftp (tcp port 20/21) for supplier staff to one server in Supplier VLAN only.
Rule 14	Partner Staff	Shared VLAN	ftp, smtp, NetBIOS	Client Encrypt	Long	Partners are allowed ftp (tcp port 20/ 21) access, SMTP (tcp port 25) and file sharing privileges.
Rule 15	Mobile Staff	Shared VLAN	ftp, smtp, NetBIOS	Client Encrypt	Long	GIAC mobile staff will only be allowed access to file resources, ftp (tcp port 20/21) and their mail through SMTP (tcp port 25)
Rule 16	Any	FW1 208.18.40.20	Firewall1	Accept	Long	This rule allows VPN access to exchange secure key information (tcp port 265) Check Point VPN-1 Public Key Transfer Protocol
Rule 17	Firewall	RSA Ace Server	SecurID	Accept	Long	This service allows encrypted communication between the SecurID client on the FW and the RSA Ace Server for verifying authentication. (tcp port 264) Check Point VPN-1 SecuRemote
Rule 18	**X** Internal	Mail.giac.ca 208.18.40.18	SMTP Scan -> SMTP in	Accept	Long	Rule accepts source of ANY except not from an internal source and allows to destination of SMTP mail. ESafe scans SMTP (tcp port 25) connections. Must match on address or *@giac.ca
Rule 19	SMTP Internal address	Exchange Server	SMTP	Accept	Long	This rule ONLY accepts SMTP Mail Transfer from SMTP server in DMZ to internal mail server on SMTP (tcp port 25) connections. Only SMTP can forward mail to Exchange server.
Rule 20	Exchange Server	SMTP	SMTP -> Scan Out	Accept	Long	This rule accepts outbound SMTP (tcp port 25) connections from Exchange to SMTP box in the DMZ. This traffic is passed through ESafe SMTP scanning.
Rule 21	SMTP	External ISP SMTP Relays 1 and 2	SMTP	Accept	Long	This rule accepts outbound SMTP (tcp port 25) connections from SMTP Mail Transfer to External ISP SMTP relays 1 and 2.
Rule 22	Real Secure Intrusion Detection Server	FW1 208.18.40.20 GIAC_Web Proxy Server	Real Secure (tcp 2998 and 902)	Accept	Long	Allow Real Secure console access to O/S and network Sensors
Rule 23	FW1 208.18.40.20 GIAC_Web Proxy Server	Real Secure Intrusion Detection Server	Real Secure (tcp Port 2998)	Accept	Long	Allow RealSecure OS-Sensor traffic to ISS Console
Rule 24	DMZ-Net	Inside Networks	Any	Reject Alert	Alert	Protect local net from the DMZ
Rule 25	Inside Networks	DMZ-Net	Any	Reject Alert	Alert	Protect DMZ from the local net
Rule 26	Inside Networks	Any	A-Std Allowed (http- tcp port 80, https tcp port-443)	Accept	Long	Supported Protocols for Internal VLANS
Rule 27	Any	Any:	Silent Services (bootp, nbdatagrams, nbname, nbsession)	Drop		Silent Drop for braodcast packets
Rule 28	Any	Any	Any	Drop	Long	**Last Rule and Importance of Order: This rule drops all other traffic that was not allowed by previous rules.**

Firewall Spoofing: The "Interface Properties – Security "tab can be set to prevent spoofing. Each of the LAN and DMZ interface should be set to "this net". This restricts source IP to addresses on that network. The Internet interface should allow any but the internal and DMZ addresses.

Syn Flood: In "Properties Setup" under the SYNDefender tab, Passive SYN

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

Gateway was selected. This ensures state is maintained by tracking the three-way handshake.

Firewall Sign on: Access to the Firewall is restricted to few employees. Logon is accomplished by individual ID. Once logged in, the Log viewer is also accessed with a second password.

Firewall Log monitoring Procedures: The log is reviewed daily. Review is recorded and pertinent information is shared between those responsible for monitoring the FW. There are different ways to export and sort data for review. These are some areas which should be reviewed.

1. ICMP - Verify all external ICMP messages should be dropped at the Firewall.
2. Port Scanning – Look for attempts to scan ports from specific IP or range of IPS.
3. SMTP only to expected SMTP resources. Anything outgoing should only be going to ISP IP address.
4. Domain: Filter on service of Domain and ensure only expected traffic is accepted.
5. FTP: Look for unauthorized downloading on FTP (tcp port 20/21). Only authorized static IP's should have accepted FTP transactions logged.
6. Follow-up on any recent suspicious activity to ensure no further action is necessary.
7. Check ports that are commonly probed and attacked. Even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. For example search for telnet (tcp port 23), SSH (tcp port 22) and NetBIOS (tcp/udp 137-139, 445). Sans recommends blocking the following Common Vulnerable Ports as found at http://www.sans.org/top20/

Appendix A – Common Vulnerable Ports

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

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

In this section, we list ports that are commonly probed and attacked. Blocking these ports is a minimum requirement for perimeter security, not a comprehensive firewall specification list. A far better rule is to block all unused ports. And even if you believe these ports are blocked, you should still actively monitor them to detect intrusion attempts. A warning is also in order: Blocking some of the ports in the following list may disable needed services. Please consider the potential effects of these recommendations before implementing them.

Keep in mind that blocking these ports is not a substitute for a comprehensive security solution. Even if the ports are blocked, an attacker who has gained access to your network via other means (a dial-up modem, a trojan e-mail attachment, or a person who is an organization insider, for example) can exploit these ports if not properly secured on every host system in your organization.

1. Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)
2. RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)
3. NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 – earlier ports plus 445(tcp and udp)
4. X Windows -- 6000/tcp through 6255/tcp
5. Naming services-- DNS (53/udp) to all machines which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp)
6. Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)
7. Web-- HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.)
8. "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
9. Miscellaneous-- TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/udp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp)
10. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages **except** "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses.)

In addition to these ports, block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses. Also block source routed packets or any packets with IP options set.

8. Search also for unexpected services like DNS (udp port 53). Verify SMTP (tcp port 25) is only directed to approved mail servers.
9. Follow-up on suspicious activity by checking other logs. Suspicious traffic is often directed at the web server. The IIS logs can be verified to determine what activity occurred.

IIS CODE:
200 = Successful - OK
206 = Successful - Partial Content
304 = Redirection - Not Modified
400 = Client Error - Bad Request
403 = Client Error - Forbidden
404 = Client Error - Not found
500 = Server Error - Internal Server Error

IIS FIELDS:
Follow-up on the GETS from suspicious IP. The following data is included in this field.

cs-uri-stem ie: /winnt/system32/cmd.exe
cs-uri-query ie: /c+%64%69%72
sc-status ie: 404 604 171 0 HTTP/1.0
sc-bytes ie: 404 604 171 0 HTTP/1.0 (server to client)
cs-bytes ie: 404 604 171 0 HTTP/1.0 (client to server)
time-taken ie: 404 604 171 0 HTTP/1.0
cs-version ie: 404 604 171 0 HTTP/1.0
cs(User-Agent) ie: Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98;+DigExt) - -
cs(Cookie) ie: ASPSESSIGQGGZE=JKDLFMJBNMJBGOGMKAKOMOJE http://www.anysite/
cs(Referer) ie: http://www.anysite/nav.htm

[cs-uri-stem] is the document that has been requested; [cs-uri-query] is the query string that was sent as part of the request being logged; [sc-status] is the status code returned by the server; [sc-bytes] is the number of bytes

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

that have been returned to the user; [time-taken] is the time in milliseconds that it took for the server to complete the processing of the request; [cs(Cookie)] is the cookie, or persistent data in the request; and [cs(Referer)] is the URL of the previous site visited by the user.

10. Periodic Checks may find unauthorized changes resulting from an undetected compromise.

- Check for most recent file added
- Check for hidden files with dir/ah
- See what services are running in Control Panel->Devices
- Check for new executables with dir\winnt*.exe/s/t
- Check for ports listening with netstat –a
- Check for statistics and ICMP activity as netstat –s

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

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

ASSIGNMENT 2 – VPN Policy

The policies for VPN are Rules 12-17 specified on the Check Point Firewall. The suppliers and international partners use VPN connection from secure gateway to secure gateway. Specific IPs are entered under Rule12 to allow these connections. Mobile Staff will also use VPN connection from host to secure gateway. All VPN connections require an additional layer of security by requiring RSA ACE SecureID authentication. Further details will follow in the tutorial.

Rule 12: Basic VPN Rule for Check Point FW-1						
Source	**Destination**	**Service**	**Action**	**Track**		
Partner FW Supplier FW GIAC FW	Partner FW Supplier FW GIAC FW	IPSEC	Accept	Long		This rule allows IPSec traffic between Firewall to Firewall for International Partners, Suppliers and Mobile Staff.
Rule 13: Additional VPN Rule for Supplier Access						
Source	**Destination**	**Service**	**Action**	**Track**		
Supplier Staff	Supplier VLAN	ftp, smtp	Client Encrypt	Long		Users will only be allowed access to specific resources using specific services; ftp (tcp port 20 and 21) and smtp (tcp port 25)
Rule 14: Additional VPN Rule for Partners Access						
Source	**Destination**	**Service**	**Action**	**Track**		
Partner Staff	Shared VLAN	ftp, smtp, NetBIOS	Client Encrypt	Long		Users will only be allowed access to specific resources using specific services; ftp (tcp port 20 and 21) and smtp (tcp port 25). Additionally file access is provided through NetBIOS (tcp/udp 135-139, 445)
Rule 15: Additional VPN Rule for Mobile Staff Access						
Source	**Destination**	**Service**	**Action**	**Track**		
Mobile Staff	Shared VLAN	ftp, smtp, NetBIOS	Client Encrypt	Long		Users will only be allowed access to specific resources using specific services; ftp (tcp port 20 and 21) and smtp (tcp port 25). Additionally file access is provided through NetBIOS (tcp/udp 135-139, 445
Rule 16: Additional VPN Rule for Exchanging Secure Key Information						
Source	**Destination**	**Service**	**Action**	**Track**		
Any	Firewall	Firewall1	Accept	Long		This rule allows VPN access to exchange secure key information.
Rule 17: Additional VPN Rule for SecurID authentication						
Source	**Destination**	**Service**	**Action**	**Track**		
Firewall	RSA Ace Server	SecurID	Accept	Long		This rule allows encrypted communication between the SecurID client on the FW and the RSA Ace Server.

ASSIGNMENT 2 – VPN TUTORIAL

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

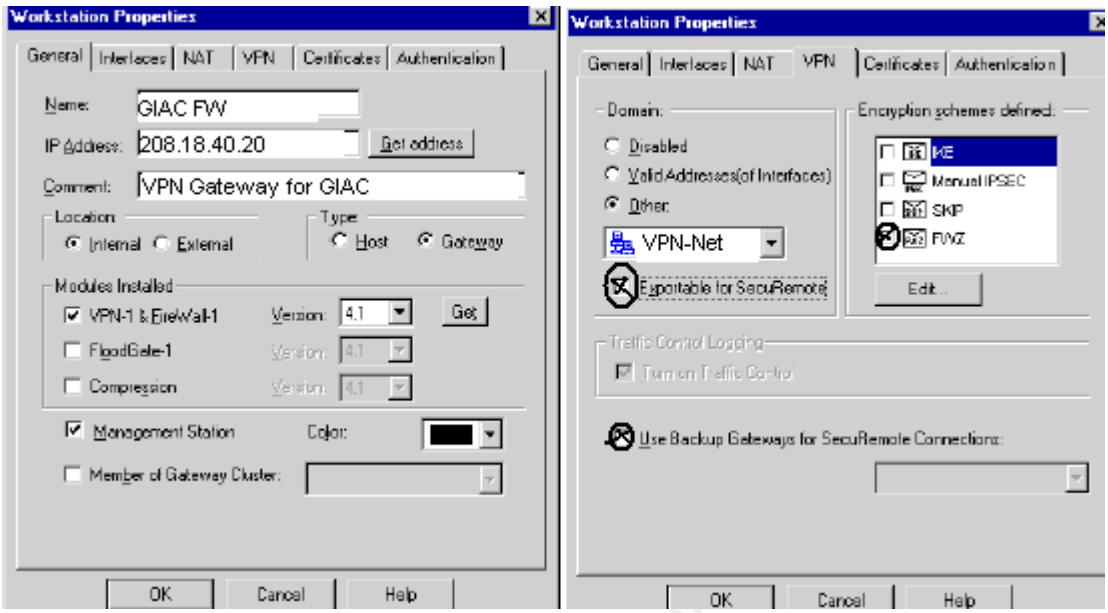
Virtual Private Networks (VPNs) connect mobile staff, suppliers and international partners over a shared or public network such as the Internet, with the same security and availability as a private network. VPNs use existing shared wide area network (WAN) infrastructures therefore are cost efficient and readily deployed. There are many different technologies which will provide a secure VPN. The solution must provide the three basic security elements of authentication, encryption and access control and integrate into the overall security policy. This tutorial will detail the setup for VPN access facilitated through Check Point's FW VPN-1 solution. This includes Check Point's SecuRemote Client and SecureClient. RSA ACE SecureID will add another layer of authentication to this VPN. This tutorial will describe FW configuration, RSA ACE server configuration and Mobile Staff laptop configuration. Then interaction between these components and integration to overall security policy will be explained.

Check Point Firewall-1 VPN Configuration Check Point FW supports several different encryption schemes. Review and compare the features of Manual IPSec, IKE, SKIP and FWZ before selecting your encryption scheme. Check Point offers excellent information and comparisons. FWZ was selected because of automatic key management and new key generation for each TCP or UDP session.
You can start by verify your Check Point licence to see if you have the features you need to set up VPN.

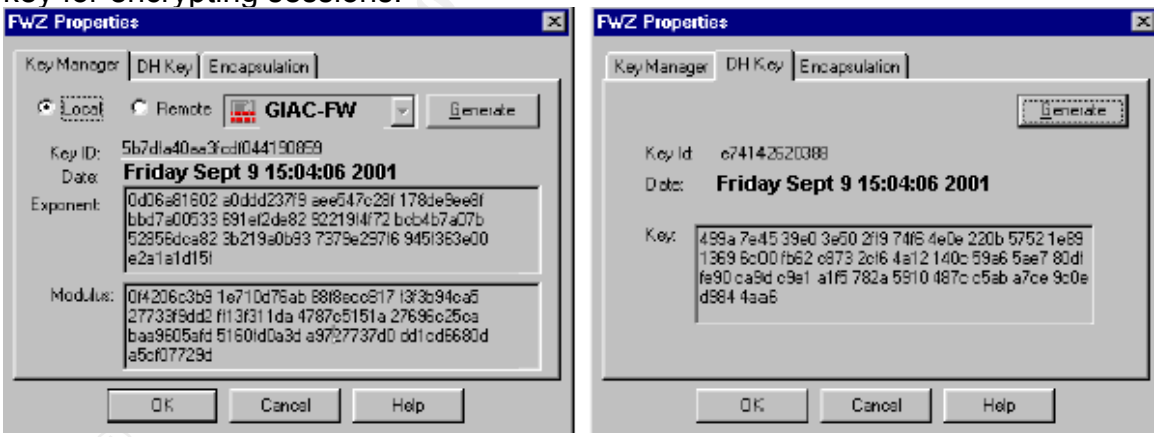
Check your Check Point FW to ensure it supports encryption. VPN should be included in the display. COMMAND: FW VER (enter) RESULT: Checkpoint VPN-1™ and Fw-1<R> Ver. 4.10 Build 41514 VPN &DES&Strong Check for the encryption feature license. COMMAND: fw printlic –p (enter) RESULT: Strings containing fwz or ike

If you are properly licensed, you can implement FWZ encryption. Create a workstation object for the encrypting Firewall. We will specify GIAC FW as the encrypting gateway. This must be set up on both ends of the gateway to gateway VPN connection. VPN-Net is added as the encryption domain with FWZ defined as the encryption scheme. The encryption domain includes all the objects like Exchange Server, File Server, etc for which traffic is encrypted and decrypted by the VPN Gateway. We are using SecuRemote so will also select 'Use backup Gateways for SecuRemote Connections".

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



The encryption keys are generated for the encrypting gateway and its CA. You have already defined FWZ in the Workstation Properties window under encryption schemes. Click on Edit and the FWZ Properties window will display. Click on Generate in the Key Manager window to generate an RSA key pair for the GIAC-FW. This is used by the Gateway to identify itself as a CA. Another key shows in the DH Key tab. This was generated when you installed the FW VPN-1. This key is used by GIAC-FW to generate a secret key for encrypting sessions.



Define each supplier and partner's Firewall as objects on the GIAC's Firewall so that all participants in the VPN connection can be defined in the rule base. The encrypt action will enforce encryption on outgoing packets and decryption on incoming packets and accept them. Ensure this rule in inserted into the rule base appropriately so that traffic between these sources are encrypted but traffic from these sources to other destinations will not be encrypted. This rule encrypts and accepts traffic from the authorized FW to the authorized FWs. Similar rules must be configured on partner and

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