GCFW Practical

By: Dan Golden

GCFW Practical
v. 4.0

Jan. 07, 2005

Table of Contents

Table of Figures 3
Abstract 4
Assignment 1: Future state of security technology 4
Intrusion Prevention Systems 4
The Risk 4
Intrusion Prevention Systems 5
Signature-based Detection 6
Protocol Anomaly Detection 7
Baseline Anomaly Detection 8
Conclusion 9
Assignment 2: Security Architecture of GIAC Enterprises 10
Access Requirements 10
Customers 10
Suppliers 10
Partners 10
GIAC Internal Employees 10
GIAC Sales/Teleworkers 10
General Public 11
Security Architecture Components 11
Border Router 11
Perimeter Firewall 11
Internal Firewall 12
Intrusion Detection Systems 12
Additional Security Devices 13
IP Scheme 13
Defense in Depth 14
Network Diagram 15
Assignment 3: Firewall Configuration 16
Firewall Management 16
Remote Access Rules 16
VPN Access Rules 17
Stealth Rule 17
Incoming Access Rules 17
DMZ Access 18
Internal Networks Outbound Access Rules 18
Clean Up Rule 18
List of References 19

Table of Figures

Figure 1 - Nachi Worm - Signature Detection 7
Figure 2 - Valid ICMP - Signature Detection 7
Figure 3 - Host Infection - Baseline Detection 9
Figure 4 - Network Diagram - Architecture 15
Figure 5 - Management - Firewall Policy 16
Figure 6 - Remote Access - Firewall Policy 16
Figure 7 - VPN - Firewall Policy 17
Figure 8 -Stealth - Firewall Policy 17
Figure 9 - Inbound - Firewall Policy 17
Figure 10 -DMZ - Firewall Policy 18
Figure 11 -Outbound - Firewall Policy 18
Figure 12 - Clean Up - Firewall Policy 18

Abstract

The following paper discusses IPS, as a new technology in network security. It will discuss the risks that security administrators are facing today and how an IPS will aid in protecting the network. In addition, we will look at the security architecture of a fictitious company, the access its customers, partners and general public will need. The devices employed to secure the network are their role will be examined.

Assignment 1: Future state of security technology

The following discusses a relatively new device that is being implemented to compliment firewalls and intrusion detection systems. This device is an Intrusion Prevention System (IPS). There is debate as to what is considered an Intrusion Prevention System. For the purpose of this section, an Intrusion Prevention Systems is a device or agent that functions similarly to a traditional intrusion detection system, but in addition to detecting and alerting on suspicious traffic, the device is able to block/drop the connection.

Intrusion Prevention Systems

The Risk

As network attacks become more sophisticated, the tools available to network administrators must advance accordingly. One area of growth in these defense tools is Intrusion Prevention. Intrusion Prevention Systems, while immature, are one of the industry's responses to virus/worm and application based attacks. Application based attacks take advantage of operating system vulnerabilities, and well-known ports that are open on the firewall. These ports such as smtp, and http/https must be open to support business critical services. Viruses and worms are generally spread through emails. Once activated these viruses and worms attack systems from the inside, trying to propagate to other internal hosts or networks. In a shift from previous years, both virus and denial of service attacks have outpaced the perennial top cost to enterprises, theft of proprietary information. Virus related costs jumped to $55 million[1]. It is no longer enough to detect and report on these attacks after they occur. The ability for a network to adapt and block virus, worm and application level attacks is a critical component in the effort to maintain a strong enterprise security posture.

In addition to the direct attacks that a corporate network might face, remote users outside the corporate security infrastructure make a more palatable target to hackers. With the increase of broadband connections to homes, the

[1] 2004 CSI/FBI Computer Crime and Security Survey – http://www.hands-on-labs.com/only4gurus/techlib/miscellaneous/fbi2004.pdf

number of unsuspecting victims grows. In the US, 48.61% of Internet users have broadband connections at home.[2] Worldwide broadband subscribers will exceed 150 million before the end of 2004, according to Point Topic[3]. Because these users are outside the corporate security zone, IT managers are somewhat helpless in protecting them. These remote user's systems could become infected while at home and then brought to work, exposing internal systems.

If a Trojan is installed on an unknowing user's laptop, this system can unwittingly become a platform in which a hacker launches their attack or gains access to information. In affect, the attacker has bypassed corporate security devices. IPS gives network administrators the ability to thwart or mitigate potential attacks through this vulnerability.

Intrusion Prevention Systems

IPSs can be broken down into two categories based on their location on the network - Host-based Intrusion Prevention Systems (HIPS) and Network Intrusion Prevention Systems (NIPS). Both versions are able to analyze traffic through several means.

Host-based IPS agents are installed directly on the system that it protects. The agent is closely tied to the operating system and monitors all incoming traffic. The performance of a host-based IPS is subject to the performance of the host that it is installed on. Each host that has the agent installed on it acts independently from all others. This provides administrators the flexibility to apply various individualized policies on hosts, which reside on the same segment. Another benefit of HIPS is that the failure of one host agent does not affect the entire network.

Network IPS systems are specialized devices that sit in-line on the network segment. Though these IPS devices are the most resource intensive, they are still relatively high performing due to the latest processors, software, and hardware advancements such as ASICs.[4] Without these advancements, NIPS could potentially become a bottleneck for network traffic, because of their in-line position on the network. Depending on which type of Network IPS is employed, a failure of the device could either cause a network outage or show no signs of a network problem. Some NIPS will fail closed, stopping all traffic that would pass through it, while others will fail open, allowing traffic to pass through uninspected. When failed open, although the network is no longer protected, a denial of service has been averted.

Both HIPS and NIPS function in relatively the same manner. The IPS kernel checks to see if the incoming packets match the signatures in its library or

[2] http://www.websiteoptimization.com/bw/0406/
[3] http://www.itfacts.biz/index.php?id=P2302
[4] SentivistISP-WP.pdf - http://www.nfr.com/resource/downloads/SentivistIPS-WP.pdf

if it fits the database for application/protocol anomalies. If the packet is deemed safe, it is passed through to the exiting interface (or in the case of HIPS, up the TCP/IP stack to the operating system). If a match is made, the packet is dropped along with any other packet associated with that session.

An IPS device can be summed up as a combination of a firewall and IDS. The device monitors network traffic much like a traditional IDS for suspicious traffic and has the ability to block/drop the connection like a firewall. The IPS employs several techniques in which it can identify malicious traffic. These techniques include signature-based detection, protocol anomaly detection, and network baseline anomaly detection.

Signature-based Detection

Signature-based detection works by matching packets on the network against a set of known patterns; this is sometimes called pattern matching. These "known pattern" signatures are created from known attacks. As the IPS inspects the packet, it compares the packet to its library of signatures. If any portion of the packet matches a signature, the connection is deemed malicious and dropped. One drawback of this method of detecting attacks, is that never before seen attacks will not flag anything. The system is completely unaware that the connection is malicious in any way, until after the damage is done. Once an attack method has become widespread its characteristics are identified, a signature is written, and it is then added to the sensors signature library. Although this method does not provide day 0 protection from exploits, it is a much faster process for the device to perform, when compared to processes such as protocol anomaly detection and network activity anomaly detection. For example, an icmp echo request packet enters the network with a payload of 0XAA.

```
0x0000   4500 005c bfe9 0000 6b01 a0a7 ---- ----       E..\....k.......
0x0010   ---- ---- 0800 2c8b 50de 2541 aaaa aaaa       ......,.P.%A....
0x0020   aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa       ................
0x0030   aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa       ................
0x0040   aaaa aaaa aaaa aaaa aaaa aaaa aaaa aaaa       ................
0x0050   aaaa aaaa aaaa aaaa aaaa aaaa                 ............
```
[5]

This packet is indicative of a Nachi worm icmp echo request. The Intrusion Prevention Systems would match the packet to the signature that is stored in its library for this known exploit.

[5] http://www.esphion.com/news/ETB-82.htm

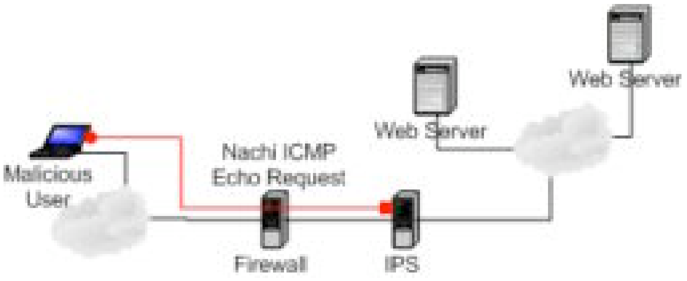


Figure 1 - Nachi Worm - Signature Detection

A standard ICMP echo request packet enters the network and will be inspected by the IPS. The packet does not contain any characteristics defined in the signatures, it will be allowed to pass through to the final destination.

```
0000  00 0c 41 3b 8c 2a 00 10 a4 b0 45 1c 08 00 45 00   ..A;.*....E...E.
0010  00 3c 16 80 00 00 80 01 3b 77 c0 a8 01 65 44 8e   .<......;w...eD.
0020  e2 2e 08 00 46 5c 03 00 04 00 61 62 63 64 65 66   ....F\....abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76   ghijklmnopqrstuv
0040  77 61 62 63 64 65 66 67 68 69                     wabcdefghi
```

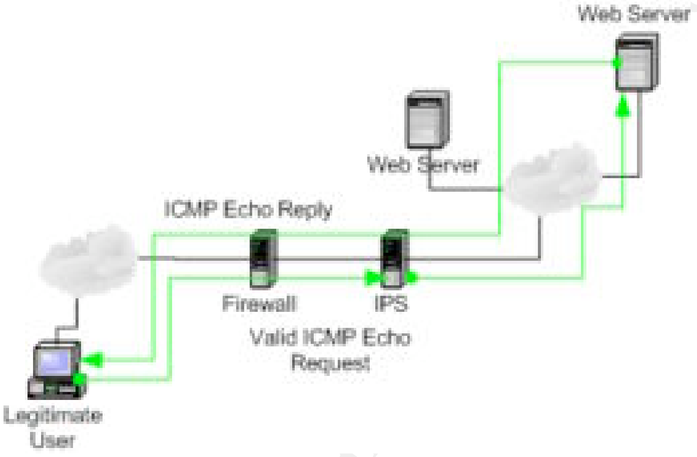


Figure 2 - Valid ICMP - Signature Detection

Protocol Anomaly Detection

Protocol anomaly detection is a more advanced monitoring process than signature based detection. Instead of looking for traffic that is malicious, protocol anomaly looks for traffic that is “correct”. Most vendors adhere to the standards laid out in RFCs for protocols. Protocol anomaly detection uses these standards to inspect packets. Whereas signature-based detection looks at each packet to see what is wrong or out of the ordinary, anomaly detection looks at the packets to make sure that they conform to the known standards. Each packet’s layers are inspected by the IPS. If a field or value does not comply with the standard for the specific layer, the traffic is considered malicious and is dropped. This detection process proves to be a more robust approach to identifying malicious traffic than to signature based detection. The ability to determine if a connection conforms to protocol standards also provides the added comfort of day 0 protection against unknown vulnerabilities and attacks. In comparison to signature-based detection, protocol anomaly is a more resource intensive process. Two examples of attacks that are detected by protocol anomaly detection are, exploiting protocol commands and injecting malicious code into packet headers. In 2002, Code Red hit the Internet, this worm exploit an buffer overflow in IIS Indexing Services.[6] At the time, there was no signature available for the exploit. Signature based sensors would not have recognized the worm, whereas a protocol anomaly sensor would have. Code Red misuses the http GET command. With this command a hacker attempts to post and execute malicious code on a web server, compromising the host.[7] The IPS would detect that the GET command violates the standards for http set out in RFC 2616[8]. Another technique to compromise a system is injecting executable code into the packet. A hacker adds the code into the header of an smtp packet. Since smtp is generally allowed by every corporate firewall the packet would be able to enter the network where it would be inspected by the IPS. The packet would fail inspection from the IPS since it does not match the standard for smtp communication. Even though the commands and code in the above examples could vary greatly from hacker to hacker, the protocol anomaly process would still be able to detect the malicious connections without having to wait for a signature to be written. This increases the strength of a corporation's security posture.

Baseline Anomaly Detection

The third technique employed by IPS is network activity anomaly detection. With this type of detection any unusual traffic behavior on the network or from a host is detected and prevented. In order for this to work, a baseline of network activity must be established. Once the baseline is established, if a host starts transmitting traffic that is unusual or the volume of traffic increases, the sensor will key in on the change and act accordingly. For example, many viruses and worms will install a mini smtp service on an infected host. This host in turn, starts sending smtp traffic to various other hosts in the hopes of propagating the virus or worm. The sudden change will be detected in the baseline established on the sensor. The traffic will then be isolated and dropped.

[6] http://www.cert.org/advisories/CA-2001-19.html
[7] http://www.isp-planet.com/perspectives/ids_p3.html
[8] http://www.faqs.org/rfcs/rfc2616.html

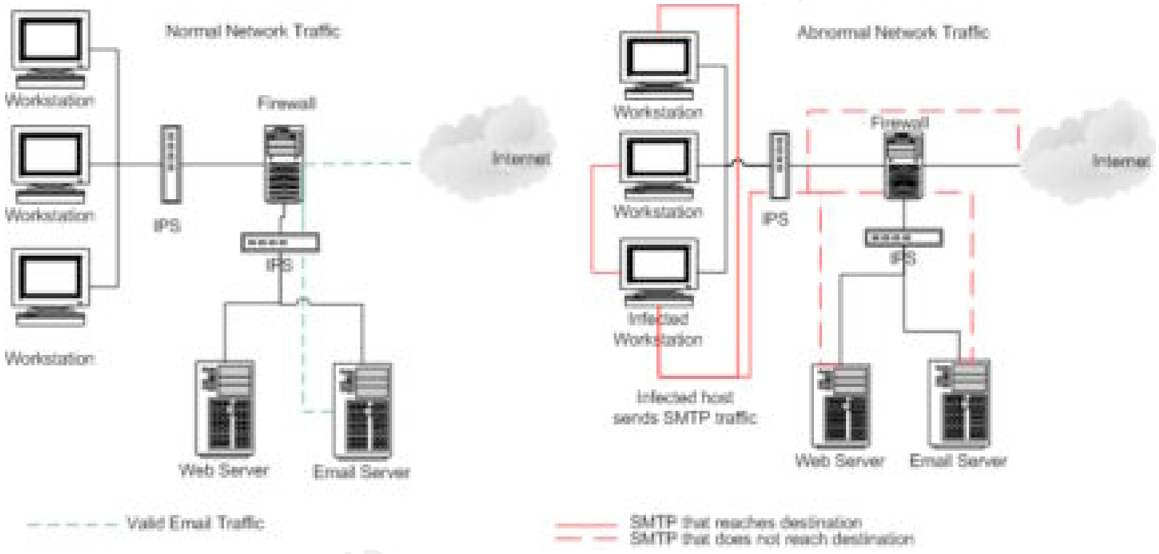


Figure 3 - Host Infection - Baseline Detection

Conclusion

Much like traditional IDS, there is a risk of false positives with IPS, in which legitimate traffic is flagged as an attack. This is in part due to the infancy of IPS devices. In traditional IDS, a large amount of false positives results in a large number of alerts. With IPS, a large amount of false positives can result in a self-inflicted denial of service. With this risk, administrators must be very careful in deciding the type of IPS and the process in which the device will detect malicious traffic. This risk also backs up the thought that an IPS is not an end all cure. It should not be considered as a complete replacement of firewalls and intrusion detection systems. Instead they should be deployed as a complimentary security device to the existing security devices. The combination of these devices will help companies combat the everyday threat that is out there.

Assignment 2: Security Architecture of GIAC Enterprises

Access Requirements

Customers

- HTTP (tcp port 80) and HTTPS (tcp port 443)

Customers will need to be able to access GIAC's web servers via http and https. General information will be provided by http. Customers wishing to place orders will utilize GIAC's https servers for secure transactions.

Suppliers

- Terminal Services (tcp 3389) FTP (tcp port 21)

Suppliers will provide fortune cookie sayings via a site-to-site vpn. In order to due so, they will need to access the database servers in DMZ-2 via terminal services and ftp.

Partners

- Terminal Services (tcp 3389) FTP (tcp port 21)

Partner companies work alongside GIAC providing fortune cookie sayings. GIAC and these partners need to maintain the same data. To facilitate this access to servers in DMZ-2 must be allowed using terminal services, ftp and a customer application using tcp port 9044.

GIAC Internal Employees

- HTTP (tcp port 80) HTTPS (tcp port 443)

All internal employees will be granted outbound http and https access to the Internet. Http access will be limited in the future with the implementation of a URI Filtering device. Each user will also be setup with a company email account.

GIAC Sales/Teleworkers

- HTTP (tcp port 80) HTTPS (tcp port 443)
- Terminal Services (tcp 3389)

These 'road warriors' will be able to access internal resources as if they were on the internal network via a vpn. GIAC has employed the use of two-factor strong authentication by the use of a RSA Ace/Radius server. This server integrates with Checkpoint's Secure mote client for client to site vpns. The IT department will also be granted access to the internal network via Secure Client This enables the team to manage and troubleshoot possible network and system issues anywhere, at anytime.

General Public

- HTTP (tcp port 80) HTTPS (tcp port 443)
  The general public will be able to access the GIAC web servers.

Security Architecture Components

GIAC employs several lines of defense for its corporate infrastructure. This section will review each device type, their specifications and the role they play.

Border Router

- Cisco 2621, IOS v.12.3

Besides the router's function as the connection point to the ISP's network, it also acts as the first layer of defense in the GIAC network, implementing basic packet filtering. Incoming connections that have the source IP address of the GIAC Internal network, or any other address set aside by RFC 1918[9], will be denied. In addition, any sourced routed packets will be denied. The border router also blocks what GIAC considers 'noisy protocols'. This group contains NetBIOS ports, tcp/udp 135, udp 137-138, tcp 139 and tcp/udp 445.

With this filtering, the router reduces a portion of traffic that has no business value from reaching the perimeter cluster. This reduces the load that the cluster has to process. GIAC has a future plan to incorporate Border Gateway Protocol (BGP) and an additional router with a second ISP connection to mitigate single point of failure at the border.

Perimeter Firewall

- Nokia IP 380, 512 MB RAM, 8 10/100 mbps Ethernet interfaces
- IPSO 3.8 Build 037, Simplified VRRP
- Checkpoint NG AI R55 HFA-012, State Sync

GIAC has deployed a pair of Nokia appliances running Checkpoint as their border firewalls. The firewalls are setup in a High Availability design, utilizing Nokia's VRRP, and Checkpoint's State Sync. These will provide a redundant configuration minimizing down time in an event of a failure of the primary firewall. It also gives the IT department the flexibility to perform maintenance on the firewalls without causing a complete disruption of service.

The border cluster provides the second filtering point of all traffic entering and leaving the GIAC network. It allows http and https traffic into the web servers located in DMZ-1 to facilitate the general public and customer access to the

[9] http://www.faqs.org/rfcs/rfc1918.html

corporate websites. The cluster also provides the end point for the GIAC remote vpn clients and the site-to-site vpns that GIAC has with its partners and suppliers. Inbound smtp is permitted through this cluster to an smtp filtering server located in DMZ-3. Traffic between the Web servers located in DMZ-1 and the database servers in DMZ-3 is permitted on tcp port 9080 and tcp port 9443.

The perimeter cluster's logs will provide the IT department with a view of the external traffic that is being sent to the GIAC network. With the firewalls layered in this environment the IT staff is able to allow traffic out from the internal network without having to log it on the border firewall. Internal traffic will be logged at the internal cluster. This makes reviewing the border firewall logs for malicious traffic such as port scans much easier. There is additional redundancy in that if there were a failure of the border cluster the staff would be able to configure the unused interfaces on the internal cluster to be external and for DMZ-1 and DMZ3, this minimizing any possible interruption of service.

Internal Firewall

- Nokia IP 380, 512 MB RAM, 8 10/100 mbps Ethernet interfaces
- IPSO 3.8 Build 037, Simplified VRRP
- Checkpoint NG AI R55 HFA-012, State Sync

The Internal Cluster provides the final filtering point. Its role is to protect GIAC's internal networks and DMZ-2. It allows the internal networks to reach the web servers in DMZ-1, Internet access, and allows the internal Sales department to reach the database servers located in DMZ-2. The cluster also allows SMTP traffic from the Esafe server located in DMZ-3 to reach the internal mail server. This cluster is the final filtering point for traffic. Traffic originating from any of the DMZs to the IT network will be dropped. Communication between DMZ-1 and DMZ-2 is allowed for the database servers to provide information to the web servers on tcp port 9080 and tcp port 9443.

With the layering of firewalls, the log data generated by the internal firewalls gives the IT department an advantage of having external log data isolated from internal log data. This separation gives the staff the ability to monitor the activity of the internal users more efficiently. This also makes log management easier, by reducing the size of the logs for the internal network. As with the redundancy with the border cluster, in the event of a failure of the internal cluster, the border clusters free interfaces can be ip'ed to mimic the internal cluster

Intrusion Detection Systems

- 3 Dell Power Edge 1750, 512 MB RAM
- NFR v. 4.1

As an additional layer of security, GIAC has incorporated Network Intrusion Detection Systems. These systems helps the GIAC IT Team to identify any possible breaches in its network security architecture, as well as to provide a useful tool in monitoring the type of traffic entering and leaving the network. These systems have been deployed in three locations, the first being on DMZ-1. This IDS will monitor for any suspicious traffic intended for the GIAC web servers. The second is located on Transport Network. This will capture traffic that is being sent to the internal network, as well as the database servers located in DMZ-2. The final sensor is placed on the internal network. This will monitor any traffic that might have breached the outer defenses. It will also be able to monitor the activity of the GIAC employees located on the internal network.

Additional Security Devices

GIAC employs three more systems in its security architecture. The first system is an ACE Two-Factor authentication server. This server's role is to act as the authentication point for the GIAC remote users, as well as for specific secure web pages used by GIAC vendors. The second device is an Esafe Virus server, which acts as a proxy for email traffic. All inbound smtp traffic is sent to the Esafe server, where it is scanned and then forwarded onto the internal email server located on the internal network. The final device is the a IT department router. The router enforces ACLs that deny traffic originating from the internal network from reaching the IT department segment.

IP Scheme

For the 4 DMZ segments use a 27-bit subnetted Class C network (192.68.1.0). Each DMZ switch has a static MAC table defined to prevent an unauthorized user from connecting a host to the segments and gaining access to the servers. This gives the IT department an additional means to controlling and securing the networks. The 27-bit subnet mask provides 30 hosts per segment. This allows the flexibility to add additional servers as the company expands. The internal network is a Class B network (172.16.30.0) that has been subnetted to a 25-bit mask. This provides a separation between the company's internal users and the IT department. The IT department network is using a 172.16.30.128/27. For remote access a 27-bit Class C network (192.168.2.0/27), hosts .1-.30 are set-aside for sales and internal users to work from home and the road. The IT department users will use (192.168.2.32/28), hosts .33-46 for remote access.

GIAC considered several options for their choice in firewalls, including Cisco Pix, Juniper NetScreen, and Checkpoint FW-1. When researching these three vendors, GIAC considered several key areas: cost, reliability, vpn capabilities and logging capabilities. In the end, Checkpoint FW-1 running on Nokia appliances was chosen. Due to the brand's logging features, user interface, platform reliability and the IT team's familiarity with the product, it was an easy choice to make. In addition, GIAC felt that Checkpoint had an edge on their competitors with Checkpoint's Secure Client vpn client and the Smart Defense features in R55.

Defense in Depth

GIAC's management and IT staff have made the decision to employ various security products in an effort to protect corporate information. The border and internal firewall clusters are task with permitting defined services to specific destinations. These devices are unable to make decisions on if a connection is legitimate or if it is malicious, specially crafted connection designed to mimic a legitimate connection. The IDSs are unable to block or deny a connection that is malicious. The information that they provide however can be used to restrict malicious traffic. If a specific source ip address were constantly sending malicious traffic to the network, the IDS would alert the IT team of this pattern. The IT team could then make the decision that the source does not have a need to reach the GIAC public servers, and block any connections from that source. The use of a two-factor authentication process helps the team eliminate inevitable use of weak passwords by users.

Separating the internal network into several smaller networks has an added benefit besides ease of management. It provides a layering effect, separating internal resources from those that are publicly accessible. If publicly accessible servers were located on the internal network, a hacker could compromise one of the servers and use the system as a launching point to obtain proprietary information.

Both teams have come to the realization that relying on type of device severely limits their ability to secure and maintain the integrity of internal resources. In the early days of network security, reliance on firewalls proved to be adequate for a period of time. In the current times, with attacks becoming more advanced, reliance on firewalls is no longer sufficient. The features listed above alone cannot provide a secure network however, when combined they provided a robust and adaptive network security stance.

Network Diagram

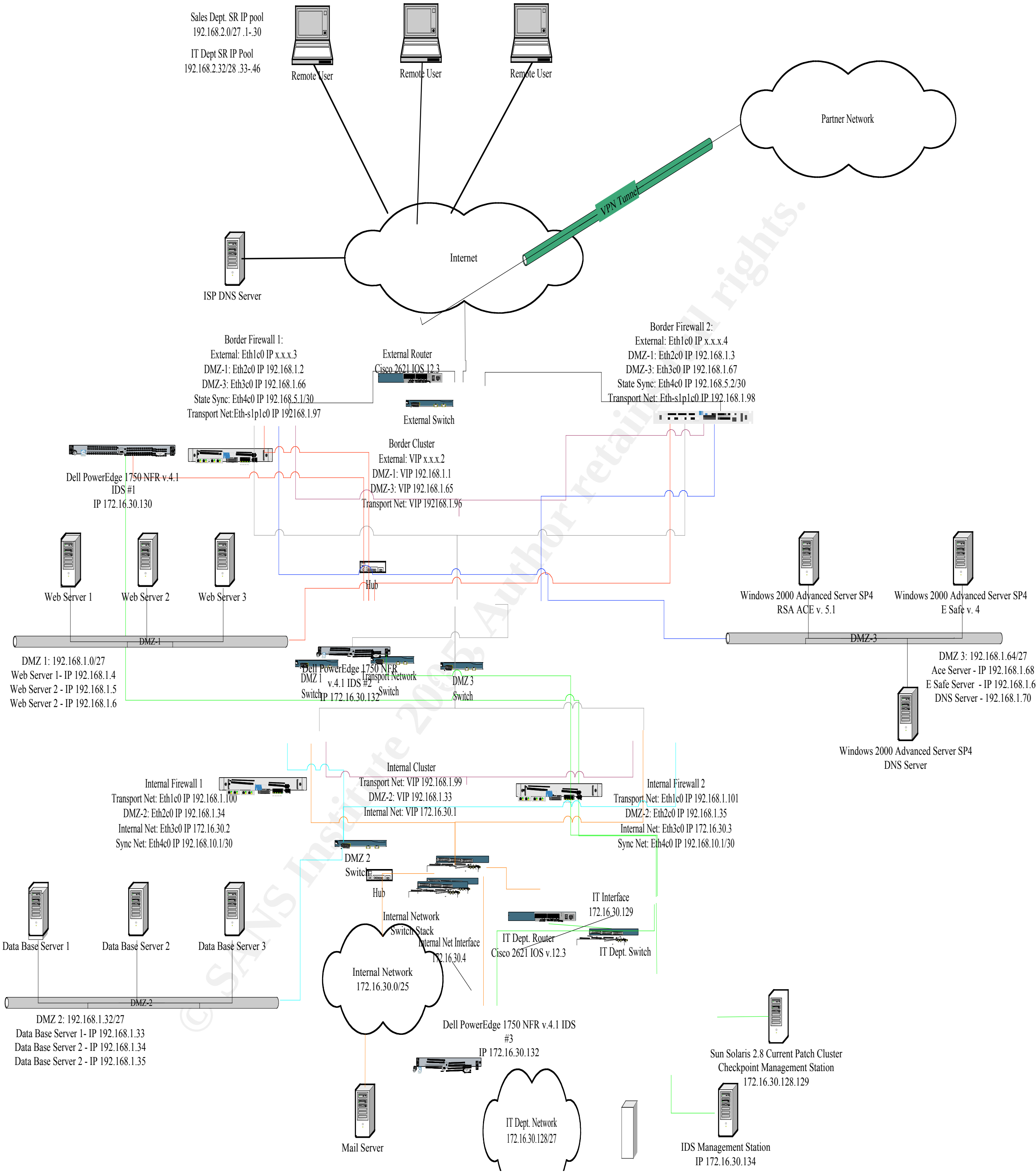
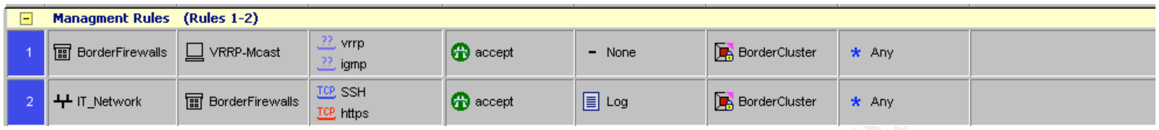

Sales Dept. SR IP pool
192.168.2.0/27 .1-.30
IT Dept SR IP Pool
192.168.2.32/28 .33-.46
Remote User
Remote User
Remote User
Partner Network
VPN Tunnel
Internet
ISP DNS Server
Border Firewall 1:
External: Eth1c0 IP x.x.x.3
DMZ-1: Eth2c0 IP 192.168.1.2
DMZ-3: Eth3c0 IP 192.168.1.66
State Sync: Eth4c0 IP 192.168.5.1/30
Transport Net:Eth-s1p1c0 IP 192168.1.97
External Router
Cisco 2621 IOS 12.3
External Switch
Border Firewall 2:
External: Eth1c0 IP x.x.x.4
DMZ-1: Eth2c0 IP 192.168.1.3
DMZ-3: Eth3c0 IP 192.168.1.67
State Sync: Eth4c0 IP 192.168.5.2/30
Transport Net: Eth-s1p1c0 IP 192.168.1.98
Dell PowerEdge 1750 NFR v.4.1
IDS #1
IP 172.16.30.130
Border Cluster
External: VIP x.x.x.2
DMZ-1: VIP 192.168.1.1
DMZ-3: VIP 192.168.1.65
Transport Net: VIP 192168.1.96
Web Server 1
Web Server 2
Web Server 3
Hub
Windows 2000 Advanced Server SP4
RSA ACE v. 5.1
Windows 2000 Advanced Server SP4
E Safe v. 4
DMZ-1
DMZ 1: 192.168.1.0/27
Web Server 1- IP 192.168.1.4
Web Server 2 - IP 192.168.1.5
Web Server 2 - IP 192.168.1.6
Dell PowerEdge 1750 NFR
v.4.1 IDS #2
IP 172.16.30.132
DMZ 1
Switch
Transport Network
Switch
DMZ 3
Switch
DMZ-3
DMZ 3: 192.168.1.64/27
Ace Server - IP 192.168.1.68
E Safe Server - IP 192.168.1.69
DNS Server - 192.168.1.70
Windows 2000 Advanced Server SP4
DNS Server
Internal Cluster
Transport Net: VIP 192.168.1.99
DMZ-2: VIP 192.168.1.33
Internal Net: VIP 172.16.30.1
Internal Firewall 1
Transport Net: Eth1c0 IP 192.168.1.100
DMZ-2: Eth2c0 IP 192.168.1.34
Internal Net: Eth3c0 IP 172.16.30.2
Sync Net: Eth4c0 IP 192.168.10.1/30
Internal Firewall 2
Transport Net: Eth1c0 IP 192.168.1.101
DMZ-2: Eth2c0 IP 192.168.1.35
Internal Net: Eth3c0 IP 172.16.30.3
Sync Net: Eth4c0 IP 192.168.10.1/30
DMZ 2
Switch
Hub
Internal Network
Switch Stack
Internal Net Interface
172.16.30.4
IT Interface
172.16.30.129
IT Dept. Router
Cisco 2621 IOS v.12.3
IT Dept. Switch
Data Base Server 1
Data Base Server 2
Data Base Server 3
Internal Network
172.16.30.0/25
DMZ-2
DMZ 2: 192.168.1.32/27
Data Base Server 1- IP 192.168.1.33
Data Base Server 2 - IP 192.168.1.34
Data Base Server 2 - IP 192.168.1.35
Dell PowerEdge 1750 NFR v.4.1 IDS
#3
IP 172.16.30.132
Sun Solaris 2.8 Current Patch Cluster
Checkpoint Management Station
172.16.30.128.129
Mail Server
IT Dept. Network
172.16.30.128/27
IDS Management Station
IP 172.16.30.134

Figure 4 - Network Diagram - Architecture

Assignment 3: Firewall Configuration

Firewall Management

The following rules allow the firewall to send necessary traffic for everyday function and allow the IT department to connect to the firewall for management.



Managment Rules (Rules 1-2)

1	BorderFirewalls	VRRP-Mcast	vrrp igmp	accept	None	BorderCluster	Any	
2	IT_Network	BorderFirewalls	SSH https	accept	Log	BorderCluster	Any	

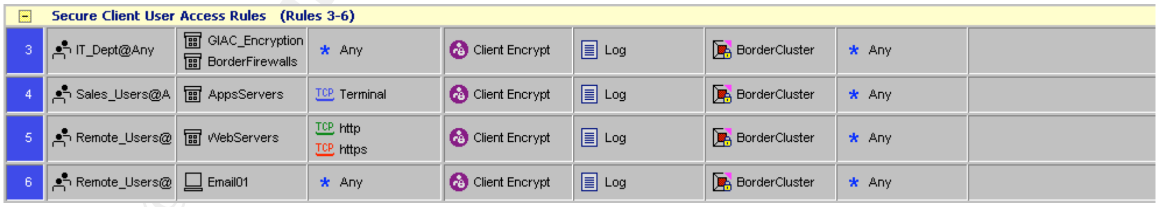
Figure 5 - Management - Firewall Policy

Rule 1 in the Border policy allows the firewalls to send their VRRP advertisements to the multicast address. This enables the firewalls to function in a High Availability configuration. Since the advertisements happen every second, this rule is used frequently. Placing this rule at the top of the rulebase makes the firewall more efficient. Also due to the frequency, logging is turned off.

Rule 2 allows connections from the IT Network to the firewall for ssh and https. This enables the team to connect to the firewall to make changes to the system via Nokia's Voyager access and ssh access for troubleshooting purposes. In the event of connectivity failure from the IT network to the Border cluster, a secured host on the IT network has a direct console connection to the firewalls.

Remote Access Rules

The VPN and Remote Access rules are the next set of rules in the rulebase. Since the remote users and site-to-site vpns will make an initial connection to the firewall directly to bring the tunnels up, they are placed above the stealth rule.



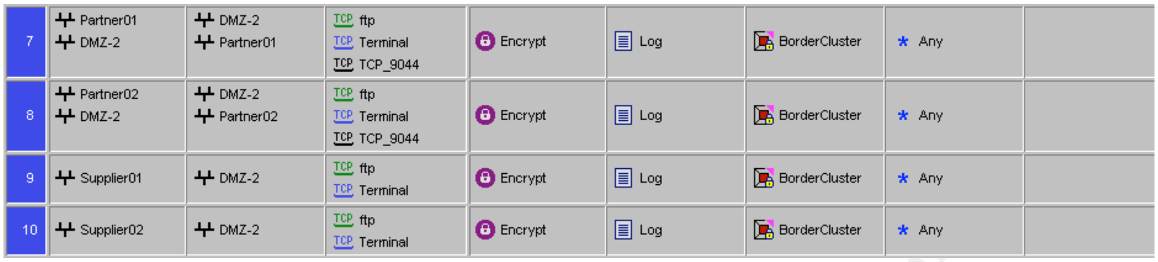
Secure Client User Access Rules (Rules 3-6)

3	IT_Dept@Any	GIAC_Encryption BorderFirewalls	Any	Client Encrypt	Log	BorderCluster	Any	
4	Sales_Users@A	AppsServers	Terminal	Client Encrypt	Log	BorderCluster	Any	
5	Remote_Users@	WebServers	http https	Client Encrypt	Log	BorderCluster	Any	
6	Remote_Users@	Email01	Any	Client Encrypt	Log	BorderCluster	Any	

Figure 6 - Remote Access - Firewall Policy

Rules 3 through 6 are for remote access. The Secure Client configuration is set to Office Mode so that the remote users will be assigned an IP address from a specified pool as well as name servers. All users will be using Secure Client version R56, in hub mode. When connected, the remote user's Internet traffic will be routed through the tunnel and out of the firewall.

VPN Access Rules

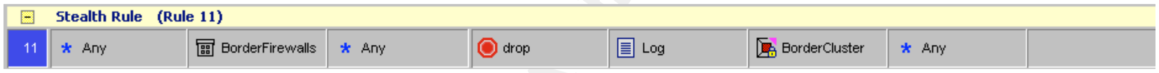


7	Partner01 DMZ-2	DMZ-2 Partner01	ftp Terminal TCP_9044	Encrypt	Log	BorderCluster	Any	
8	Partner02 DMZ-2	DMZ-2 Partner02	ftp Terminal TCP_9044	Encrypt	Log	BorderCluster	Any	
9	Supplier01	DMZ-2	ftp Terminal	Encrypt	Log	BorderCluster	Any	
10	Supplier02	DMZ-2	ftp Terminal	Encrypt	Log	BorderCluster	Any	

Figure 7 - VPN - Firewall Policy

Rules 7 through 10 have been established for the partner and supplier vpns. Suppliers are access to the servers in DMZ 2 for ftp and Terminal Services. This allows them to send bulk fortune cookie sayings. GIAC and its partners require a bi-directional vpn. This supports the need to update data across the vpn, ensuring both companies have the most current information

Stealth Rule



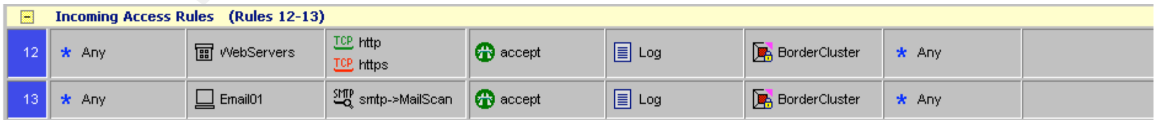
⊟	Stealth Rule (Rule 11)							
11	Any	BorderFirewalls	Any	drop	Log	BorderCluster	Any	

Figure 8 -Stealth - Firewall Policy

Rule 11 is the stealth rule, which drops all traffic destined to the firewall. The action is set to drop instead of deny as not to give a potential attacker information about the defenses. This rule is placed directly after the remote access and vpn rules to allow those connections. It is placed as far up in the rulebase as possible.

Incoming Access Rules

Rules covering inbound business services:



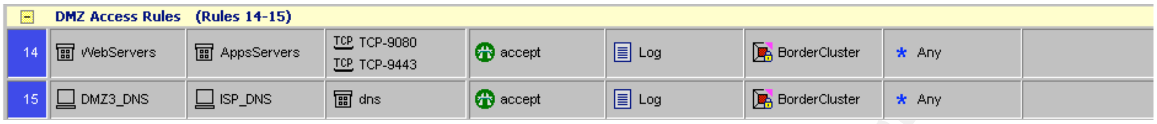
⊟	Incoming Access Rules (Rules 12-13)							
12	Any	WebServers	http https	accept	Log	BorderCluster	Any	
13	Any	Email01	smtp->MailScan	accept	Log	BorderCluster	Any	

Figure 9 - Inbound - Firewall Policy

Rules 12 and 13 deal with access to the GIAC network from the Internet. Since these rules are used frequently they are placed just after the Stealth rule. This helps in the processing of traffic and comparison against the rule set. Rule 12 allows http and https from anywhere to the web servers that are located in

DMZ-1. Inbound smtp is allowed into DMZ-3 via an smtp resource. This resource directs the incoming emails to the Esafe server. The Esafe server will scan the mail for possible viruses and worms. Once deemed safe, the mail will be sent to the internal email server.

DMZ Access



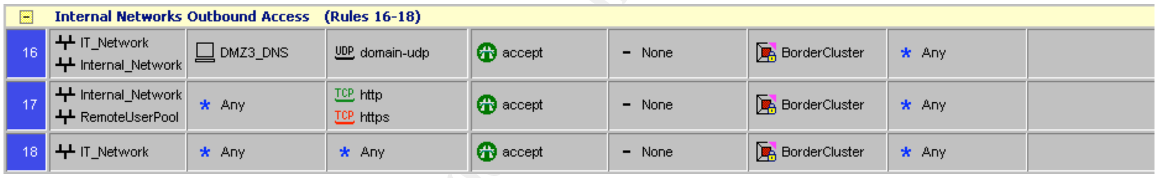
DMZ Access Rules (Rules 14-15)

14	WebServers	AppsServers	TCP TCP-9080 TCP TCP-9443	accept	Log	BorderCluster	Any	
15	DMZ3_DNS	ISP_DNS	dns	accept	Log	BorderCluster	Any	

Figure 10 -DMZ - Firewall Policy

Rule 14 allows the web servers located in DMZ-1 to query the application servers located in DMZ-2. This supports the selling of sayings to customers. Rule 15 permits the internal GIAC DNS server to query the ISP's DNS server for queries and zone lookups.

Internal Networks Outbound Access Rules



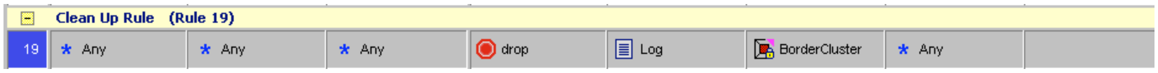
Internal Networks Outbound Access (Rules 16-18)

16	IT_Network Internal_Network	DMZ3_DNS	UDP domain-udp	accept	- None	BorderCluster	Any	
17	Internal_Network RemoteUserPool	Any	TCP http TCP https	accept	- None	BorderCluster	Any	
18	IT_Network	Any	Any	accept	- None	BorderCluster	Any	

Figure 11 -Outbound - Firewall Policy

Rules 16 and 17 address the requirement for the internal users to access the Internet. Internal users are limited in the services that they are permitted to use. For these users, management feels that only http and https are needed to conduct business. The IT department is not limited in the services allowed out. In order to fulfill the duties in securing the network and ensuring seamless connectivity, the services used will vary greatly. These rules are not logged; the internal firewall cluster will handle logging this traffic. Rule 18 allows internal hosts to query the dns server located in DMZ-3 for name resolution.

Clean Up Rule



Clean Up Rule (Rule 19)

19	Any	Any	Any	drop	Log	BorderCluster	Any	

Figure 12 - Clean Up - Firewall Policy

The final rule in the policy is the clean up rule. Checkpoint has an implied rule stating that any traffic that does not match a permitted rule in the policy is dropped. In order for the IT department to understand the network it is necessary to see what users are attempting to do. The Clean Up rule places an explicit drop rule at the end of the policy with logging enabled.

List of References

Barkett, Mike. "Intrusion Prevention Systems." NFR Security, Inc. 20 Dec. 2004. <http://www.nfr.com/resource/downloads/SentivistIPS-WP.pdf > Keyword search: "IPS"

"Broadband Statistics." Last modified 27 Dec. 2004. 28 Dec. 2004. <http://www.itfacts.biz/index.php?id=P2302>

"CERT Advisory." CERT Coordination Center, Carnegie Mellon Software Engineering Institute. 17 Jan. 2002. 28 Dec. 2004. <http://www.cert.org/advisories/CA-2001-19.html> Keyword search: "Code Red"

Desai, Neil. "Intrusion Prevention Systems: The Next Step in the Evolution of IDS." Security Focus. 27 Feb. 2003. 28 Dec. 2004. <http://www.securityfocus.com/infocus/1670> Keyword search: "Intrusion Prevention System"

"Esphion Technical Bulletin ETB-82: W32.Nachi.worm and W32.Welchia.worm." Esphion Ltd. 20 Aug. 2003. 30 Dec. 2004.

<http://www.esphion.com/news/ETB-82.htm> Keyword search: “Nachi icmp”

Fielding, R., J. Gettys, J. Mogul, H. Frystyk, L Masinter, P. Leach, T. Berners-Lee. “RFC 2616- Hypertext Transfer Protocol—HTTP/1.1.” June 1999. 30 Dec. 2004. <http://www.faqs.org/rfcs/rfc2616.html> Keyword search: “rfc http”.

Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson. “CSI/FBI Computer Crime and Security Survey 2004.” Computer Security Institute and San Francisco Federal Bureau of Investigation’s Computer Intrusion Squad. 20 Dec. 2004. < http://www.hands-on-labs.com/only4gurus/techlib/miscellaneous/fbi2004.pdf > Keyword search: “FBI Computer Crime Survey download”

“Intrustion Detection: Reducing Network Security Risk.” Recourse Technologies. 24 Dec. 2001. 30 Dec. 2004. <http://www.isp-planet.com/perspectives/ids_p3.html>

“Intrusion Detection Systems: Defining Protocol Anomaly Detection.” The Symantec Advantage”. Issue 16, Autumn 2003. <http://www.symantec.com/symadvantage/016/pad.html> Keyword search “protocol anomaly detection”

"Intrusion Prevention Systems (IPS)." The NSS Group. Jan 2004. <http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm> Keyword search " intrusion prevention systems'

"June 2004 Bandwidth Report." Web Site Optimization, LLC.19 Jun 2004. 20 Dec 2004. <http://www.websiteoptimization.com/bw/0406/> Keyword search "US broadband users"

Kent Frederick, Karen. "Network Intrusion Detection Signatures." Security Focus. Last 19 Dec. 2001. 28 Dec. 2004. <http://www.securityfocus.com/infocus/1524> Keyword search: "Intrusion Detection Signatures"

Lemonnier, Erwan. "Protocol Anomaly Detection in Network-based IDSs." Defcom. 28 June 2001. 20 Dec. 2004. <http://erwan.lemonnier.free.fr/exjobb/report/protocol_anomaly_detection.pdf> Keyword search: "Protocol Anomaly Detection"

Postel, Jonathan B. "RFC 821- Simple Mail Transfer Protocol." August 1982. 28

Dec. 2004. <http://www.faqs.org/rfcs/rfc821.html> Keyword search: "rfc smtp"

"Protocol Anomaly Detection IDSs." Livermore Software Laboratories, Intl. 9 Sept 2004. <http://www.lsli.com/pad.whitepaper.pdf> Keyword search "protocol anomaly detection"