



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

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



Additionally, the SYSKEY utility (provided by MS Windows NT SP 3) will be used to allow NT passwords to be stored in an encrypted format. SYSKEY adds an extra layer of security to the password data stored in the SAM database by encrypting the hashed password data using a 128-bit system key. Because there is no uninstall option for SYSKEY, the passphrase will be stored in a sealed envelope with a designated person.

For confidential information on the webserver, there are three options:

- (1) Restrictions by IP address, subnet, or domain: Individual documents or whole directories are protected in such a way that only browsers connecting from certain IP (Internet) addresses, IP subnets, or domains can access them.
- (2) Restriction by username and password: Documents or directories are protected so that the remote user has to provide a name and a password in order to get access
- (3) Encryption using public key cryptography: Both the request for the document and the document itself are encrypted in such a way that the text cannot be read by anyone but the intended recipient. Public key cryptography can also be used for reliable user verification.

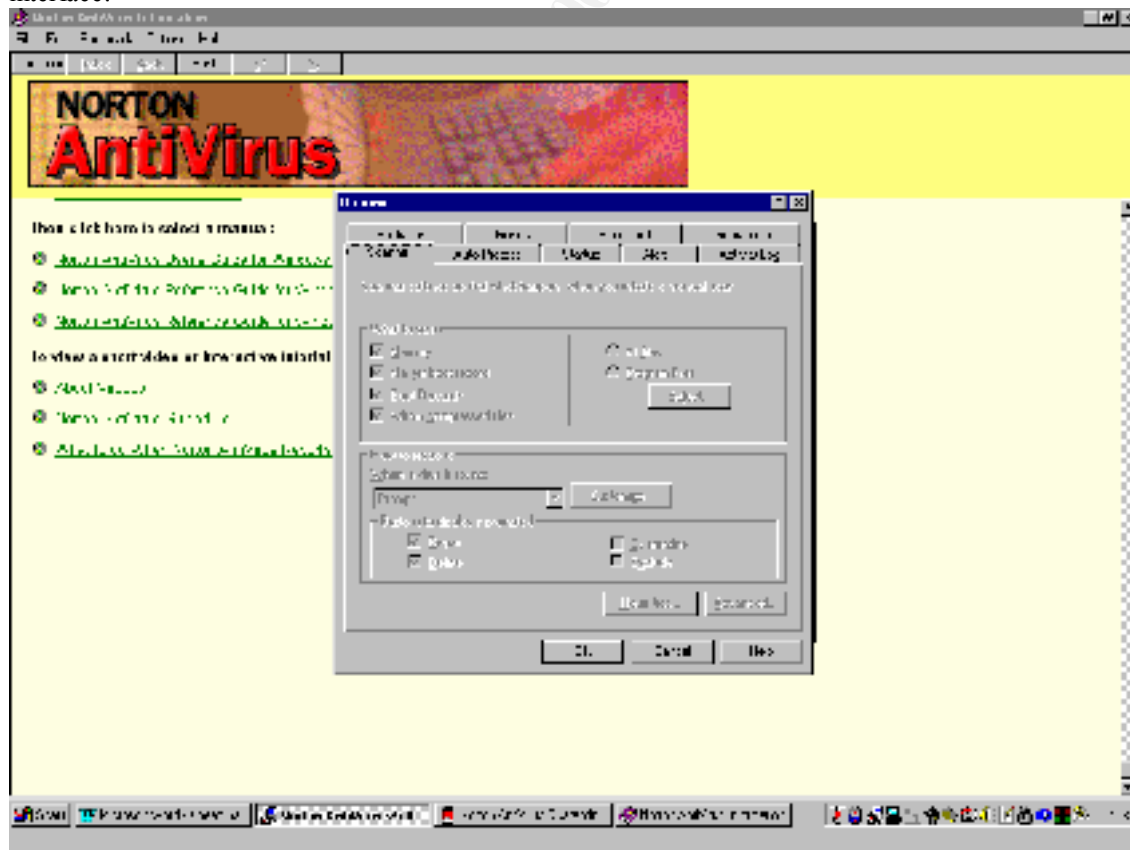
In the above design for GIAC Enterprise's "Online fortune cookie" company, a username and password will protect confidential information on the webserver.

#### 4. Encrypt data sent across networks.

All hosts on the internal network and on the screened network will use SSH, the secure shell, to communicate with other hosts inside the firewall. Using SSH, all traffic between the hosts will be encrypted (<http://www.sans.org/newlook/resources/ssh.htm#16>.)

#### 5. Use and regularly update anti-virus software.

The company will use Norton Antivirus v.5 (<http://www.symantec.com>). Here is an illustration of the interface:



**6. Restrict access to data by business “need to know”.**

MS Windows NT offers file -level access. Using this facility, different user groups can be created (e.g. administrators, online cookie company employees, others) with varying levels of access to files.

**7. Assign unique IDs to each person with computer access to data.**

The requirement for unique IDs will be included in the company’s security policy, and repeated in the relevant sections of the security procedures manual.

**8. Track access to data by unique ID.**

NT auditing will be turned on to create logs of what data is accessed by whom and when it was accessed (NT does not provide logging by default). Before you can audit a file’s activity, you must turn on the Windows NT auditing feature. To do so, start User Manager from the Administrative Tools program group.

**9. Don’t use vendor -supplied defaults for system passwords and other security parameters.**

MS Windows NT SP 2 provides the passfilt.dll filter for systems administrators who choose not to write filters of their own. Later Service Packs has improved the passfilt.dll.

After making a change to the NT registry to include the passfilt.dll, the following password policy is implemented:

- Passwords may not contain your user name or any part of your full name.
- Passwords must be at least six characters long.
- Passwords must contain elements from three of the four following types of characters:

Character types	Examples
English upper case letters	A, B, C, ... Z
English lower case letters	a, b, c, ... z
Westernized arabic numerals	0, 1, 2, ... 9
Non-alphanumeric characters (special characters)	!,%,^

**10. Regularly test security systems and processes.**

There are five parts to this effort:

(1) Because a good audit needs a good baseline, a written procedure will be developed to use MS -supplied tools daily (from the NT Resource Kit at <http://www.microsoft.com/ntserver/nts/downloads/recommended/ntkit/default.asp>). By automating the running of some of these tools (using the NT scheduler ‘AT’ to run a batch job), and e -mailing exceptions to the systems administrator, an understanding of the normal behaviour of the network can be gathered. A popular tool to include in the batch file is NTlast (to extract logon information such as failed and successful logons from an NT server).

(2) The systems administrator will also run public domain analysis tools on the environment (border router, network firewall and the networks protected by the Firewall) weekly. These tools include SATAN and nmap, which scan a host’s ports to identify vulnerabilities.

(3) The staff in the IT department will subscribe to a security advisory service, such as CERT ([http://www.cert.org/contact\\_cert/certmaillist.html](http://www.cert.org/contact_cert/certmaillist.html)) or GIAC (<http://www.sans.org/giac.htm>), to raise awareness within the company of current security threats. Another reason for subscribing to one of these organisations is to have a contact to report suspicious events to. Reporting suspicious activity in logfiles helps the Information Security community, by co -ordinating research efforts to deal with the most common suspicious behaviours.

(4) An external company will be engaged once a year to perform an ethical hack on the environment. This will provide the company’s technical staff with up-to-date information about the latest security tools, and will also verify the integrity of the information security efforts.

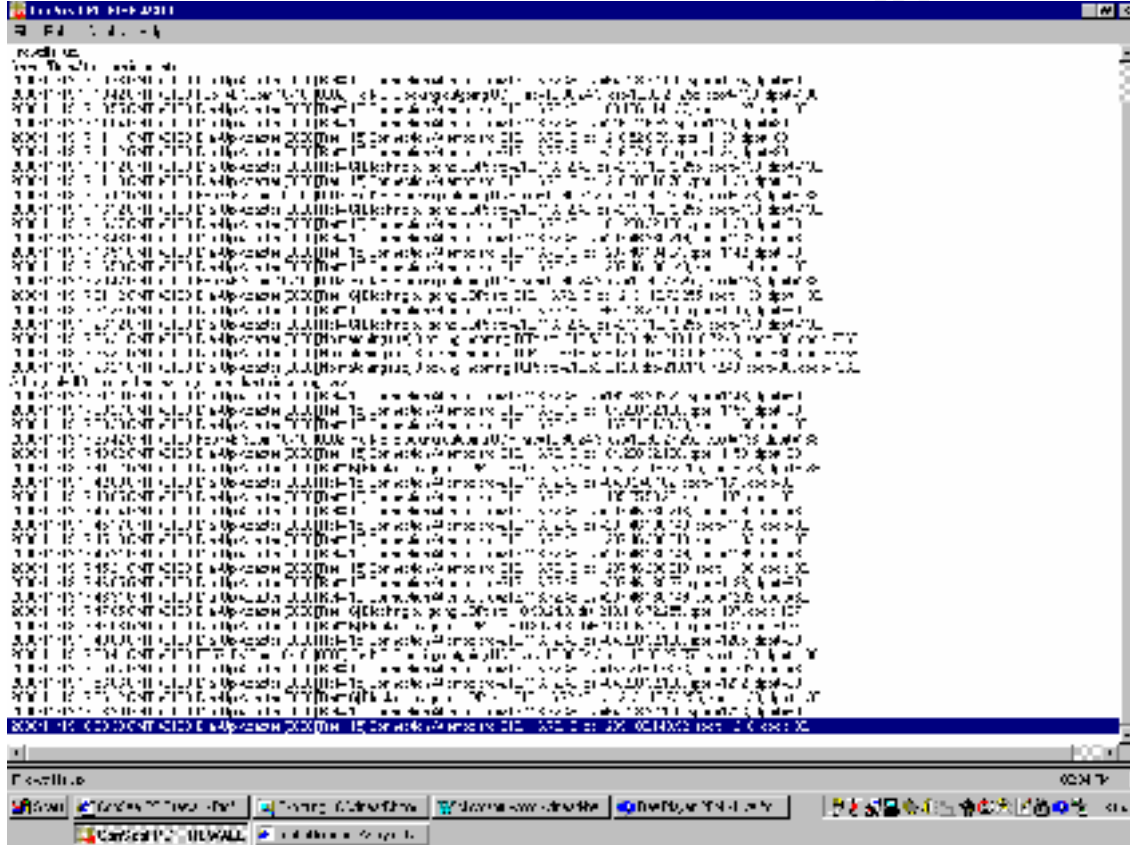
(5) IT staff will test that security components fail to a known state. For instance, should there be a problem with the Fire wall, all network traffic should be blocked rather than automatically let through.

## Assignment 2: Security Policy

This is a tutorial on how to implement filtering at the “Online fortune cookie” company  
ADDITIONAL to that recommended in the SANS Top 10 document  
(<http://www.sans.org/top10.html>).

ConSeal PC Firewall v2.06, developed by the Canada-based firm Signal 9, is the perimeter defence being used. In January 2000, McAfee.com announced that it was taking over Signal 9. Further information about this Firewall is available from <http://www.consealfirewall.com>.

The user interface for the firewall looks like this:



Information on blocking instructions for the “top ten” security vulnerabilities may be found from Gerard Fowley’s practical at <http://www.sans.org/giac/gcfw.htm>. The practical includes blocking instructions for the following traffic:

### Border Router

- Anti spoofing protection and logging for ingress and egress.
- Denial and logging of management or direct access attempts to outer and inner firewalls.
- Denial and logging of egress from unexpected IP addresses.

### Outer Firewall

- Anti spoofing protection and logging for ingress and egress.
- Denial-of-service protection and logging for eCommerce network.
- Static network address translation (NAT) for eCommerce network servers.
- Denial and logging of unexpected management or direct access attempts to inner firewall and border router.
- Denial and logging of egress from unexpected IP addresses.

- Restriction of ingress to eCommerce network and logging of exceptions (probably too much traffic to log all normal access).
- Restriction and logging of egress from eCommerce network.
- Restriction and logging of ingress & egress of Service network.
- Restriction and logging of egress from inner firewall's external dynamic NAT addresses (translated source address of internal egress traffic).
- Denial and logging of all other traffic.

In addition to that filtering, I would recommend the following:

#### **Border Router**

To control the transmission of packets, and to prevent the Network Firewall from becoming a performance bottleneck, the Border Router can do some packet filtering. As the company is an e-commerce site, response times will be very important, and will justify the improved performance that a Border Router will deliver. When choosing a Border Router, some popular options are Cisco, Bay or using a PC clone running a router emulator such as gated.

A CISCO 1600 Series Router "connects Ethernet LANs to WANs via ISDN, asynchronous serial and synchronous serial connections, supporting Frame Relay, leased lines, Switched 56, Switched Multimegabit Data Service (SMDS), and X.25", and is available for less than \$1,300 (<http://www.networkdeals.com/proddetail.asp?LineNumber=171>).

I would recommend ensuring that the anti-spoofing protection includes blocking all inbound packets where the source IP address is a private address (10.\*.\*.\*, 192.168.\*.\*, 172.16.\*.\* - 172.31.\*.\*). Legitimate inbound traffic will have a valid source IP.

A discussion of the importance to the community of egress filtering can be found at <http://www.sans.org/y2k/egress.htm> (Chris Brenton).

#### **Network Firewall**

Signal 9's ConSeal PC Firewall is an IP filtering firewall, i.e. it works at the packet level. It is designed to control the flow of packets based the source, destination, port and packet type information contained in each packet. All traffic is blocked, unless specifically permitted by a firewall rule. Network filters are quicker than the alternatives (e.g. proxy firewalls, stateful firewalls), but do not provide extensive useful logging, and may be compromised by an attacker (by using a permitted service, such as http, to tunnel banned traffic, such as Internet Relay Chat [IRC]).

So, while ConSeal PC Firewall can block communication, it does not inspect the content of the datagram. This underlines the importance of the anti-virus software, and of internet content software (such as NetNanny or SurfControl).

The default setting on the Network Firewall will be to deny all traffic. The initial installation of ConSeal PC FIREWALL permits few services (For instance, outgoing ICMP echo requests and incoming replies are allowed). For maximum efficiency, a Firewall Rulebase will have a small Rulebase (i.e. less than 30 rules). An effective way to generate a suitable Firewall Rulebase is to start with this limited default installation in a test environment, and to use the learning mode to monitor the traffic that attempts to pass through. A decision can then be made on a service-by-service basis, about whether to allow a particular service. After a few days of additions and testing, the Firewall could be put into production, where careful monitoring would be necessary for the first week, to ensure that no essential services were being blocked.

This approach is best combined with an understanding of some popular vulnerabilities. SANS (<http://www.sans.org>) has a list of blocking instructions for the top ten security vulnerabilities. But because some of these blocking instructions may disable needed services, it is important to decide on each one in turn. The test period mentioned earlier provides an ideal opportunity to decide whether or not to implement each of the following blocking instructions:

- (1) Block "spoofed" addresses – packets coming from outside your company sourced from internal addresses or private (RFC1918 and network 127) addresses. Also block source routed packets.
- (2) Login services – telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp).
- (3) RPC and NFS – Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp).
- (4) NetBIOS in WindowsNT – 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows2000 – earlier ports plus 445 (tcp and udp).
- (5) X Windows – 6000/tcp through 6255/tcp.
- (6) Naming services – DNS (53/udp) to all machines, which are not DNS servers, DNS zone transfers (53/tcp) except from external secondaries, LDAP (389/tcp and 389/udp).
- (7) Mail – SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp).
- (8) Web – HTTP (80/tcp) and SSL (443/tcp) except to external Web servers, may also want to block common high-order HTTP port choices (8000/tcp, 8080/tcp, 8888/tcp, etc.).
- (9) "Small Services" – ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)
- (10) Miscellaneous – TFTP (69/udp), finger (79/tcp), NNTP (119/tcp), NTP (123/tcp), LPD (515/tcp), syslog (514/udp), SNMP (161/tcp and 161/udp, 162/tcp and 162/udp), BGP (179/tcp), SOCKS (1080/tcp).

Following on from the SANS list, here are some additional blocking recommendations for this environment:

#### **(1) NetBus 12345/tcp**

Like Back Orifice, NetBus is a trojan -horse program that allows a remote user to access and control your machine by way of its Internet link.

#### **(2) Back Orifice 31337/tcp**

Here is a sample filter to block this trojan -horse.

```
Reference #42:
Block in and out
Remote Address and Mask: 10.90.24.250 / 255.255.255.255
Remote port range 1024-5000 Temp. Range
Local Address and Mask: 127.0.0.1 / 255.255.255.255
This local address is 'My Address'
Local port 31337 BO -Danger!!!
Priority 100
Applies always
```

#### **(3) Internet Relay Chat (IRC) 6660 -6667/tcp**

Block 6660-6667/tcp to block IRC traffic from crossing the firewall. The use of IRC has a network bandwidth cost, and may also bring the company's network to the attention of hackers.

#### **(4) Streaming Audio 7070/tcp, 6970 -7170/udp**

The use of Streaming Audio (e.g. people listening to radio stations over the internet) also causes network bandwidth problems. Clients receive incoming audio streams from servers on UDP ports in the range 6970-7170. This is setup by the outgoing control connection on TCP port 7070.

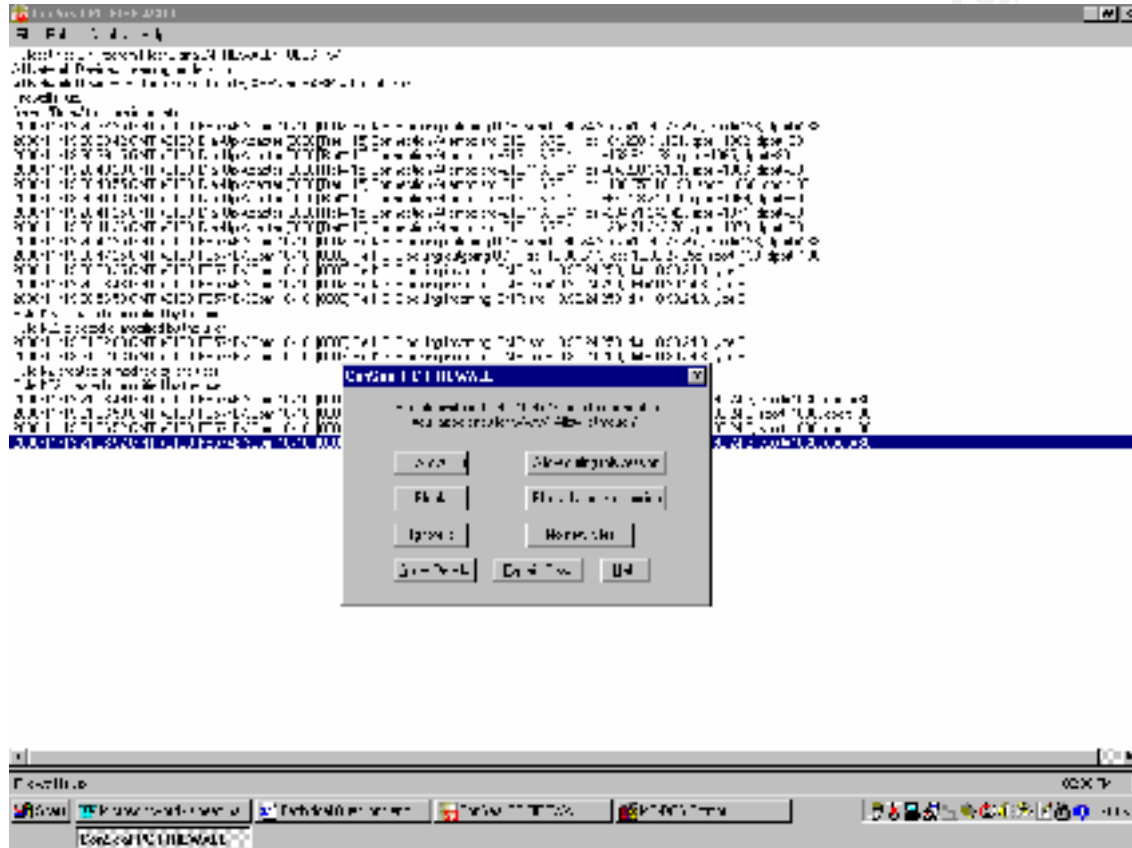
#### **(5) PowWow 13223/tcp**

The "PowWow" chat program from Tribal Voice allows users to open up private chat connections with each other on this port. The program is very aggressive at trying to establish the connection and



will "camp" on the TCP port waiting for a response. This causes a connection attempt at regular intervals like a heartbeat.

These additional filters can be supplemented by the learning mode of the firewall. Here is an illustration of ConSeal PC FIREWALL alerting the technician that a service is requesting permission to pass through the Firewall. The technician can then choose from the following options: Allow, Allow during this session, Block, Block during this session or Ignore. ConSeal PC FIREWALL also offers further details about the service:



Using this approach, the following Rulebase was created:

There is one ruleset for all network devices

Advanced:

Protocols other than IP, ARP and RARP are blocked

Ref#	Description	A/B	Dir	Remote
Address	Remote Mask	Remote Port s	Local Address	Local Mask
Local Ports	Usage	Priority	Option	Flags
TCP rules:				
30	Block 'Land' attack.	Block	In	Out My
Address	255.255.255.255	All Ports	My Address	
255.255.255.255	All Ports	Always	20	w
12	Allow Identification.	Allow	In	Out All
Addresses	0.0.0.0	All Ports	My Address	
255.255.255.255	Identification	Always	90	F w



```

45 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Allow In Out
255.255.255.255 NetBIOS Always 100 * F
43 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 PCAnywhere Always 100 *
42 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 BO -Danger!!! Always 100 *
40 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 Netbus -Danger!!! Always 100 *
35 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Allow In Out
255.255.255.255 HTTPS Always 100 * F
34 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Allow In Out
255.255.255.255 8080 -8080 Always 100 * F
33 TCP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Allow In Out
255.255.255.255 WWW Always 100 * F
31 TCP/IP
216.52.6.120 255.255.255.255 WWW My Address Block In Out
255.255.255.255 7366 -7366 Always 100 *
15 Allow most Internet access (using TCP). Allow In Out All
Addresses 0.0.0.0 All Ports My Address
255.255.255.255 Temp. Range Always 100 F C
5 Block WinNuke, fileshares and printshares during d Block In Out All
Addresses 0.0.0.0 All Ports My Address
255.255.255.255 NetBIOS Dialup Active 100 1
UDP rules:
44 UDP/IP
10.90.24.250 255.255.255.255 1041 -1041 My Address Block In Out
255.255.255.255 2001 -2001 Always 100 *
41 UDP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 BO -Danger!!! Always 100 *
39 UDP/IP
10.90.24.250 255.255.25 5.255 Temp. Range My Address Allow In Out
255.255.255.255 Ftp Always 100 * F
38 UDP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 8000 -8000 Always 100 *
37 UDP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 8881 -8881 Always 100 *
36 UDP/IP
10.90.24.250 255.255.255.255 Temp. Range My Address Block In Out
255.255.255.255 8888 -8888 Always 100 *
9 Allow name resolution (DNS). Allow In Out All
Addresses 0.0.0.0 DNS My Address
255.255.255.255 Temp. Range Always 100 F
6 Block NetBIOS during dialup. Block In Out All
Addresses 0.0.0.0 NetB IOS My Address
255.255.255.255 NetBIOS Dialup Active 100 1
7 Allow NetBIOS (when no dialup is active). Allow In Out All
Addresses 0.0.0.0 NetBIOS All Addresses 0.0.0.0
NetBIOS Always 200 F
ICMP rules:

```

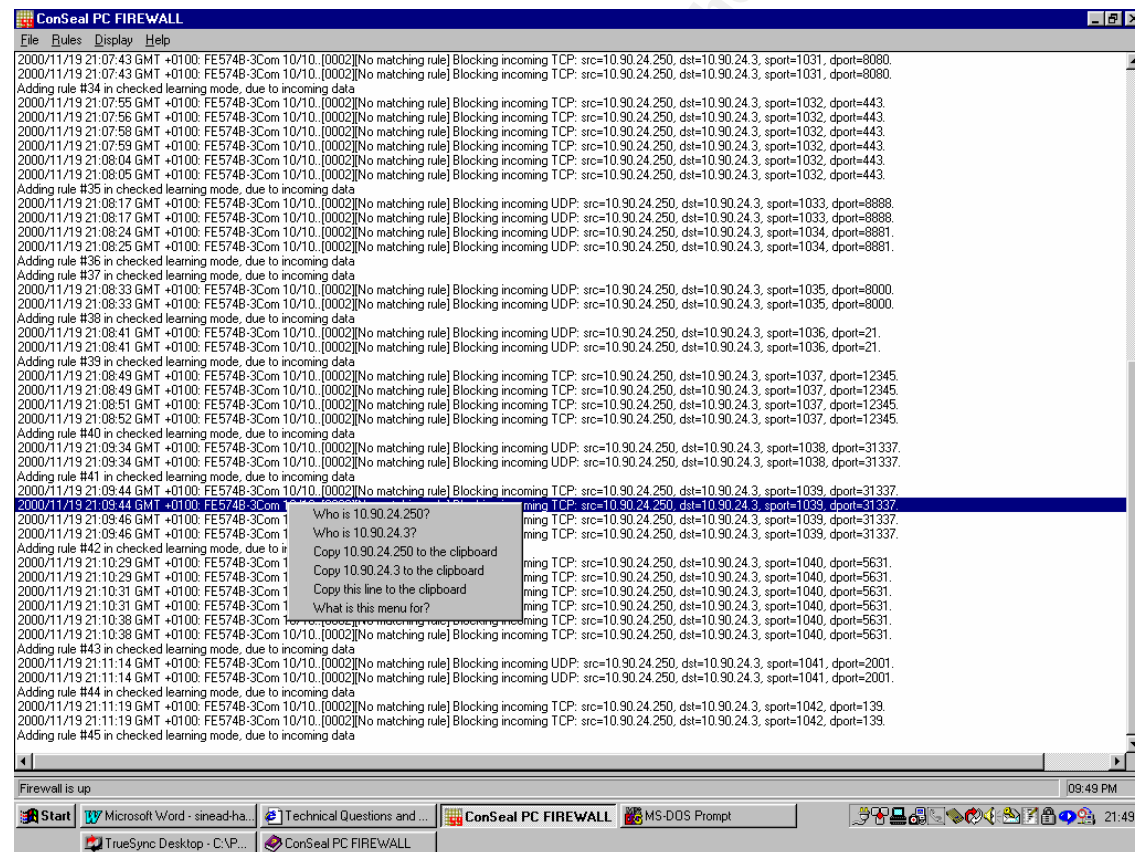
```

2 Ping others.
Addresses 0.0.0.0 Ping Reply My Address Allow In Out All
255.255.255.255 Ping Send Always 10 0 F
32 Allow ICMP Echo Reply
Addresses 0.0.0.0 Ping Send My Address Allow In Out All
255.255.255.255 Ping Reply Always 100 L
3 Block ICMP nukes and more.
Addresses 0.0.0.0 All Types All Addresses 0.0.0.0 Block In Out All
All Types Always 200 w
ARP rules:
1 Allow ARP.
Addresses 0.0.0.0 All Addresses 0.0.0.0 Allow In Out All
Always 100 F
RARP rules:
No rules, all traffic will be blocked.

```

The traffic used to test the Rulebase was generated by ISS Internet Scanner. This is why in this example there are so many vulnerabilities expressly blocked. In reality, this is not necessary because the default setting is “No rules, all traffic will be blocked”.

Here is an illustration of the log information generated by the ISS scan:



Note that information is provided about the source IP address, the source port, the destination IP address, the destination port, a description of the traffic and a timestamp. By right clicking an entry, the technician can do a DNS lookup to identify the hostname from the IP address.

Of course, one can also add filters manually. ConSeal PC FIREWALL offers an easy to use interface for adding new rules. In addition, one can view the syntax of the rules provided by the initial

[illegible]

Firewalls can also provide protection from routing -based attacks, such as source routing and attempts to redirect routing paths to compromised sites via ICMP redirects. A firewall could reject all source -routed packets and ICMP redirects and then inform administrators of the incidents.

c:\adlib express\work\sinead hanley\_gcfw.doc\DC

## Assignment 3: Audit of the security architecture

### A. Assessment plan

An audit is a process of review to identify configuration errors in the environment. It differs from a penetration test (where a single weakness is found and then exploited) in that the goal is to identify as many risks as possible and then to eliminate those risks.

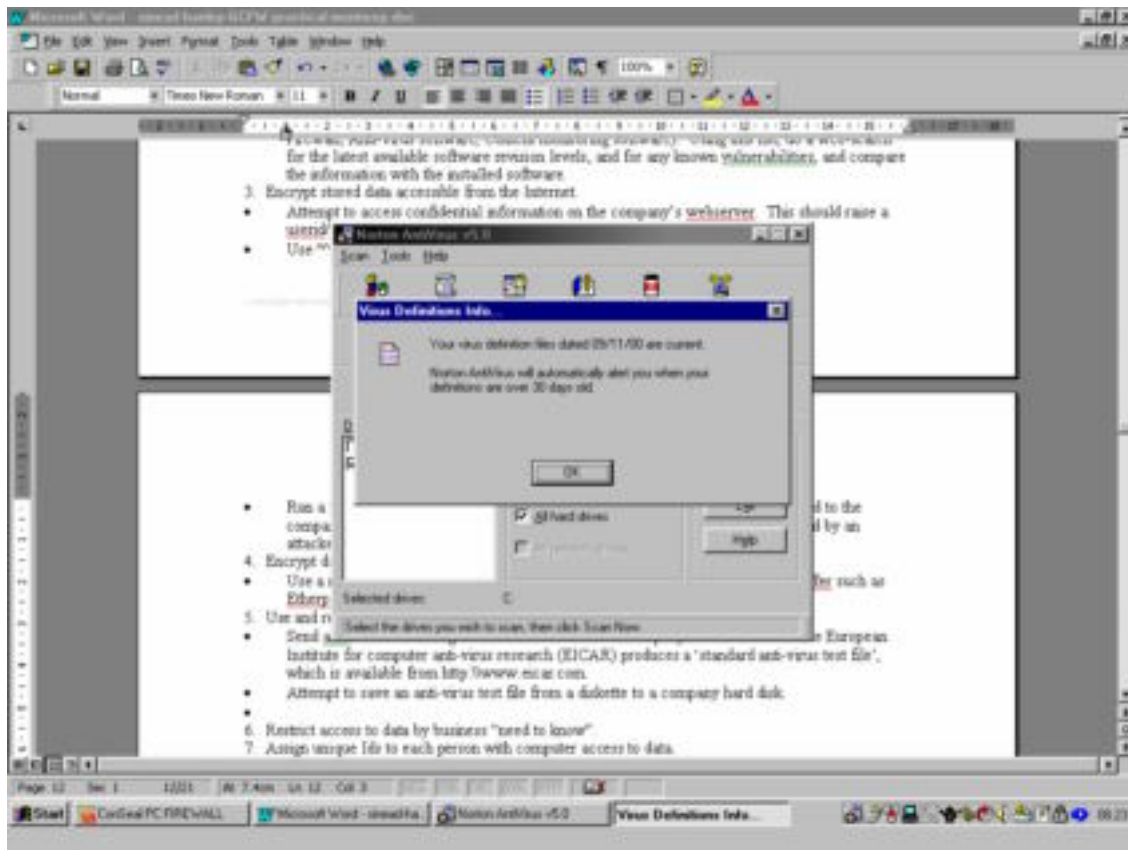
Here is the approach I recommend:

- Begin with a baseline of normal activity, which can be gathered from the on-site technician, and from viewing the event logs.
- Identify the operating system levels and patch levels across the company's environment. Consistent software revision levels make an attacker's job more difficult (it limits the exploits available to him), and the company's technician's job easier (with fewer revision levels to consider, it is easier to focus on and act on relevant security alerts).
- Identify those staff members who have dedicated Information Security responsibilities.
- Gather all relevant documentation (such as Security Policy, Security Procedures Document, Firewall configuration document, Firewall procedures document, Network diagrams, and Employee handbook).
- Arrange a suitable time to carry out the audit. Although network analysis tools can create performance problems if run at peak times, it is important to have access to the on-site personnel, so the audit is likely to be carried out during normal business hours.
- The costs of performing the audit (in terms of the time of internal and external personnel) must be balanced against the thoroughness of the tests. Three days is enough to identify a task list of urgent things to attend to. It is prudent to budget for two people (ideally, if the budget allows, one of these will be external to the company) for three days.
- Get agreement from the on-site IT staff to have a closing meeting to discuss the results, and then for the on-site staff to follow up any outstanding points, e.g. investigate unexplained open ports.
- Some audit tools (e.g. Axent's NetRecon and ISS Internet Scanner) are expensive. In many cases, alternative tools are available in the public domain.
- Identify the risks in performing the audit, and communicate these risks to management at the company. Vulnerability scanning tools can have unpredictable results, e.g. a Denial of Service (DOS) attack against the company itself. Network performance may be negatively affected by audit tool activity. Password cracking tools may violate user privacy. It is important to get written approval for the audit from the company's management before beginning any work.

Here is a plan to test all of the VISA requirements:

1. Install and maintain a working network firewall to protect data accessible via the Internet.
  - Using the Rulebase documentation, attempt to pass traffic through the Firewall that should be blocked. The audit is verifying that the Firewall has been correctly configured. For example, while a certain type of traffic is prohibited by a Firewall rule, the position of the rule in the Rulebase might prevent the rule from being triggered.
  - Run a vulnerability scanner (such as Axent's NetRecon) on the network from outside the firewall. The results of this scan will further test the existing configuration, and will also suggest additional services to block.
  - Run a port scanner such as nmap against the firewall.
  - Check that the software revision level of the Firewall is up-to-date, to avoid unnecessary vulnerabilities.

- Assess whether there are procedures in place to amend the firewall's Rulebase. If there are none, the environment is vulnerable to a social engineering attack, where an attacker could simply call the firewall administrator, and ask for a particular service to be allowed. The traffic that a firewall should block (e.g. Internet Relay Chat – IRC) should be listed in the company's security policy.
  - Assess whether the company's security team has a good idea of baseline network activity, through regular monitoring of system and security application logs, and through regular monitoring of the open ports on systems (using 'netstat -a').
  - Assess whether the Firewall's underlying operating system has been hardened to become a bastion host. If the underlying operating system security is weak, then the Firewall's Rulebase can be easily circumvented.
2. Keep security patches up -to-date.
    - Prepare a list of the company's installed operating systems and security software (BIND, Firewall, Anti-virus software, Content monitoring software). Using this list, do a web-search for the latest available software revision levels, and for any known vulnerability, and compare the information with the installed software.
  3. Encrypt stored data accessible from the Internet.
    - Attempt to access confidential information on the company's webserver. This should raise a userid/password challenge.
    - Use a tool like 'sental' to search for unprotected shares on the internal networks.
    - Run a wardialer (such as toneloc, or phonesweep) against the range of telephone numbers assigned to the company. This will identify any modems set to auto-answer, which could be used by an attacker to access confidential information.
  4. Encrypt data sent across networks.
    - Use a network sniffer (either the free tcpdump/windump, or purchase a commercial sniffer such as Etherpeek or Observer) to analyse traffic across the network.
  5. Use and regularly update anti -virus software.
    - Send an e-mail containing an anti -virus test file to a company e-mail address. The European Institute for computer anti-virus research (EICAR) produces a 'standard anti -virus test file', which is available from <http://www.eicar.com>.
    - Attempt to save an anti -virus test file from a diskette to a company hard disk.
    - Check how recent the installed anti -virus software is. If the anti-virus engine is not up -to-date, it may not be able to make full use of the latest anti -virus signatures.
    - Check how recent the installed anti -virus signatures are across a sample of the company's machines. This sample should include a machine from a mobile worker. Here is an illustration of a query on the age of the anti -virus signatures:



6. Restrict access to data by business “need to know”.
  - Check which NT groups have been created, and which users are in each group, using either the standard net.exe, or if you have access to the NT resource kit, use addusers.exe, which documents both local and global accounts.
  - Attempt to access a file that should be restricted to users in the Administrator group, while logged in as a standard user.
7. Assign unique IDs to each person with computer access to data.
  - Check the written procedures used by the IT staff to create user IDs to assess whether unique IDs are emphasised.
  - Question a random sample of users to assess that unique IDs are actually assigned.
  - Ask the IT staff whether any there are any pool user IDs, ‘visitor’ for instance.
  - Use ‘NTlast’ to check the logon information for signs of an account being used by more than one person.
8. Track access to data by unique ID.
  - Ensure that NT auditing has been turned on.
  - Ensure that there is a written list of those files that are confidential, and whose access must be logged.
  - Ask to see the logs for these confidential files, and assess whether there is a process in place to escalate failed access attempts. There are many security tools available, but the most secure environment is one where as much of the audit effort as possible is automated, with exceptions reported to on-site IT staff. In this way, the burden on staff to manually look through log files is lessened.
9. Don’t use vendor-supplied defaults for system passwords and other security parameters.
  - If management have given written permission, run a password cracker against the password file. Some commercial vulnerability scanners (e.g. Axent’s NetRecon) include password cracking as an option, but there are also powerful tools available for free in the public domain,

- e.g. l0phtcrack (available from <http://www.l0pht.com>). Beware of unintentionally locking users' accounts if the maximum number of permitted wrong attempts is reached.
- Check the guidelines that users are given about setting passwords, to establish whether they are encouraged to set strong passwords. However, as the Germans say "Vertrauen ist gut; Kontrolle ist besser".
  - Ask for a new user account to be created, and attempt to set a new password to see the password setting controls first hand.
  - Ask whether passfilt.dll has been implemented, or whether the administrator has written a custom filter of his own to harden the password controls.
10. Regularly test security systems and processes.
- Look for evidence of regular self-tests by the on-site IT staff, using publicly available tools such as nmap and tcpdump.
  - Attempt some social engineering, by telephoning the IT desk, and asking for a password to be reset. Ideally, this attempt should reveal that the company's staff are regularly briefed about and tested on security issues.
  - Without a company culture that emphasises the importance of Information Security, any controls put in place are open to abuse from employees. Assess security awareness within the company by speaking with some employees. Security awareness can be raised through posters, through lunchtime sessions, through competitions, through e-mail updates, and through spot checks with penalties. For example, if a company has a clear desk policy (physical security is equally important as logical security), one could confiscate any documents/keys found lying on desks when people have gone home. The penalty for violating the clear desk policy could be that a person needs to get his manager to send an e-mail to the security team to get the document back.

## B. Implement assessment

To confirm that the firewall & perimeter router are actually implementing the security policy, I would use the commercial scanner: ISS Internet Scanner.

This scanner uses profiles to configure which tests to perform. There are two key dimensions to the security audit: 1. Verify that there are no configuration errors in the environment, i.e. make sure that certain traffic is actually being blocked if everyone thinks that it is being blocked. 2. Suggest ways to improve the current configuration, based on industry best practice and on an analysis of the audit logs.

I would create an ISS Internet Scanner profile to test the existing configuration: a level three NT scan with both Brute Force and Denial of Service options turned off. Using the Brute Force option can lead to accounts being locked out en masse. It would be equally unpleasant if one of the 79 possible Denial of Service attacks succeeded during business hours (and as this is an e-commerce environment, there are no restrictions on business hours).

Here is an illustration of the ISS Internet Scanner interface:







- The results of the ISS scan be followed up, e.g. to investigate whether each running service is a required service. This process should result in changes to the configuration to reflect the any vulnerabilities.
- Employee awareness of security be raised.
- A hardware support contract be arranged, so that should the firewall or border router need to be serviced, a replacement could be provided within an agreed amount of time, and the business' revenue would not be jeopardised.
- There be a weekly review of the Firewall logs to ensure that the Rulebase is behaving as expected, and to look for patterns of suspicious activity.
- Someone be made responsible for Information Security in the environment. This gives the rest of the company a focal point, and it means that security issues are less likely to fall to the bottom of everyone's priority list.

## APPENDIX 1: DETAILED RULEBASE for ConSeal PC FIRE WALL

Ruleset file for ConSeal PC FIREWALL  
Created on Windows 95/98, file format v1.2

Firewall State:  
Firewall is Up  
Logging is on  
Start in the desktop (not SysTray)

Ruleset Scope:  
One Ruleset for All Network Devices

Ruleset Usage:  
Always

Password:  
Password not used

There is one ruleset for all network devices

Next Reference Number: 46

Learning mode: Checked (the user is prompted when new traffic is found)

Advanced:  
Protocols other than IP, ARP and RARP are blocked

TCP rules:  
Traffic using this protocol that does not match a rule will be blocked

Reference #30:  
Block 'Land' attack.

Description: This attack tries to make your system  
connect to itself, causing it to stop responding and  
requiring a reboot.

Details: The Priority of 20 makes it take precedence  
of other rules. The remote address is 'My Address'  
because the attack spoofs it to make it appear to have

come from your system.  
Service: Identification  
Block in and out  
Remote Address and Mask: 127.0.0.1 / 255.255.255.255  
This remote address is 'My Address'  
Remote port range 0 -65535 All Ports  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port range 0 -65535 All Ports  
Priority 20

c:\adlib express\work\sinead\_hanley\_gcfw.doc\DC

Applies always

Options:

- F - block fragments (takes effect only on allow rules)
- w - Log Once (warn, no more than once every 2 seconds)

Reference #12:

Allow Identification.

Description: Some systems require your identity before allowing you to access services, such as email and IRC.

Details: The remote system makes an incoming connection so this rule allows incoming connections. The Warning beep is on so you know when your identity is being accessed.

Service: Identification

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port range 0 -65535 All Ports

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 113 Identification

Priority 90

Applies always

Options:

- F - block fragments (takes effect only on allow rules)
- w - Log Once (warn, no more than once every 2 seconds)

Reference #45:

Allow in and out

Remote Address and Mask: 10.90.24.250 / 255.255.255.255

Remote port range 1024 -5000 Temp. Range

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 139 NetBIOS

Priority 100

Applies always

Options:

- \* - rule was made in learning mode
- F - block fragments (takes effect only on allow rules)

Reference #43:

Block in and out

Remote Address and Mask: 10.90.24.250 / 255.255.255.255

Remote port range 1024 -5000 Temp. Range

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 5631 PCAnywhere

Priority 100

Applies always

Options:

- \* - rule was made in learning mode
- F - block fragments (takes effect only on allow rules)

Reference #42:  
Block in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024-5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 31337 BO -Danger!!!  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #40:  
Block in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024-5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 1234 5 Netbus-Danger!!!  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #35:  
Allow in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024-5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 443 HTTPS  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #34:  
Allow in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024-5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 8080 8080-8080  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #33:  
Allow in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024-5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 80 WWW  
Priority 100  
Applies always

Options:

- \* - rule was made in learning mode
- F - block fragments (takes effect only on allow rules)

Reference #31:

Block in and out

Remote Address and Mask: 216.52.6.120 / 255.255.255.255

Remote port 80 WWW

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 7366 7366 -7366

Priority 100

Applies always

Options:

- \* - rule was made in learning mode
- F - block fragments (takes effect only on allow rules)

Reference #15:

Allow most Internet access (using TCP).

Description: This rule allows you to do web browsing, email, IRC and most other (TCP -based) services. The rule is not made to allow others to access services on your system.

Details: The local port range, 1024 -5000, is all you usually need to access remote services. Most services on your system are in the range 1 -1023. Incoming connections are allowed so DCC and FTP will work.

If you block incoming connections, use FTP PASV mode.

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port range 0 -65535 All Ports

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port range 1024 -5000 Temp. Range

Priority 100

Applies always

Options:

- F - block fragments (takes effect only on allow rules)
- C - Log Connection (logs the allowed TCP connection attempts)

Reference #5:

Block WinNuke, fileshares and printshares during dialup.

Description: This rule blocks access to your hard drive



while you have a dialup connection active. The WinNuke attack attempts to connect (to port 139) to make your system crash. The rule is intended to protect people while dialed out to the Internet.

Details: This rule blocks TCP port 139. It is only active during dialup. To change this, click the Next button below to see the Usage page and change when

the rule applies.

Service: Fileshares -TCP

Block in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port range 0 -65535 All Ports

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 139 NetBIOS

Priority 100

Applies when dialup is active

Options:

- F - block fragments (takes effect only on allow rules)

- 1 - Log Once (log blocked packets, no more than once every 2 seconds)

UDP rules:

Traffic using this protocol that does not match a rule will be blocked

Reference #44:

Block in and out

Remote Address and Mask: 10.90.24.250 / 255.255.255.255

Remote port 1041 1041 -1041

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 2001 2001 -2001

Priority 100

Applies always

Options:

- \* - rule was made in learning mode

- F - block fragments (takes effect only on allow rules)

Reference #41:

Block in and out

Remote Address and Mask: 10.90.24.250 / 255.255.255.255

Remote port range 1024 -5000 Temp. Range

Local Address and Mask : 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port 31337 BO -Danger!!!

Priority 100

Applies always

Options:

- \* - rule was made in learning mode

- F - block fragments (takes effect only on allow rules)

Reference #39:

Allow in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024 -5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 21 Ftp  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #38:  
Block in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024 -5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255. 255.255  
This local address is 'My Address'  
Local port 8000 8000 -8000  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #37:  
Block in and out  
Remote Address and Ma sk: 10.90.24.250 / 255.255.255.255  
Remote port range 1024 -5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 8881 8881 -8881  
Priority 100  
Applies always  
Options:  
\* - rule was made in learnin g mode  
F - block fragments (takes effect only on allow rules)

Reference #36:  
Block in and out  
Remote Address and Mask: 10.90.24.250 / 255.255.255.255  
Remote port range 1024 -5000 Temp. Range  
Local Address and Mask: 127.0.0.1 / 255.255.255.255  
This local address is 'My Address'  
Local port 8888 8888 -8888  
Priority 100  
Applies always  
Options:  
\* - rule was made in learning mode  
F - block fragments (takes effect only on allow rules)

Reference #9:  
Allow name resolution (DNS).

Description: This rule al lows your system to ask your  
DNS server to translate a name like 'www.signal9.com'

to an IP address like 195.151.12.15. This is necessary for web browsing and most other services.

Details: Most attacks are based on sending fragments.

This rule blocks fragments, so you should be safe.

Most Internet users talk to DNS servers provided by

their ISP.

Service: DNS

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port 53 DNS

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port range 1024 -5000 Temp. Range

Priority 100

Applies always

Options:

F - block fragments (takes effect only on allow rules)

Reference #6:

Block NetBIOS during dialup.

Description: Your system announces its presence on a network when it connects. There is no need to send this to the Internet.

Details: This rule applies when dialup is active. It is intended to protect people dialing in to the Internet.

To change it, select the Next button to get to the

Usage page and change when the rule applies. The

Priority value is 100 so it takes precedence over rule

7, which would allow NetBIOS otherwise.

Service: Fileshares -UDP

Block in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port range 137 -138 NetBIOS

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Local port range 137 -138 NetBIOS

Priority 100

Applies when dialup is active

Options:

- F - block fragments (takes effect only on allow rules)
- 1 - Log Once (log blocked packets, no more than once every 2 seconds)

Reference #7:

Allow NetBIOS (when no dialup is active).

Description: This rule allows your system to announce its presence. It is only used when you are not dialed out.

Details: The Priority is 200, which means rule 6 takes precedence when dialup is active. This rule will only

allow with dialup is inactive and rule 6 is not in use.

Service: Fileshares -UDP

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Remote port range 137 -138 NetBIOS

Local Address and Mask: 255.255.255.255 / 0.0.0.0

This is all local addresses

Local port range 137 -138 NetBIOS

Priority 200

Applies always

Options:

- F - block fragments (takes effect only on allow rules)

ICMP rules:

Traffic using this protocol that does not match a rule will be blocked

Reference #2:

Ping others.

Description: This rule allows you to ping others.

Details: The local type allows 'Ping request' out

and the remote type allows 'Ping Reply' in. The

Priority is 100 so this rule takes precedence over

rule 3, which will block all ICMP (including nukes).

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Incoming type 0 Ping Reply

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Outgoing type 8 Ping Send

Priority 100

Applies always

Options:

F - block fragments (takes effect only on allow rules)

Reference #32:

Allow ICMP Echo Reply

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Incoming type 8 Ping Send

Local Address and Mask: 127.0.0.1 / 255.255.255.255

This local address is 'My Address'

Outgoing type 0 Ping Reply

Priority 100

Applies always

Options:

L - Log Always (log all packets blocked by this rule)

Reference #3:

Block ICMP nukes and more.

Description: This rule blocks all ICMP types not allowed by other rules. It blocks the ICMP nuke that makes your system disconnect from services like IRC.

Details: The Priority of 200 means rule 2 takes precedence. If ICMP is received and it is not ping reply, this rule will block it. This rule is important because it blocks ICMP type 3 which is the basis of many attacks that disconnect you from services.

Block in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Incoming type range 0 -255 All Types

Local Address and Mask: 255.255.255.255 / 0.0.0.0

This is all local addresses

Outgoing type range 0 -255 All Types

Priority 200

Applies always

Options:

F - block fragments (takes effect only on allow rules)

w - Log Once (warn, no more than once every 2 seconds)

ARP rules:

Traffic using this protocol that does not match a rule will be blocked

Reference #1:

Allow ARP.

Description: This rule allows your system to know how to reach others. It is allowed because it is not the basis of any known attacks.

Details: Blocking ARP effectively makes you unreachable .

This rule should not be changed unless you really have

to and know what you are doing. It is pretty safe.

Allow in and out

Remote Address and Mask: 255.255.255.255 / 0.0.0.0

This is all remote addresses

Local Address and Mask: 255.255.255.255 / 0.0.0.0

This is all local addresses

Priority 100

Applies always

Options:

F - block fragments (takes effect only on allow rules)

RARP rules:

No rules, all traffic will be blocked.