# Global Information Assurance Certification Paper

Mike Chapple
GIAC Level Two Practical Examination
Certified Firewall Analyst

### *Network Background*

This solution covers the implementation of a perimeter defense mechanism for a small business in the professional services industry. The company has 75 employees with desktop Internet access in a central location connected to the Internet via a single T-1 line and a Cisco router. Low volume web and SMTP servers are maintained for public access. Travelling/home office users do not require VPN access to the corporate network, but do require access to their electronic mail. All such users access the corporate network through the same dial-up ISP. They utilize the ISP's SMTP server for outbound mail but require access to the corporate POP3 server for inbound mail.

### *Perimeter Defense Solution*

Funds are not available for the purchase of a firewall or proxy server product or the associated hardware required to run such software. From a pure security perspective, this would be the ideal solution. However, from a business perspective, the added cost of implementing such measures is prohibitive when compared to the perceived benefit. Therefore, the perimeter defense solution must utilize the existing Cisco router only. Due to the relatively low level of security provided by this solution, special attention must be paid to host-based defenses as well, especially on mission-critical systems.

### *Specific Vulnerability Countermeasures*

Vulnerability: 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.

Description: There are several ranges of IP addresses reserved for internal network use. These ranges are 10.0.0.0 – 10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255. None of these addresses should be seen originating from outside the router.

Network Specific Behavior: The company makes use of addresses in the 192.168 private IP address space. They also possess two "legal" ip addresses (12.8.x.x and 12.8.y.y) for the publicly addressable SMTP/POP server and HTML server, respectively. No traffic should be allowed into the network that bears a private IP address or one of the two legal IP addresses

Filter: acc 101 deny ip 10.0.0.0 0.255.255.255 any

acc 101 deny ip 172.16.0.0 0.15.255.255 any
acc 101 deny ip 192.168.0.0 0.0.255.255 any
acc 101 deny ip host 12.8.x.x any
acc 101 deny ip host 12.8.y.y any
no ip source-route

Filter Description: Each of these lines adds a specific denial to the access list. They specify that all IP packets are to be denied. The first three specify the network address and subnet mask for each private IP range and block incoming traffic from those addresses headed to any host. The next two block any traffic coming from our two "legal" IP addresses. The final line prohibits IP packets that are source-routed.

Filter Testing: The easiest way to test these filters would be to use a packet creation tool outside the router and injecting packets with blocked IP source addresses and valid destination addresses to ensure they are blocked. The difficult way would be to configure hosts with invalid IP addresses and having them attempt connections to the inside. A packet sniffer should be placed inside the router to verify compliance.

---

Vulnerability: Login services-- telnet (23/tcp), SSH (22/tcp), FTP (21/tcp), NetBIOS (139/tcp), rlogin et al (512/tcp through 514/tcp)

Description: These login services allow opportunities for outside users to authenticate themselves to internal machines.

Network Specific Behavior: None of these services are required for legitimate business purposes and they can all be blocked.

Filter: acc 101 deny tcp any any eq 21
acc 101 deny tcp any any eq 22
acc 101 deny tcp any any eq 23
acc 101 deny tcp any any eq 139
acc 101 deny tcp any any range 512 514

Filter Description: These filters are all similar to the previous filters. The two differences are that they block TCP only (as opposed to the previous filters that blocked IP in general) and the last filter blocks a range of ports (as opposed to a single port).

Filter Testing: This is simple to test. Simply use a machine attached to the Internet and attempt connections using these services. The packet sniffer inside the network should not see any related activity and the connection attempt should fail.

---

Vulnerability: RPC and NFS-- Portmap/rpcbind (111/tcp and 111/udp), NFS (2049/tcp and 2049/udp), lockd (4045/tcp and 4045/udp)

Description: These low-level services allow file system and/or operating system manipulation remotely.

Network Specific Behavior: There is no legitimate business need for any of these services at this time and they should all be blocked.

Filter: acc 101 deny tcp any any eq 111
acc 101 deny udp any any eq 111
acc 101 deny tcp any any eq 2049
acc 101 deny udp any any eq 2049
acc 101 deny tcp any any eq 4045
acc 101 deny udp any any eq 4045

Filter Description: Again, these filters are merely variations of the previous ones. They add the characteristic of blocking UDP datagrams as well.

Filter Testing: These rules can be verified using either of the previous methods.

---

Vulnerability: NetBIOS in Windows NT -- 135 (tcp and udp), 137 (udp), 138 (udp), 139 (tcp). Windows 2000 - earlier ports plus 445(tcp and udp)

Description: These ports provide low-level Windows registration, authentication and file services.

Network Specific Behavior: No low-level Windows networking connections should be allowed from remote hosts. All ports should be blocked.

Filter: acc 101 deny tcp any any eq 135
acc 101 deny udp any any eq 135
acc 101 deny tcp any any range 137 139
acc 101 deny udp any any range 137 139
acc 101 deny tcp any any eq 445
acc 101 deny udp any any eq 445

Filter Description: These filters are self-explanatory.

Filter Testing: A packet creation tool would be the best method for testing these rules.

---

Vulnerability: X Windows -- 6000/tcp through 6255/tcp

Description: X Windows services utilize this range of ports to manage user interfaces remotely.

Network Specific Behavior: X Windows is not utilized on this network. All ports should be blocked.

Filter: acc 101 deny tcp any any range 6000 6255

Filter Description: Self-explanatory

Filter Testing: A packet creation tool should be utilized for these rules as well.

---

Vulnerability: 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)

Description: DNS constitutes one of the most significant security threats on the Internet due to the number of known vulnerabilities and the potential for intelligence gathering.

Network Specific Behavior: External DNS hosting for this network is provided by the ISP so there are no publicly available DNS servers and no zone transfers are authorized. LDAP is not implemented. Therefore, all ports should be blocked.

Filter: acc 101 deny tcp any any eq 53
acc 101 deny udp any any eq 53
acc 101 deny tcp any any eq 389
acc 101 deny udp any any eq 389

Filter Description: Self-explanatory

Filter Testing: nslookup and telnet can be used to test the DNS rules from an external host. This should be supplemented by the packet creation tool to test LDAP blocking.

---

Vulnerability: Mail-- SMTP (25/tcp) to all machines, which are not external mail relays, POP (109/tcp and 110/tcp), IMAP (143/tcp)

Description: Mail servers are another major security threat due to the large number of known vulnerabilities and the degree of accessibility required for external connectivity.

Network Specific Behavior: 12.8.x.x is the only machine on the network authorized to receive incoming SMTP traffic. Some external users coming from a dial-up ISP are permitted to use POP services. Their IP addresses will always be in the network aaa.bbb.0.0 with netmask 0.0.255.255. IMAP is not implemented.

Filter: acc 101 permit tcp any host 12.8.x.x eq 25
acc 101 deny tcp any any eq 25
acc 101 permit tcp aaa.bbb.0.0 0.0.255.255 host 12.8.x.x range 109 110
acc 101 deny tcp any any range 109 110
acc 101 deny tcp any any eq 143

Filter Description: The first rule allows incoming SMTP traffic to the mail server. The second rule denies all other incoming SMTP traffic. The third rule allows incoming POP traffic from the known ISP while the fourth rule blocks all others. The final rule blocks all incoming IMAP.

Filter Testing: This rule is best tested with the packet creation tool/sniffer combination.

---

Vulnerability: 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.)

Description: Web servers also constitute a weakness in network defenses due to their inherent accessibility from the outside.

Network Specific Behavior: The only host permitted to offer web services is 12.8.y.y on the well-known port 80. All other HTTP traffic should be blocked. SSL is not implemented and should be blocked for all hosts.

Filter: acc 101 permit tcp any host 12.8.y.y eq 80
acc 101 deny tcp any any eq 80
acc 101 deny tcp any any eq 443
acc 101 deny tcp any any eq 8000
acc 101 deny tcp any any eq 8080
acc 101 deny tcp any any eq 8888

Filter Testing: This rule can be tested using an external machine with a web browser and ensuring the requests are not passed through the router with our packet sniffer.

---

Vulnerability: "Small Services"-- ports below 20/tcp and 20/udp, time (37/tcp and 37/udp)

Description: Low numbered ports provide specified services (like echo and chargen) which should not be accessible from outside the network.

Network Specific Behavior: There is no legitimate business need for these services and they should be disabled.

Filter: acc 101 deny tcp any any lt 20

acc 101 deny udp any any lt 20
acc 101 deny tcp any any eq 37
acc 101 deny udp any any eq 37

Filter Description: These filters are self-explanatory with the addition of the "lt" operator which blocks ports lower than the specified port.

Filter Testing: These rules are best tested utilizing the packet creator/sniffer combination.

---

Vulnerability: 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)

Description: This is a combination of routing protocols, news services, and other functions not normally implemented. Each of these services has some form of known vulnerabilities and should be locked down if not needed.

Network Specific Behavior: None of these services are required by external users and all associated ports should be blocked.

Filter: acc 101 deny udp any any eq 69
acc 101 deny tcp any any eq 79
acc 101 deny tcp any any eq 119
acc 101 deny tcp any any eq 123
acc 101 deny tcp any any eq 515
acc 101 deny udp any any eq 514
acc 101 deny tcp any any range 161 162
acc 101 deny udp any any range 161 162
acc 101 deny tcp any any eq 179
acc 101 deny tcp any any eq 1080

Filter Description: Self-explanatory

Filter Testing: The packet creator/sniffer combination would work best here.

---

Vulnerability: ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and unreachable messages

Description: These ICMP packet types can be used to gather intelligence on a network.

Network Specific Behavior: These should be blocked.

Filter: acc 101 deny icmp any any echo

acc 102 deny icmp any any echo-reply
acc 102 deny icmp any any time-exceeded
acc 102 deny icmp any any host-unreachable

Filter Description: Self-explanatory

Filter Testing: These can be tested utilizing the ping and traceroute tools as well as a packet creator from outside the network. Additionally, the packet creator and sniffer should have their positions reversed to double-check that the prohibited output activities do not pass through the router to the Internet.

### *Filter Order*

Overall, it should be observed that this implementation is for academic purposes only to remain within the parameters of this assignment. Due to the relatively few services required by external users, it would be much more efficient (and secure) to simply block all services by default and only permit the few services that are authorized.

That being said, the access lists should be created in the following order:

Access List 101
acc 101 permit tcp any host 12.8.y.y eq 80
acc 101 deny tcp any any eq 80
acc 101 deny tcp any any eq 443
acc 101 deny tcp any any eq 8000
acc 101 deny tcp any any eq 8080
acc 101 deny tcp any any eq 8888
acc 101 permit tcp any host 12.8.x.x eq 25
acc 101 deny tcp any any eq 25
acc 101 permit tcp aaa.bbb.0.0 0.0.255.255 host 12.8.x.x range 109 110
acc 101 deny tcp any any range 109 110
acc 101 deny ip 10.0.0.0 0.255.255.255 any
acc 101 deny ip 172.16.0.0 0.15.255.255 any
acc 101 deny ip 192.168.0.0 0.0.255.255 any
acc 101 deny ip host 12.8.x.x any
acc 101 deny ip host 12.8.y.y any
acc 101 deny icmp any any echo
acc 101 deny tcp any any lt 20
acc 101 deny tcp any any eq 21
acc 101 deny tcp any any eq 22
acc 101 deny tcp any any eq 23
acc 101 deny tcp any any eq 37
acc 101 deny tcp any any eq 53
acc 101 deny tcp any any eq 79
acc 101 deny tcp any any eq 111

```
acc 101 deny tcp any any eq 119
acc 101 deny tcp any any eq 123
acc 101 deny tcp any any eq 135
acc 101 deny tcp any any range 137 139
acc 101 deny tcp any any eq 139
acc 101 deny tcp any any eq 143
acc 101 deny tcp any any range 161 162
acc 101 deny tcp any any eq 179
acc 101 deny tcp any any eq 389
acc 101 deny tcp any any eq 445
acc 101 deny tcp any any range 512 514
acc 101 deny tcp any any eq 515
acc 101 deny tcp any any eq 1080
acc 101 deny tcp any any eq 2049
acc 101 deny tcp any any eq 4045
acc 101 deny tcp any any range 6000 6255
acc 101 deny udp any any lt 20
acc 101 deny udp any any eq 37
acc 101 deny udp any any eq 53
acc 101 deny udp any any eq 69
acc 101 deny udp any any eq 111
acc 101 deny udp any any eq 135
acc 101 deny udp any any range 137 139
acc 101 deny udp any any range 161 162
acc 101 deny udp any any eq 389
acc 101 deny udp any any eq 445
acc 101 deny udp any any eq 514
acc 101 deny udp any any eq 2049
acc 101 deny udp any any eq 4045
acc 101 permit ip any any
```

Access List 102

```
acc 102 deny icmp any any echo-reply
acc 102 deny icmp any any time-exceeded
acc 102 deny icmp any any host-unreachable
acc 102 permit ip any any
```

The rationale for this ordering is really quite simple. First, some of the permit and deny rules are ordered so that the permissive rules appear before the restrictive ones. For example, we first allow specific HTTP activity to the authorized server. The next series of rules blocks all HTTP activity. This is due to the fact that Cisco IOS interprets the rules in a top-down fashion and acts upon the first matching rule. For a similar reason, some of the more commonly-used rules (like HTTP and SMTP) have been moved to the top of the list to save processing time. The remainder of the rules are simply sorted first by protocol and then by port for readability. Finally, each access list ends with a rule that permits all activity that is not explicitly denied. I would prefer the inverse – denying all

activity which is not specifically permitted – but that was outside the parameters of this assignment.

### *Implementation*

Once the access lists have been input, the configuration is relatively straightforward:

int s0 (to access the interface)
ip access 101 in (to apply the ingress filtering rules)
ip access 102 out (to apply the egress filtering rules)
no ip source-route (to implement the no source-routing requirement)