Global Information Assurance Certification Paper

Marilyn Morris
San Jose Track 3 Practical Assignments

Exam questions for 3.1 TCP/IP for Intrusion Detection and Perimeter Defense

1) Which is **not** one of TCP/IP's four layer protocol stacks?
   a) application
   b) session
   c) transport
   d) network

Answer: b

2) A host running tcpdump gathers:
   a) packets addressed to that host only
   b) packets sent by that same host
   c) all packet traffic on the network
   d) the IP addresses of all hosts on the network

Answer: c

3) Which TCP flag terminates a connection gracefully?
   a) reset
   b) stop sig
   c) syn
   d) fin

Answer: d

4) What does the –x option in tcpdump do?
   a) makes it execute
   b) shows the output in hexadecimal
   c) gives a short version of the output
   d) gives an expanded version of the output

Answer: b

5) A nibble is:
   a) half of a byte
   b) how hexadecimal output is expressed
   c) the lowest unit of I/O possible
   d) two bytes

Answer: a

6) What are the terms for the logical address of a host interface and the hardware address respectively?
   a) LU and MAX
   b) IP and MAC
   c) They are both called TCP/IP
   d) Local and MACH

Answer: b

7) A fragment ID number:
   a) is randomly assigned, then incremented by the number of bytes sent in each fragment of the datagram
   b) is incremented by 1 for each fragment sent
   c) remains the same for all fragments of a single IP datagram
   d) is the same as the IP address of the sender

Answer: c

8) The reply to a request for a TCP session will have which flag(s) in it?
   a) both a syn and an ack
   b) an ack only
   c) a fin only
   d) a syn and a fin

Answer: a

9) What is MTU discovery?
   a) when a host queries for another host's machine address
   b) when a hacker tries to find out what ports are listening on a Web server
   c) when a firewall attempts to discover the source of malicious packets
   d) when a host intentionally sets the DF flag on a large datagram to find out the maximum transmission unit for hosts along the destination path

Answer: d

10) Why does DNS use TCP sometimes and UDP other times?
   a) because of high demands, it uses whichever is available at the time
   b) most queries are short and can be sent UDP; zone transfers go TCP
   c) it depends on how DNS is configured
   d) it depends on what the firewall allows

Answer: b

Exam questions for 3.2 Firewalls 101

1) As far as a security mechanism, a firewall is
   a) all you ever need if properly configured
   b) the last resort
   c) can keep out unwanted traffic and provide one layer of security
   d) just like a router

Answer: c

2) Screened networks and DMZ servers are:
   a) basically the same
   b) different in structure, but have the same level of protection
   c) screened networks are made up o DMZ servers
   d) screened networks have firewall protection, DMZ servers are outside the firewall

Answer: d

3) If a bridge receives a packet it doesn't know the address of, it will
   a) forward it
   b) send it back
   c) discard it
   d) return it with an error

Answer: a

4) An increased number of broadcasts over a network is
   a) a sign of speed and efficiency – very desirable
   b) caused by packet filtering
   c) increases CPU load and decreases bandwidth
   d) can be decreased by adding bridges

Answer: c

5) a Hub is also called a
   a) bridge
   b) concentrator
   c) router
   d) power pak

Answer: b

6) Where is the preferred place to filter "noisy" traffic?
   a) firewall
   b) bridge
   c) border gateway
   d) hub

Answer: c

7) Not getting a response to an echo request (ping) means
   a) you aren't communicating
   b) everything is normal
   c) your application is corrupted
   d) either you aren't communicating or your request is being denied (use arp–a to see if your ping made an entry in the arp table)

Answer: d

8) Through its masquerading rule, linux ipchains can provide
   a) a dynamic many-to-one translation of internal hosts communicating to the Internet
   b) a static many-to-one translation of internal hosts communicating to the Internet
   c) a one-to-one translation of internal hosts communicating to the Internet
   d) a many-to-many translation of internal hosts communicating to the Internet

Answer: a

9) IPChains are
   a) a list of IP addresses that can be applied to firewall policy
   b) a firewall ruleset manipulation tool available in linux kernels 2.2.x and above
   c) the output list from a DNS look up
   d) a datagram packet frame

Answer: b

10) VPN stands for
   a) Virtual private network
   b) verified path network
   c) vertical proxy net
   d) very promiscuous node

Answer: a

Exam questions 3.3 Defense In-Depth

1) Border routers are ideally
   a) the last line of defense against attackers
   b) used for initial screening before the firewall
   c) the only screening most networks need
   d) not used for any type of security purposes

Answer: b

2) When you have a router/firewall combination
   a) they should compliment each other by filtering different things
   b) they should mirror each other for redundancy
   c) they should both by default allow everything
   d) they should both by default deny everything

Answer: a

3) On a standard access list, the designation 198.112.12.0 0.0.255.255 means
   a) permit or deny anything that starts with 198.112.12
   b) permit or deny anything that starts with 192.112
   c) permit or deny only 198.112.12.0
   d) permit or deny anything that ends with 12.0

Answer: b

4) "access list 99 permit 0.0.0.0 255.255.255.255" can also be expressed as
   a) access list 99 permit 255.255.255.255 0.0.0.0
   b) access list 99 permit host 0.0.0.0
   c) access list 99 permit any
   d) can only be expressed one way

Answer: c

5) Which is **not** a type of Cisco ACL?
   a) standard
   b) expanded
   c) extended
   d) reflexive

Answer: b

6) A standard ACL is
   a) slow and not very useful
   b) slow, but simple to use
   c) allows complex comparisons
   d) fast, but offers limited control

Answer: d

7) When you first install a firewall it is best to
   a) start it with the defaults, then change things as you learn how it works
   b) have the vendor pre-configure it for you
   c) clear all the defaults, then open up only what your security policy allows
   d) add as many rules as possible

Answer: c

8) Which is **not** a part of recommended DNS security?
   a) split internal and external DNS
   b) use ACL to limit zone transfers
   c) logging
   d) deny all traffic

Answer: d

9) The choice of os installed on your internal hosts has what effect on their security?
   a) none – all security is taken care of by perimeter defenses
   b) very little, since all operating systems are subject to the same threats
   c) an important consideration, since some require no authentication, while others have varying degrees of access control
   d) most critical – the entire network is dependent on the internal host's abilities to protect themselves

Answer: c

10) To secure your network you need to
    a) install security layers that execute your policy, each layer configured as if the other layers will fail
    b) only install and properly configure a firewall
    c) decide whether you want to secure with a firewall or secure your hosts, then do it very well
    d) create a tight security policy

Answer: a

Marilyn Morris
San Jose Track 3 Practical Assignments

Practical Assignment #1 Egress Filtering

The purpose of egress filtering is to control the traffic leaving your network. While it is more common to focus defenses on traffic entering your network, administrators are becoming aware of spoofing and the possibility of being involuntary participants in Denial of Service attacks.

Case in point: an attacker crafts a packet with a false source IP address – the address of a site he wishes to attack. He may send a UDP echo request (ping) to the broadcast addresses of several large networks. Every machine on those networks will flood the victim with replies, causing a Denial of Service. If the administrator of the malicious user's site (or the site that was compromised) had done egress filtering, the attack would have been stopped near the source.

To stop spoofing from your site, only allow traffic out of your network that has a source address that is part of your legal address space. You can do this by applying a filter; filtering can be done on firewalls, routers and hosts, but is typically done on all of your border routers. Generically, a filter works like this:

Permit all my site's valid IP addresses outbound
Deny anything else outbound

(The general rule of routers and firewalls is that the packet will be compared to each rule starting with the first; it will move to the next rule in sequence until it finds a match, then it will apply that rule. The last rule should be the default rule – usually either a permit or deny of anything that didn't match the specific rules.)

If your legal address space was 198.112.20.0, on a Cisco router, you would create a filter that looks like this:

```
interface ethernet 0
ip address 198.112.20.1 255.255.255.0
ip access-group 10 in

access-list 10 permit ip 198.112.20.0 0.0.0.255
access-list 10 deny ip any log
```

The access list 10 is applied inbound to the interface facing your internal network. This is so it will intercept and discard the denied packets before they enter the router from your network, thus saving routing resources. A packet with a source IP in which the first three octets were 198.112.20, fourth octet anything, would be permitted to pass into the router and out the other side to the Internet. The second line drops any packets that don't match the previous rule(s) and also logs anything that was dropped; this is a very good idea.

To test your filter(s), you can simply craft a packet with an invalid IP address by temporarily changing your host's IP address to one that is not legitimate for your network, then sending the packet. If everything is working, the packet will be dropped, but the incident will be logged.

Egress filtering done this way will not stress your routers, and will make you a good Internet neighbor.

Sources: SANS "Help Defeat Denial of Service Attacks: Step-by-Step"
SANS GIAC "Resisting the Effects of Distributed Denial of Service Attacks"

Marilyn Morris
San Jose Track 3 Practical Assignments

Practical Assignment #2 – Firewall Policy Violations

The source of these logs is www.sans.org. Some are from the GIAC detects page, and some from the IDS practicals (which were very informative and knowledge expanding for me!)

Rule:	Source	Destination	Service	Action	Track
	<trusted IP's>	DNS server	domain – TCP	accept	no

(This policy rule blocks unauthorized zone transfers via the default deny all rule at the end of the access list; it is in effect saying "if you are trying to access the DNS—TCP service and you don't match the source IP, you will not qualify, therefore not be accepted.")

Log #1 shows a DNS scan being denied, probably by an ACL rule denying requests to destination port 53 from any source that was not listed/authorized. This is a port 53 UDP connection, not TCP and rarely blocked, so it could also be an intrusion detection system that recognized a known attack signature and denied the connection. These scans can be used to gather information about your internal network so hackers can narrow down their probes.

Apr 12 15:21:08 rt0 11984: 4d18h: %SEC-6-IPACCESSLOGP: list 102 denied udp 210.244.51.20(912) -> secondary.external.dns(53), 1 packet
Apr 12 15:26:57 rt0 11992: 4d18h: %SEC-6-IPACCESSLOGP: list 102 denied udp 210.244.51.20(910) -> primary.external.dns(53), 11 packets
Apr 12 15:41:36 rt0 12019: 4d18h: %SEC-6-IPACCESSLOGP: list 102 denied udp 210.244.51.20(743) -> primary.external.dns(53), 1 packet
Apr 12 15:41:40 rt0 12020: 4d18h: %SEC-6-IPACCESSLOGP: list 102 denied udp 210.244.51.20(745) -> secondary.external.dns(53), 1 packet
Apr 12 15:46:58 rt0 12028: 4d18h: %SEC-6-IPACCESSLOGP: list 102 denied udp 210.244.51.20(745) -> secondary.external.dns(53), 11 packets

Field definitions:
Apr 12 15:46:58 [timestamp] rt0 [host name] : %SEC-6-IPACCESSLOGP: list 102 [ACL list applied] denied [action] udp [transport protocol] 210.244.51.20(745) [source address + port] -> secondary.external.dns(53) [destination address + port]

Rule:	Source	Destination	Service	Action	Track
	Any	sendmail	smtp	accept	no

(This policy rule inversely denies any smtp requests to hosts other than the sendmail server.)

Log #2 shows a scan for responsive hosts on port 25 (mail). If a listening port is found, it will probably attempt relaying – this is an exploit used by SPAMers. All non-essential services on hosts should be turned off; if they are essential, they should be hardened with the latest patches and os upgrades. This connection could have been denied by a firewall rule, or if it is an active smtp port, again, it could have been denied by an IDS detecting a known signature.

Apr 12 00:27:02 rt0 9812: 4d03h: %SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.4.223(1563) -> external.smtp.server(25), 1 packet
Apr 12 00:27:51 rt0 9813: 4d03h: %SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.4.223(1936) -> external.smtp2.server(25), 1 packet
Apr 12 00:32:06 rt0 9817: 4d03h: %SEC-6-IPACCESSLOGP: list 102 denied tcp 192.168.4.223(1563) -> external.smtp.server(25), 3 packets

Field definitions:
Apr 12 00:33:06 [timestamp] rt0 [hostname] 9819: 4d03h: %SEC-6-IPACCESSLOGP: list 102[ACL list applied] denied [action] tcp[transport protocol] 192.168.4.223(1936) [source address + port] -> external.smtp2.server(25) [destination address + port], 3 packets

---

Rule:	Source	Destination	Service	Action	Track
	External	any	icmp echo request	drop	yes

Log #3a shows fragmented icmp echo request. It is unlikely that icmp traffic would ever need to be fragmented, and so should never be allowed into the network if fragmented. The requests are coming in at a very high speed and the last fragment never arrives for any fragment ID, so the purpose is probably to cause a denial of service by overwhelming the proxy server.

```
03:16:01.508947 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50698:1480@0+)
03:16:01.517820 tif.inria.fr > proxy.mysite.com: (frag 50698:1480@1480+)
03:16:01.525788 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50699:1480@0+)
03:16:01.525788 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50699:1480@0+)
03:16:01.533775 tif.inria.fr > proxy.mysite.com: (frag 50699:1480@1480+)
03:16:01.547976 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50700:1480@0+)
03:16:01.547976 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50700:1480@0+)
03:16:01.555945 tif.inria.fr > proxy.mysite.com: (frag 50700:1480@1480+)
03:16:01.567608 tif.inria.fr > proxy.mysite.com: (frag 50700:1480@2960+)
03:16:01.575567 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50701:1480@0+)
03:16:01.575567 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50701:1480@0+)
03:16:01.583547 tif.inria.fr > proxy.mysite.com: (frag 50701:1480@1480+)
03:16:01.592646 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50702:1480@0+)
03:16:01.592646 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50702:1480@0+)
03:16:02.500846 tif.inria.fr > proxy.mysite.com: icmp: echo request (frag
50711:1480@0+)
```

```
Field Definitions:
03:16:02.500846 [timestamp] tif.inria.fr [source ip] > proxy.mysite.com [dest
ip]: icmp: echo request [protocol and type] (frag 50711 [frag ID]:1480@0 [bytes
sent in this packet @ placement position] + [more packets coming flag])
```

Log #3b is a tcpdump showing an icmp echo request (ping) coming from outside. These can be initial reconnaissance scans looking for live hosts, or part of an attack on a spoofed source host. The ttl is suspicious. It is best to deny ping requests and replies from outside your network.

15:46:26.764770 195.256.224.125 > 130.256.0.9: icmp: echo request [ttl 1]
15:47:50.638015 195.256.224.125 > 130.256.0.9: icmp: echo request [ttl 1]
15:49:14.323237 195.256.224.125 > 130.256.0.9: icmp: echo request [ttl 1]
15:50:38.108791 195.256.224.125 > 130.256.0.9: icmp: echo request [ttl 1]

Field definitions:
15:52:02.114761 [timestamp] 195.256.224.125 [source IP] > 130.256.0.9: [dest IP]icmp: echo request [protocol and type] [ttl 1] [time-to-live is 1 hop]

Rule:	Source	Destination	Service	Action	Track
	Internal address range Originating from the Internet	any	any	drop	yes

(This rule drops spoofed traffic masquerading as an internal host.)

Log #4 shows a DoS attack generated by spoofing the source address and making it the same as the destination (victim); this has a very nasty effect on NT platforms. This one is easy to filter by denying all incoming traffic with source addresses of your internal network

Time stamp-----| source ip------| port destination ip-| port-| protocol type

12:35:26.916369 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.916566 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.916682 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.916796 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.916910 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.917023 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]
12:35:26.917137 192.168.38.110.135 > 192.168.38.110.135: udp 46 [tos 0x3,ECT,CE]

Rule:	Source	Destination	Service	Action	Track
	Any	any	NBT	reject	no

(NetBIOS traffic is noisy broadcasts which would fill the logs rapidly if tracked.)

Log #5 is really two different logs showing a NetBIOS port scan for unprotected shares; this is are potentially serious security hole on Windows systems, but also SMB shares (UNIX) with poorly configured access control. I thought these were both from Snort scanners, but the output is slightly different. Steps should be taken to protect any necessary shares when setting them up. Access to port 137 should be blocked at the firewall.

Apr 26 21:48:04 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.100:137
Apr 26 21:48:22 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.102:137

Apr 26 21:48:31 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.103:137
Apr 26 21:48:40 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.104:137
Apr 26 21:48:49 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.105:137
Apr 26 21:49:07 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.107:137
Apr 26 21:49:34 zion snort[25745]: SMB Name Wildcard:
200.4.12.12:137 -> MY.NET.175.110:137

Field definitions:
Apr 26 21:51:59 [Timestamp] zion [hostname] snort[25745]: SMB Name Wildcard: [Type of attack]
200.4.12.12:137 [source ip + port]- -> MY.NET.175.125:137 [dest ip + port]

Another detect, same thing -- from @home cable modem.

```
04/04-08:05:08.874585 24.66.210.139:137 -> my.host.ip:137
UDP TTL:110 TOS:0x0 ID:7046

04/04-08:05:10.353907 24.66.210.139:137 -> my.host.ip:137
UDP TTL:111 TOS:0x0 ID:7302
```

Marilyn Morris
San Jose Track 3 Practical Assignments

Assignment #3 – Defense in Depth Architecture

Design A: In this design, the client has an internal network that is connected to the Internet with a firewall and router between them. The client also has an extranet where they maintain a large database of product inventories pricing, and production schedules, and order status. There are a large number of customers and sales agents looking at this information daily. At this time, orders and payments are not processed through here. The client wishes to keep this separate from his trusted network. The extranet is connected to the Internet via a separate router and firewall.

The border routers are configured to "allow all" after these rules are applied:

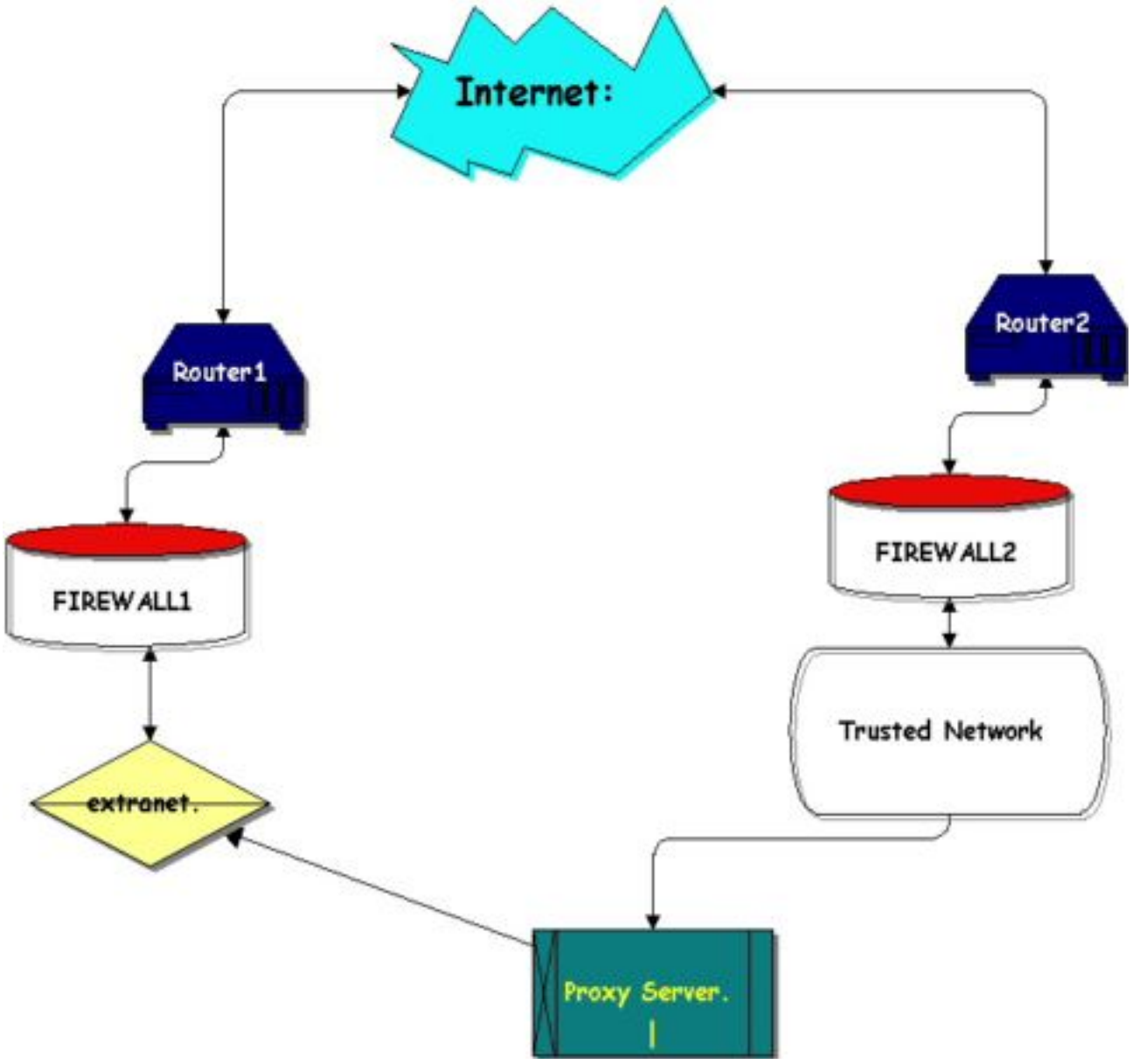
no ip source-routing	(source routing can be used to by-pass ACL rules.)
no ip direct-broadcast	(will prevent directed broadcasts from causing denial of service)
no icmp-unreachable	(disables sending notification messages if a service is blocked.)

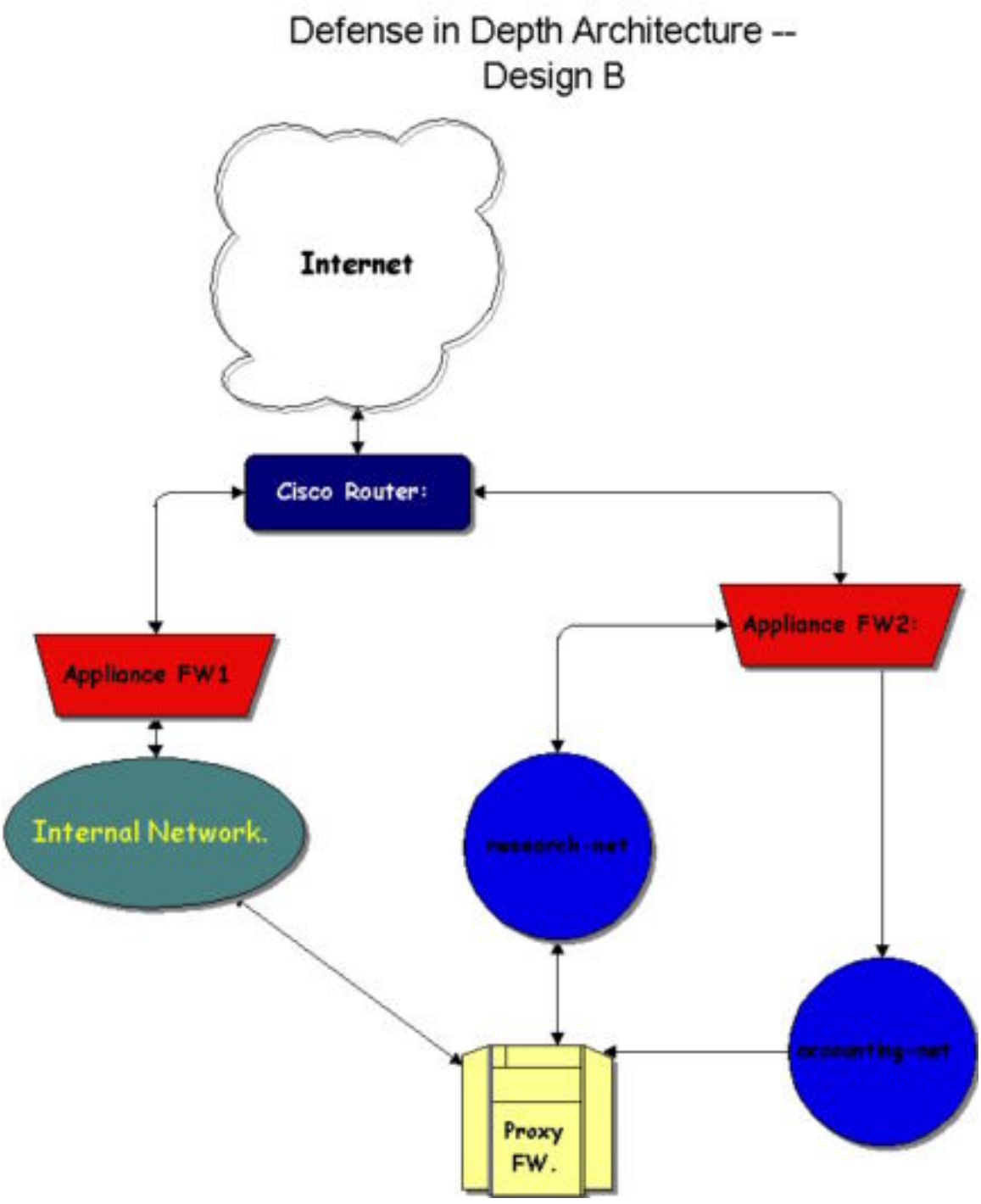
And a filter is applied that drops packets claiming to have the same source IP addresses as the network they are entering.

The firewall for the both networks allow inbound only the services necessary like http and mail. Most outbound traffic is allowed; non-legitimate source addresses on packets going out to the Internet are dropped and logged on both firewalls via an egress filter.

The extranet database is updated from the internal network via a one-way proxy server that only allows incoming from the internal network and sends updates out to the extranet.

See diagram on next page.





A proposed use of the equipment available is shown here: the two appliance firewalls are placed between the border router and the protected sub-nets. The confidential nature of the accounting and research groups are addressed by 1) having a different firewall between them and the Internet that can be configured to meet special needs, and 2) having a proxy server between them and the rest of the company to secure against inside breaches.

Marilyn Morris
San Jose Firewalls and Perimeter Defense Tract Practical Assignments

Self Test

The Challenge: Your client has an existing network and has recently connected to an ISP and is starting to use the Internet. They are novices in the security requirements of exposing themselves to Internet's opportunities and risks. They want you to assess their situation and recommend what should be done in an order of importance so that they can get as much as they can afford and be sure they are having the most impact. This will provide a scalable plan for the future, and an awareness of issues and perils as they expand their use of the Internet.

Response:

1) Give them an overview of the threats that exist when open to the Internet, and strongly encourage them to do a risk analysis. Many clearly written white papers and books are available to help them understand the choices they can make – for example, they made decide to narrow their access until they can afford the amount of protection they need.
2) Select and install virus protection software on all hosts; instruct them on how it works and how to update it.
3) Require a security policy be developed – help them if they need it.
4) Map their existing network and find out as much about future plans as they know.
5) Show them ways they can filter out some of the traffic coming through the router; introduce them to ACLs and the most useful rules including:
   No ip source-routing
   No ip direct-broadcast
   No icmp-echo
6) Specify a good, but least complicated firewall; document suggested rules and be prepared to configure it for them. Explain that defaults should be cleared from the initial firewall settings, and a default rule of "deny all" will be applied after only authorized traffic and services are allowed. Include an egress filter that will drop and log outgoing traffic with spoofed source addresses.
7) Recommend network intrusion detection systems, and host intrusion detection systems for at least the critical servers.
8) Provide a diagram of what their ideally-protected network would look like: