Firewalls & Network Monitoring

UNIVERSITY OF OREGON

NSRC
Network Startup Resource Center

Contradiction of requirements

- Need to monitor services
- Need to protect network services

- Remember Basic Security Principles
  - Confidentiality
  - Integrity
  - Availability

If you don't monitor services, availability suffers

Our Basic Premise

We need to allow access to:

- Terminal (SSH) or port 22
- Web and Web-SSL or ports 80 and 443
- DNS or port 53 via UDP and TCP
- Verify availability of server, router or switch, i.e. ping (ICMP type 8)

Don’t block Ping

Please!

“It’s an essential tool to verify the health and availability of your network, servers and services. Without *ping* it is very difficult to solve problems and you often cannot ask for help from others.”

More formally what we mean is…

Don't block all forms of ICMP. Allow ICMP Echo Request Type 8 (OS firewalls).

If you use ACLs on your routers consider allowing outbound and/or inbound:

- ICMP *unreachable*
- ICMP *Time exceeded*
- ICMP *Echo reply*

In addition, for path MTU discovery issues:

- ICMP *Parameter problem*
- ICMP *Source quench*

Some examples: IPTables

```
iptables -F
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp   --dport 22 -j ACCEPT
iptables -A INPUT -p tcp   --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -A INPUT -p udp  --dport 53 -j ACCEPT
iptables -A INPUT -p tcp   --dport 53 -j ACCEPT
iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
iptables -A INPUT -j REJECT
iptables -A FORWARD -j REJECT
```

Some Examples: Cisco ACLs

```
access-list 101 remark [<Allows PING and Traceroute>]
access-list 101 permit icmp any any unreachable
access-list 101 permit icmp any any time-exceeded
access-list 101 permit icmp any any echo-reply
access-list 101 permit icmp any any parameter-problem
access-list 101 permit icmp any any source-quench
!
interface Ethernet1
ip access-group 101 in
```

Etc…

Some examples: Cisco ASA

```
interface Ethernet0/0
nameif outside
 security-level 0
 ip address 60.25.45.10 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
 ip address 10.0.0.250 255.255.255.0
!
access-list IN extended permit tcp any host 60.25.45.10 eq 22
access-list IN extended permit tcp any host 60.25.45.10 eq 80
access-list IN extended permit tcp any host 60.25.45.10 eq 443
access-list IN extended permit tcp any host 60.25.45.10 eq 53
access-list IN extended permit udp any host 60.25.45.10 eq 53
!
static (inside,outside) 60.25.45.10  10.0.0.4 netmask 255.255.255.255 0 0
access-group IN in interface outside
```

In summary

- Without access you cannot monitor
- Without monitoring you cannot know state

- Without knowing state you cannot:
  - Guarrantee availability of services
  - Efficiently diagnose and resolve failures