CSET 2200

Firewalls

Security so far

- Routers have ACL
- Can filter packets
- Often performed in hardware

Firewalls

- Perform similar filtering to Router
- Track state
- Purpose built to inspect traffic
- Software filtering normally

Differences

- For basic purposes not much difference
- Firewalls track state
- Firewalls have richer configuration syntax
- Slower since software

Cisco Firewalls

- Original ones called Pix
- Now ASA (Adaptive Security Appliance)
- Come in many models

ASA

- Based on Intel chips
- Run custom PIX/ASA OS
- Models range from small soho to multi-gb solutions

Configuration

- Somewhat like IOS
- A good number of differences
- Has more features to configure ACLs

Interfaces

- Interfaces get names also called zones
- Naming convention is somewhat different
- Normally a dedicated management interface

Security Zones

- Zones are names and applied to interfaces
- Each zone has a security level
- More secure (Higher value) can talk to less secure
- Less secure requres explicit ACL
- Traffic on same zone inter/intra interface can be defined

ACL Configuration

- New ASA supports objects and groups
- Let you name IPs
- Also lets you create groups
- Makes configuration easier to read

ACL Example

```
object-group network CNWR_trusted
 network-object 64.254.140.0 255.255.255.224
 network-object 64.254.134.0 255.255.255.0
 network-object 72.240.52.32 255.255.255.240
access-list acl_out extended permit tcp any host cnwr_exch
access-list acl_out extended permit tcp 72.240.52.32 255.25
access-list acl_out extended permit tcp host 75.101.140.73
access-list acl_out extended permit tcp host 72.240.50.75 h
access-list acl_out extended permit tcp host 64.254.140.98
access-list acl_out extended permit udp object-group CNWR_t
access-list acl_out extended permit udp object-group CNWR_t
access-list acl_out extended permit tcp object-group CNWR_t
```

NAT and the ASA

- Configuration Style has varied over the years
- Current versions configure on objects
- Configure NAT-0 and Pool/PAT in after statements

NAT Example

```
object network IP-10.100.8.72
 nat (inside,iisdmz) static 192.168.98.204
nat (inside,outside) after-auto source dynamic inside_nat_
nat (norisdmz,outside) after-auto source dynamic norisdmz_
```

VPN (Virtual Private Network)

- ASA and Routers support VPN
- Routers need the right license
- VPN creates a virtual tunnel between networks
- Traffic usually encrypted

Inspections

- ASA supports deep packet inspection
- Ensures right traffic passing on a port
- Example - HTTP over the DNS ports

Questions

Demonstration

Questions

Next time - IPv6