Cisco Zone Based Firewall

Grundprinzip

- Traffic innerhalb einer Zone: erlaubt
- Traffic zur `self`-Zone (IP-Adressen der Routerschnittstellen): erlaubt
- Traffic über Schnittstelle, die in keiner Zone ist: verboten
- Traffic von einer Zone zur anderen: standardmässig verboten, kann durch Policy erlaubt werden
- `inspect` (Stateful inspection): allow returning traffic

Konfiguration

1. Zone erstellen

```
ROUTER(config)# zone security ZONE
```

2. Schnittstelle einer Zone zuweisen

```
ROUTER(config-if)# zone-member security ZONE
```

3. Class Map (welcher Traffic?) [match-all | match-any]

a) über Protocol

```
ROUTER(config)# class-map type inspect ICMP-CMAP
ROUTER(config-cmap)# match protocol icmp

ROUTER(config)# class-map type inspect match-any WEB-CMAP
ROUTER(config-cmap)# match protocol http
ROUTER(config-cmap)# match protocol https
```

b) über ACL

```
ROUTER(config)# ip access-list extended VPN-ACL
ROUTER(config-ext-nacl)# permit udp any any eq isakmp
ROUTER(config-ext-nacl)# permit ahp any any
ROUTER(config-ext-nacl)# permit esp any any
ROUTER(config-ext-nacl)# permit udp any any eq non500-isakmp

ROUTER(config)# class-map type inspect match-any VPN-CMAP
ROUTER(ROUTER(config-cmap)# match access-group name VPN-ACL
```

4. Policy Map (was darf Traffic?) [inspect | pass | drop]

```
ROUTER(config)# policy-map type inspect ZONE1-ZONE2-PMAP
ROUTER(config-pmap)# class type inspect ICMP-CMAP
ROUTER(config-pmap-c)# inspect
ROUTER(config-pmap-c)# exit
ROUTER(config-pmap)# class type inspect WEB-CMAP
ROUTER(config-pmap-c)# inspect
```

5. Zone Pair konfigurieren und Policy zuweisen (wo gilt die Policy?)

```
ROUTER(config)# zone-pair security ZONE1-TO-ZONE2 source ZONE1 destination ZONE2
ROUTER(config-sec-zone-pair)# service-policy type inspect ZONE1-ZONE2-PMAP
```

Diagnose

```
ROUTER# show zone security                                  # Zonen und Schnittstellen
ROUTER# show zone-pair security                             # Zonenpaare und Policies
ROUTER# show policy-map type inspect zone-pair sessions     # offene Sessions
```