Cisco Security und Layer 2

ISPA Academy

29. September 2016

Michael Kafka (DeepSec GmbH)

Cisco Instructor

Themen

Data Plane, Control Plane, Management Plane

Risk Mitigation Management Access

Layer 2 Risk Mitigation

Layer 2 Encryption

3 Planes:
Data, Control, Management

Separate Konfiguration:

Data Plane:

- User Traffic, Routing, Payload

Control Plane:

- Dynamische Kontrolle, OSPF, ARP etc.

Management Plane:

- Konfiguration, Reporting, Monitoring

Data Plane

Risk Mitigation:

- Access-Lists (eingeschränkte Möglichkeiten)
- Stateful Firewall
- Zone Based Firewall
- QoS Parameter: Policing

Data Plane ACL

Simple Packet Filter

- Can be bypassed
- Fragmentation Attacken

```
access-list 101 deny icmp any any
access-list 101 permit ip any any
interface <interface>
ip access-group 101 {in|out}
```

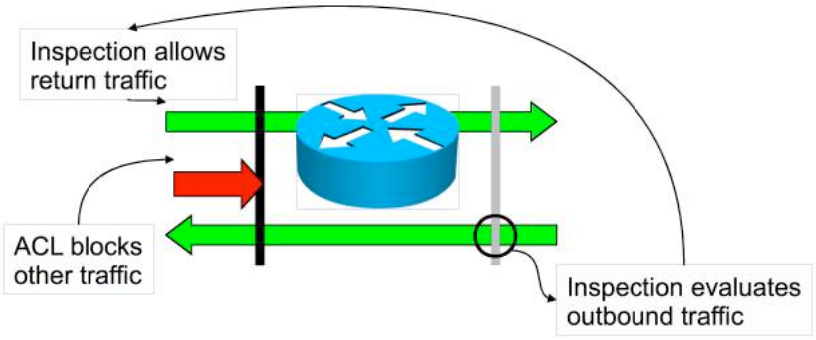
Data Plane Stateful Firewall

"Classical Firewall" CBAC

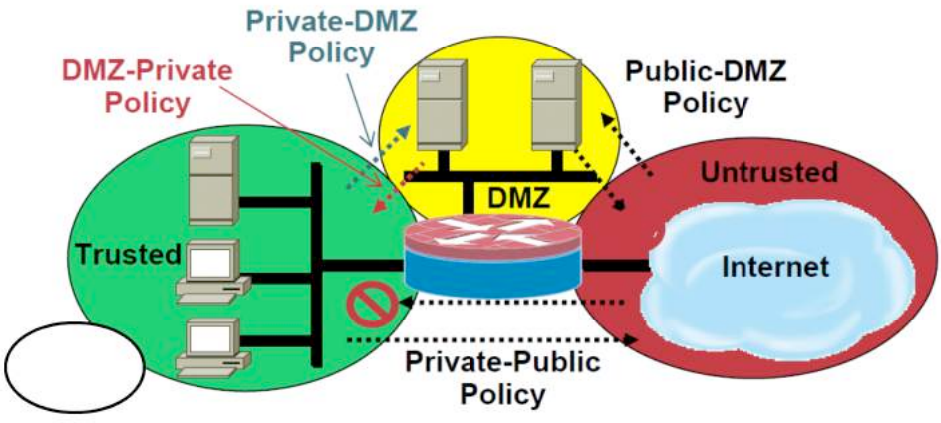
- Erlaubt gültigen Return-Traffic
- Komplexe Konfiguration (Fehlermöglichkeit)

```
access-list 101 deny ip any any
ip inspect name mysite ftp
ip inspect name mysite smtp
ip inspect name mysite tcp
interface Ethernet0
 ip inspect mysite in
interface Ethernet1
 access-group 101 in
```

Data Plane Stateful Firewall



Data Plane Zone Based Firewall



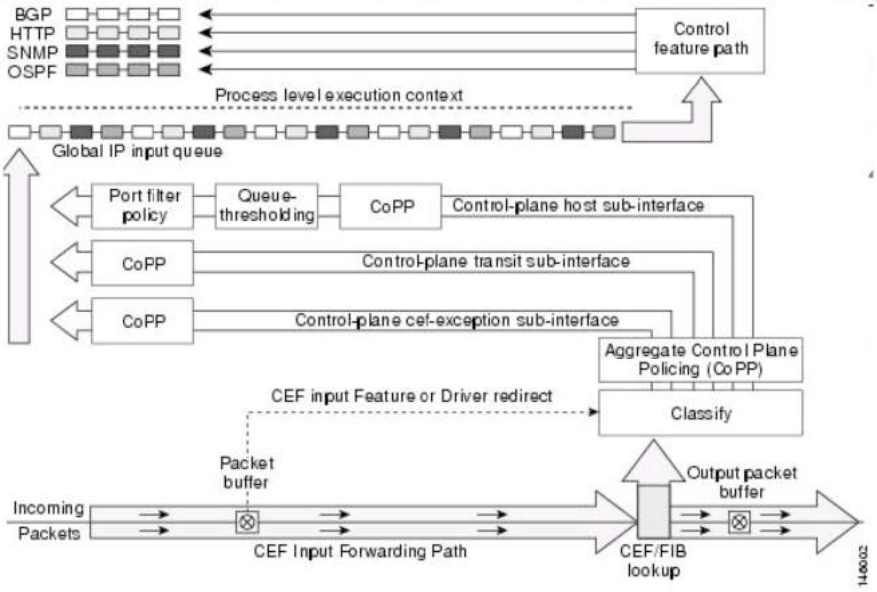
Data Plane Zone Based Firewall

Klare Konfiguration:

```
zone security z1
 description finance department networks
zone security z2
 description engineering services network
zone-pair security zp source z1 destination z2
 service-policy type inspect p1

interface ethernet0
 zone-member security z1
interface ethernet0
 zone-member security z2
```

Control Plane



Control Plane Protection

Erweiterung zu Control Plane Policing :

- Port Filter

```
Router(config)# class-map type port-filter pf-class
Router(config-cmap)# match closed-ports
Router(config)# policy-map type port-filter policy
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop

Router(config)# control-plane host
Router(config-cp)# service-policy type port-filter input policy
```

Control Plane Protection

Erweiterung zu Control Plane Policing :

- Queue Threshold (Bsp. SNMP: NMAP!)

```
Router(config)# class-map type queue-threshold qt-class
Router(config-cmap)# match protocol snmp
Router(config)# policy-map type queue-threshold policy
Router(config-pmap)# class qt-class
Router(config-pmap-c)# queue-limit 50

Router(config)# control-plane host
Router(config-cp)# service-pol type queue-thresh input policy
```

Control Plane (Weitere Features)

ICMP und ARP

- Kontrolle über akzeptierte ICMPs
- Kontrolle über generierte ICMPs
- Statische ARP

```
ip icmp rate-limit unreachable …
[no] ip icmp redirect
[no] ip mask-reply
[no] ip unreachables

arp {ip-address | vrf vrf-name} hardware-address encap-type
```

Management Access

Secure Managament mit Verschlüsselung

- Leider an Crypto-Lizenz gebunden ("K9")
- SSH (ohne Zertifikate!)
- SSL (Self-Signed oder CA)
- SNMPv3
- HTTPS (Für Filetransfer)
- Weitere über IPsec

Management Access

Access-Listen für Dienste:

- Remote Console (z.B: Telnet, SSH)
- SNMP zugriff

```
access-list 1 permit 10.0.9.0 255.255.255.0
Access-list 2 permit host 10.0.9.12

line vty 0 15
 transport input ssh
 access-class 1

snmp-server community comaccess ro 2
```

Management Access
Role Based Command Line


```
Router#enable view
Password: Curium2008
Router#configure terminal
router(config)#parser view NetOps
router(config-view)#secret 0 hardtocrackpw
router(config-view)#commands exec include ping
router(config-view)#commands exec include all show
router(config-view)#commands exec include telnet
router(config-view)#commands exec include traceroute
router(config-view)#commands exec include write
router(config-view)#commands exec include configure
router(config-view)#commands configure include access-list
router(config-view)#commands configure include all interface
router(config-view)#commands configure include all ip

router#enable view NetOps   …(enter password for this view)
```

Routing Protokolle

Für Alle relevanten Routing Protokolle

- Authentisierung
- Filter

```
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.16.64.0 0.0.0.255 area 0
 area 0 authentication message-digest
interface Serial0
 ip address 192.16.64.2 255.255.255.0
 ip ospf message-digest-key 1 md5 [ospf-auth-key]
```

Layer 2 Risk Mitigation

Layer features hautpsächlich auf Switches:

- PVLANs and ACLs
- Port security
- DHCP snooping
- Dynamic ARP Inspection
- IP Source Guard

PVLANs und VLAN ACLs

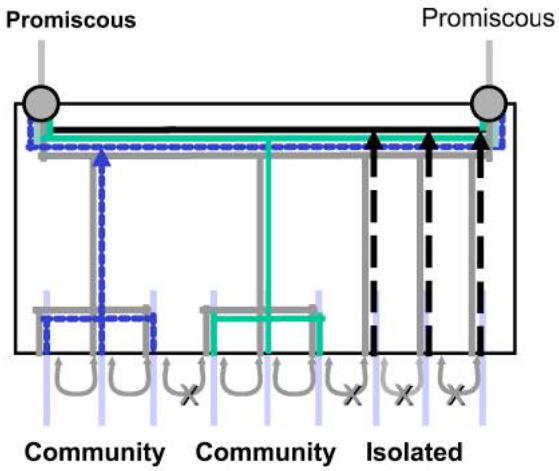
Private VLANs:

- Limitieren Broadcast und Forwarding
- Member und Promiscous Port
- Member sendet nur an Promiscous
- Member empfängt nur von Promiscous

VLAN ACLS (auf manchen Plattformen)

- Wie Router ACLs
- Filtern Pakete auf VLAN, nicht auf Port Ebene

PVLANs Details



Port Security

Hauptsächlich für MAC-Limitierung

- Limitiert active MAC-Adressen per Switch Port
- Definiert "Violate Action":
  - Shut down
  - Restrict
  - Protect

Mitigation für:

- Mac Flooding
- Manche DoS Floods

DHCP Snooping

Lernt MAC/IP Binding durch trusted DHCP

- Grundlage für weitere Filter
- DHCP Server als trusted konfiguriert
- Baut ARP-Table
- Filter untrusted DHCP-Replies

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 90
Switch(config)#interface FastEthernet 0/5
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping limit rate 300
```

Dynamic ARP Inspection

Inspiziert ARP-Replies

- Vergleich mit trusted DHCP-Table
- Drop nonconforming

```
Switch(config)#ip arp inspection vlan 10
Switch(config)#interface fastethernet 3/3
Switch(config-if)#ip arp inspection trust
Switch(config-if)#switchport mode trunk
Switch(config-if)#ip arp inspection limit rate 100
```

IP Source Guard

Verifiziert IP Source gegen trusted DHCP-Table

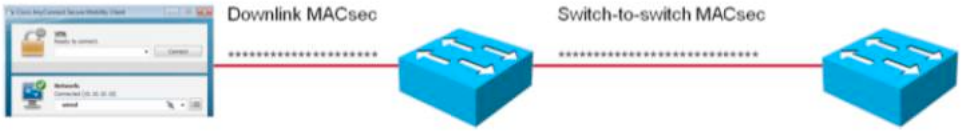
- Schutz gegen IP Spoofing

```
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 100
Switch(config)#interface fastethernet 0/1
Switch(config-if)#ip verify source port-security
```

MAC-sec 802-Encryption

IEEE-Standard

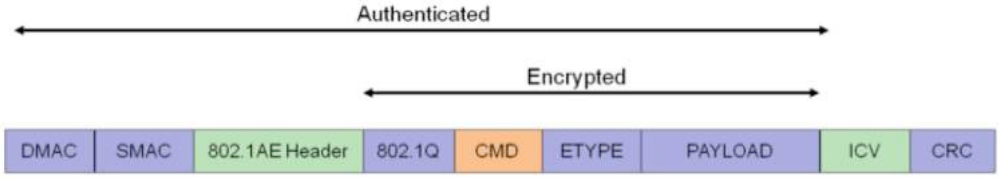
- Verschlüsselt auf Layer 2 (802.1AE)
- Handelt AES-Keys aus
- Uplink/Downlink Varianten
- Uplink (Switch/Switch): eigenes Protokoll
- Downlink: Extension zu 802.1X



MAC-sec Kryptographie

Verwendet NG-Crypto

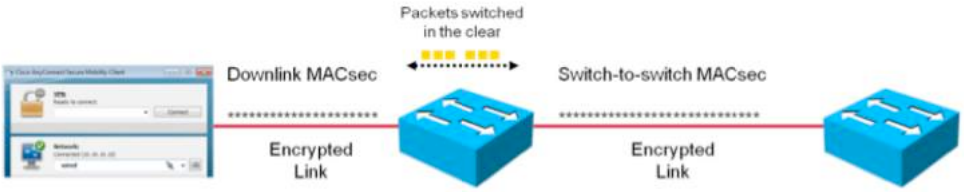
- AES128 gcm
- Confidentiality
- Integrity
- Replay Protection



MAC-sec Hop by Hop

Transparent für Endgeräte

- Hop by Hop Encryption
- "Bump in the Wire"
- Switching im Klartext
- QoS etc gewährleistet



MAC-sec Downlink

Per Interface

- Wird am Switchport aktiviert
- Benötigt einen MAC-sec Client

```
HQ-Sw(config)#
interface GigabitEthernet0/1
macsec
mka default-policy
authentication linksec policy should-secure
```

MACsec Uplink (Switch/Switch)

Konfigration am Interface

- Initiert SAP
- Definiert Crypto-Policies
- Fall-Back Policies erlaubt

```
Router# configure terminal
Router(config)# interface gi 2/1
Router(config-if)# cts manual
Router(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm null no-encap
```

Fragen/Diskussion

Vielen Dank!