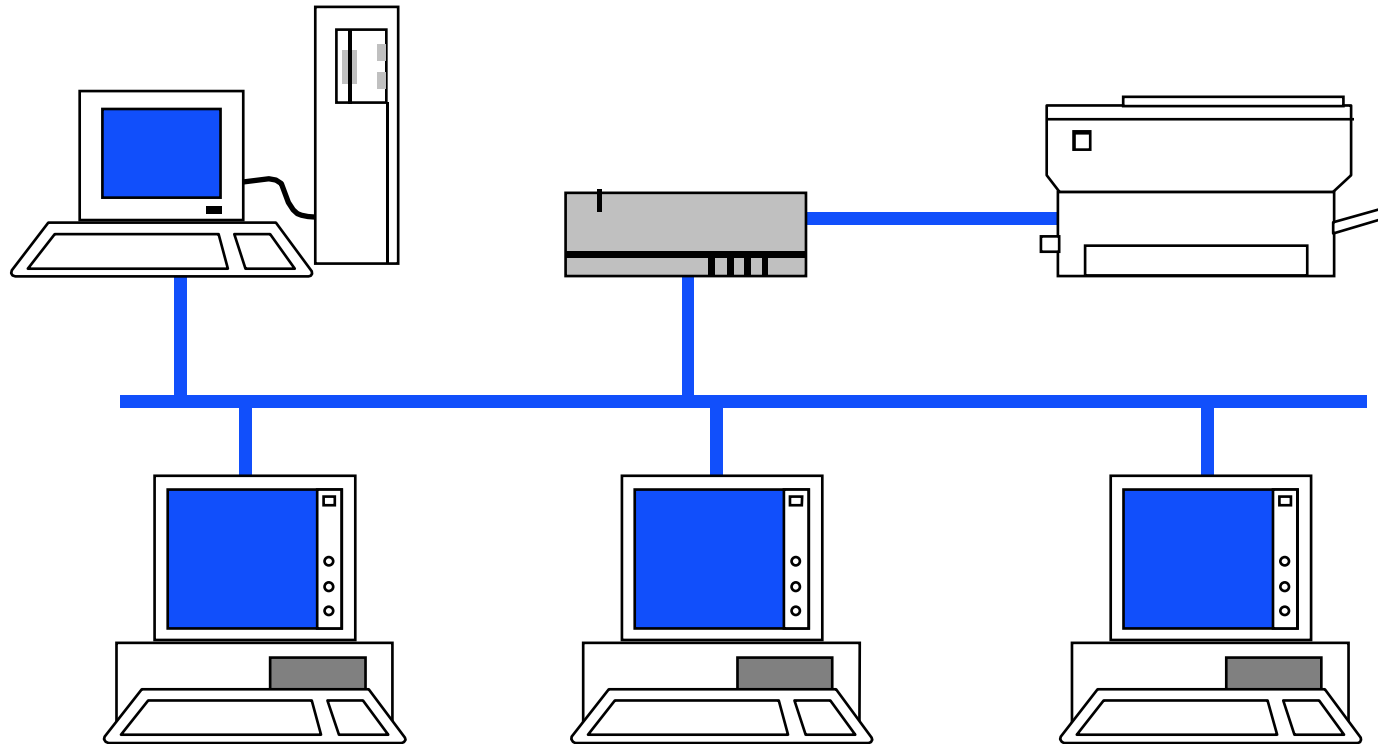


Cisco ASA - Einführung

Mag. Dr. Klaus Coufal



Übersicht

1. ASA – Was ist das?
2. Betriebsmodi
3. Commandline - Bedienung
4. Schnittstellen
5. ASA-OS (Finesse -> Linux)

1. ASA – Was ist das?

- Advanced Security Appliance
- ASA steht für eine Familie von Stateful Inspection Firewalls der Firma Cisco
- Kein Router!
- NAT, PAT und DHCP-Support
- Automatische Konfiguration der Sicherheit über Sicherheitsstufen.

2. Betriebsmodi

- User Mode (Kaum Befehle)
 ↓(enable) ↑(disable)
- Privileged Mode (Alle Befehle außer
 Konfiguration)
 ↓(configure terminal) ↑(exit)
- Configuration Mode (Alle Befehle)

3. Commandline - Bedienung

- Hilfe
- Abkürzungen
- Mehrseitige Ausgaben
- Kontrollzeichen

Hilfe




- Durch den Befehl „help“ oder das „?“ wird ein Hilfetext ausgegeben
- Ebenso bei einem Syntaxfehler
- Wie bei IOS kann die Hilfe auch für eine Subebene eines Befehls angefordert werden

Abkürzungen














- Alle Befehle können soweit abgekürzt werden, bis sie noch eindeutig sind.
- 0 als IP-Adresse wird als 0.0.0.0 interpretiert.

Mehrseitige Ausgaben

Mehrseitige Ausgaben bleiben nach 24 Zeilen (einstellbar) stehen, dabei gelten folgende Steuerzeichen:

-  Nächste Zeile
-  Nächste Seite
-  Abbruch

Kontrollzeichen (Auszug)

-  Zeilenanfang
-  Zeilenende
-  Zeile löschen
-  Zeile wiederholen
-  oder  Ein Zeichen nach links
-  oder  Ein Zeichen nach rechts
-  oder  Vorige Zeile
-  oder  Nächste Zeile
-  oder BS Löscht ein Zeichen

4. Schnittstellen

- Je nach Modell sind verschiedene Ethernet-Netzwerkschnittstellen implementiert z.B.:
- ASA 5505 >2 (8*10/100 MBit/s Switch)
mit VLAN-Support)
- ...
- ASA 5585-X bis zu 10 (GBit/s)

5. ASA-OS 1

- Unterschiede zu IOS
- Wichtige Befehle
- Konfiguration ansehen, speichern, ...
- Allgemeine Konfigurationsbefehle
- Schnittstellenkonfiguration
- Translation Rules
- ACLs (Access Control Lists)

5. ASA-OS 2

- ASA als DHCP-Server
- VPN-Tunnel
- Management der ASA
 - Telnet
 - SSH
 - ASDM (ASA Secure Device Manager)
- Datum, Uhrzeit und ntp
- Logging

Unterschiede zu IOS

- Keine Sekundäre IP-Adressen
- In ACLs Subnetmasken statt Wildcards
- Kann kein DNS nutzen

Wichtige Befehle 1

- reload
- ping <name/ip>
- show <befehl>
 - show dhcpd bindings
 - ...
- clear <befehl>
 - clear arp

Wichtige Befehle 2

- `passwd <linepassword>`
 - Default: `cisco` (oder *Keines gesetzt*)
- `enable password <enablepassword>`
 - Default: *Keines gesetzt*

Konfiguration bearbeiten

- **show configuration** Anzeige der Startupkonf.
- **show running-config (write terminal)** Anzeige der laufenden Konfiguration
- **copy running-config startup-config (write memory)** Sichern der laufenden Konfiguration in das NVRAM
- **write erase** Löschen der Konfiguration
- **copy running-config tftp:[//<server>/<file>] (write net <ip>:<file>)** Kopieren der Konfiguration auf einen TFTP-Server

Allgemeine Konfigurationsbefehle

- hostname <Name>
- domain-name <dns-domain>
- crypto key generate rsa modulus <keylength>
 - z.B.: crypto key generate rsa mod 2048
- show crypto key mypubkey rsa
- crypto key zeroize rsa

Schnittstellenkonfiguration

- Interface auswählen
interface <interfaceID>
- Namen und Sicherheitsstufe vergeben
nameif <name>
security-level <perimeter>
- IP-Adresse zuordnen
ip address <ip> <mask>
oder
ip address dhcp [setroute]

Perimeter

- Wert zwischen 0 und 100
- 0 ist unsicher (Internet)
- 100 sicher (Intranet; nur für „inside“)
- 0 und 100 müssen existieren
- Schnittstellen mit dem selben Perimeterwert können keine Daten austauschen!

Perimeter-Bedeutung

- Je höher der Perimeterwert desto sicherer ist die Schnittstelle
- Ohne Regeln gilt:

Von einer Schnittstelle mit höherem Perimeterwert zu einer Schnittstelle mit niedrigerem Perimeterwert ist Alles erlaubt und umgekehrt gar nichts!

Schnittstellenkonfiguration - Beispiel

- interface vlan1
 - nameif outside
 - security-level 0
 - ip address dhcp setroute
- interface vlan2
 - nameif inside
 - security-level 100
 - ip address 192.168.1.1 255.255.255.0

Translation Rules

- Befehle zur Definition
 - nat
 - global
 - static
- Befehle zum Ansehen und Löschen der Translation Slots
 - show xlate
 - clear xlate

Translation – Kein NAT

- Identity NAT
 - nat (inside) 0 <net-ip> <mask>
 - NatID 0 steht für Identity NAT
 - Kein Zugriff von außen möglich
- Static NAT
 - static (inside, outside) <net-ip> <net-ip>
netmask <mask>
 - Externe und Interne IPs gleich

Translation – Static NAT

- Auch One-to-One-NAT genannt
 - static (inside, outside) <extern-net-IP>
<intern-net-IP> netmask <mask>
 - Auch für einen einzelnen Rechner möglich
(<mask>=255.255.255.255)

Translation – Dynamic NAT

- One-to-One NAT mit IP-Address-Pool
 - nat (inside) <nr>
 - global (outside) <nr> <start-IP> <end-IP>
netmask <mask>
 - <nr> ist zwischen 1 und $2^{32}-1$ und muß bei zusammengehörigen nat und global-Befehlen identisch sein.
 - Kein Zugriff von außen möglich

Translation - PAT

- Port-level multiplexed NAT
- Many-to-One-NAT
 - nat (inside) <nr> <net-IP> <mask>
 - global (outside) <nr> <IP-Address>
- Oder
 - nat (inside) <nr> <net-IP> <mask>
 - global (outside) <nr> interface

ACL – Grundlagen

- Abarbeitung von oben nach unten bis ein passender Eintrag gefunden wird (spätestens beim impliziten „deny ip any any“ am Ende)
- Eine ACL wird mit „access-group“ einer Schnittstelle zugeordnet
- Nur eine „incoming“ ACL pro Schnittstelle
- Nur eine „outgoing“ ACL pro Schnittstelle

ACL – Syntax

- `access-list <name|nr> permit|deny
<protocol> <source> <destination>
[<parameter>]`
 `access-list 3 permit icmp any any echo-reply`
 `access-list 7 permit tcp any any eq 22`
- `access-group <name|nr> { in | out }`
`interface <if-name>`

ACL – IP-Angaben

- <Netaddress> <Subnetmask>
192.168.0.0 255.255.255.0
- host <IP>
host 192.189.51.100
(=192.168.51.100 255.255.255.255)
- any
any (= 0.0.0.0 0.0.0.0)

ACL – Protokolle

- icmp
icmp <quelle> <ziel> [<teilprotokoll>]
- tcp
tcp <quelle> <ziel> [range <port1> <port2>]
- udp
udp <quelle> <ziel> [eq <portname|portnr>]
- ip
- ...

ACL – Beispiel 1

```
access-list zentral permit icmp any any echo-reply
access-list zentral permit icmp any any unreachable
access-list zentral permit icmp any any time-exceeded
access-list zentral permit tcp host 192.189.51.100 62.199.66.16
    255.255.255.240 eq 22
access-list zentral permit udp any host 62.199.66.23 eq 53
access-list zentral permit tcp any host 62.199.66.23 eq 53
access-list zentral permit tcp any host 62.199.66.24 eq 25
access-list zentral permit tcp any host 62.199.66.25 eq 80
access-group zentral in interface outside
```

ACL – Beispiel 2

```
access-list 3 permit icmp any any echo
access-list 3 permit icmp any any unreachable
access-list 3 permit icmp any any time-exceeded
access-list 3 permit tcp any any eq 80
access-list 3 permit udp any host 192.189.51.195 eq 53
access-list 3 permit tcp any host 192.189.51.195 eq 53
access-list 3 permit tcp any host 192.189.51.100 eq 25
access-list 3 permit tcp any host 192.189.51.100 eq 110
access-group 3 in interface inside
```


ASA als DHCP-Server

- `dhcpd address <first>-<last> <if>`
- `dhcpd domain <dns-domain>`
- `dhcpd dns <dnsserverip1> [<ip2>]`
- `dhcpd wins <winserverip1> [<ip2>]`
- `dhcpd lease <lease-time>`
- `dhcpd enable <if>`
- `dhcpd auto_config <if>`

DHCP-Server Troubleshooting

- show dhcpd statistics
Anzeige von Statistik-Information des DHCP-Servers
- show dhcpd binding
Anzeige der vergebenen IP-Adressen
- debug dhcpd event
- debug dhcpd packet

VPN-Tunnel Vorbereitung

- Definieren der Datenpakete für den Tunnel
access-list <name|nr> permit ip <quelle> <ziel>
- Erlauben des VPN-Traffics
Mit dem Befehl
sysopt connection permit-vpn
oder
entsprechenden Einträge in den ACLs
- Ausnahme für NAT wenn notwendig
NAT (<if>) 0 access-list <name|nr>

VPN-Tunnel

- Einrichten der Verbindungsparameter
crypto ipsec transform-set <name> <parameter>
crypto map <mapname> <nr> <parameter>
- Einrichten der Policy
crypto isakmp policy <nr>
 <parameter> <value>
- Aktivieren des Tunnels
tunnel-group <peer-IP> type <type>
tunnel-group <peer-IP> ipsec-attributes
 <attr> <val>

VPN-Tunnel – Beispiel Teil 1

- `access-list 100 permit ip 192.168.1.0
255.255.255.0 192.168.2.0 255.255.255.0`
- `sysopt connection permit-vpn`
- `crypto ipsec transform-set filial esp-3des esp-
md5-hmac`
- `crypto map filialmap 30 match address 100`
- `crypto map filialmap 30 set peer 192.168.0.2`
- `crypto map filialmap 30 set transform-set filial`
- `crypto map filialmap interface outside`

VPN-Tunnel – Beispiel Teil 2

- nat (inside) 0 access-list 100
- crypto isakmp enable outside
- crypto isakmp policy 10
 - authentication pre-share
 - encryption 3des
 - hash md5
 - group 2
- tunnel-group 192.168.0.2 type ipsec-l2l
- tunnel-group 192.168.0.2 ipsec-attributes
 - pre-shared-key test

VPN-Tunnel Überprüfung

- `show crypto isakmp sa`
Anzeige der aktuellen „IKE security associations“
- `show crypto ipsec sa`
Anzeige der aktuellen „IPsec security associations“
- `debug crypto isakmp sa <level>`
- `debug crypto ipsec sa <level>`

ASA – Management

- Zugriff direkt auf die Konsole (VT100)
- Zugriff via Telnet
- Zugriff via SSH
- Zugriff via HTTP/ ASDM (ASA Secure Device Manager)

Management – Telnet

- IPs müssen freigeschalten werden
 - telnet <ip> <mask> <if>
 - z.B.:
telnet 192.168.1.2 255.255.255.255 inside
 - Von Outside nicht direkt möglich
- Timeout festlegen (Default: 5 min)
 - telnet timeout 10

Management – SSH 1

- Schlüsselpaar notwendig
- IPs müssen freigeschalten werden
 - ssh <ip> <mask> <if>
 - z.B.:
ssh 192.168.1.2 255.255.255.255 inside
ssh 192.189.51.0 255.255.255.0 outside
- Timeout festlegen (Default: 5 min)
 - ssh timeout 10

Management – SSH 2

- SSH Version 1 und 2
 - Einstellbar mit dem Kommando:
ssh version { 1 | 2 }
- Benutzername: pix
- Password: <linepassword>

Management – http, ASDM 1

- Schlüsselpaar notwendig
- http-Server aktivieren:
 - http server enable [port]
- IPs müssen freigeschalten werden
 - http <ip> <mask> <if>

Management – http, ASDM 2

- Zugriff via `https://<asa-IP>[:port]`
- Kein Benutzername notwendig
- Password: `<enablepassword>`

Datum, Uhrzeit und ntp

- clock set <hh:mm:ss> {<day> <month> | <month> <day>} <year>
- clock summer-time <zone> recurring [<week> <weekday> <month> <hh:mm> <week> <weekday> <month> <hh:mm>] [<offset>]
- clock timezone <zone> <hours> [<minutes>]
- show clock [detail]
- ntp server <ip_address> [key <number>] source <if_name> [prefer]
- show ntp [associations [detail] | status]

Datum, Uhrzeit und ntp – Beispiel

- Beispiel für Mitteleuropa
 - clock timezone CET 1
 - clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00 60
 - ntp server 192.168.1.121 source inside
 - ntp server 192.168.1.122 source inside

Logging 1

- [no] logging on
- [no] logging timestamp
- [no] logging standby
- [no] logging host [<in_if>] <l_ip>
[<tcp|6>|<udp|17>/port#] [format {emblem}]
- [no] logging console <level>
- [no] logging buffered <level>
- [no] logging monitor <level>

Logging 2

- [no] logging history <level>
- [no] logging trap <level>
- [no] logging message <syslog_id> level <level>
- [no] logging facility <fac>
- [no] logging device-id hostname | ipaddress <if_name> | string <text>
- logging queue <queue_size>
- show logging [{message [<syslog_id>|all]} | level | disabled]

Logging – Beispiel

- logging on
- logging console error
- logging buffered warning
- logging host (inside) 192.168.1.23
- logging trap informational
- logging timestamp