Access Listen

Arten

- Standard
- Extended
- Named
    - Standard
    - Extended

Allgemein

- Verwendung von Wildcards
- eine Access-List pro:
    - Richtung
    - Interface
- Eine ***Standard Access-List*** sollte immer ***so nah wie möglich am Ziel*** implementiert werden, da nur die Source-Adresse kontrolliert wird.
- Eine ***Extended Access-List*** sollte immer ***so nah wie möglich an der Source*** implementiert werden.
- 0-Bits werden geprüft / 1er-Bits werden ignoriert

Erstellen einer Standard Access-List:
Router(config)#access-list 20 deny 172.16.20.2 0.0.0.255
Router(config)#access-list 20 permit any

Implementierung auf Interface:
Router(config)#int s0
Router(config-interface)#ip access-group 20 in

Entfernen der Access-List:
Router(config)#int serial 0
Router(config-interface)#no ip access-group 20 in
Router(config)#no access-list 20
Die ACL vom Interface entfernen und die ACL selber löschen!

Telnet Zugangsbeschränkung:
Router(config)#access-list 10 permit host 192.168.0.10
Router(config)#line vty 0 4
Router(config-line)# access-class 10 in

Hier wird der Zugriff auf den Host 192.168.0.10 begrenzt.

Salinas IT-Service GmbH
Prenzlauer Allee 8
10405 Berlin

www.salinas-it.de
Telefon: 030-25010852
Email: info@salinas-it.de

Erstellen einer Extended Access-List:

Beispiel 1: Verbieten von HTTP Verkehr.

Router(config)#access-list 101 deny tcp any any eq 80
Router(config)#access-list 101 permit ip any any
Router(config)#int s0
Router(config-interface)#ip access-group 101 in

Beispiel 2: Zugriff auf den lokalen Webserver des Routers unterbinden

Router(config)#access-list 1 deny any
Router(config)#ip http access-class 1

Erstellen einer Named Access-List:

Router(config)#ip access-list extended test
Router(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255
Router(config)#int s0
Router(config-interface)#ip access-group test out

Kontrolle Access-List:

Router#show ip interface ethernet 0
Router#show access-lists
Router#show running-config

Gruppierung der Nummerierten Access Lists

Wertebereich	Funktion	Filtert nach
1-99	IP Standard Access List	Absender IP-Adresse
100-199	IP Extended Access List	Absender IP-Adresse, Absender Port, Ziel IP-Adresse, Ziel-Port
200-299	Protocol Type-code Access List	Ethernet Protokoll (IP, IPX, etc.)
300-399	DECnet Access List	DECnet
400-499	XNS Standard	Xerox Network System
500-599	XNS Extended	Xerox Network System
600-699	Appletalk Access List	Apple Netzwerkprotokoll
700-799	48-bit MAC Address Access List	Absender MAC-Adresse, Ziel MAC-Adresse (nur Ethernet)
800-899	IPX Standard Access List	Novell-Netzwerk
900-999	IPX Extended Access List	Novell-Netzwerk
1000-1099	IPX SAP Access List	Novell-Netzwerk
1100-1199	Extended 48-bit MAC Address Access List	Absender MAC-Adressen Bereich, Ziel MAC-Adressen Bereich (nur Ethernet)
1200-1299	IPX Summary Address Access List	Novell-Netzwerk
1300-1999	IP Standard Access List (erweiterter Bereich)	Absender IP-Adresse
2000-2699	IP Extended Access List (erweiterter Bereich)	Absender IP-Adresse, Absender Port, Ziel IP-Adresse, Ziel-Port