IOS Router Security

2G05

Andreas Aurand
Network Consultant

HP NWCC

DECUS Symposium 2003

Agenda

- **Interaktive Zugang**
- **Lokale Services des Routers absichern**
  - Syslog
  - NTP
  - SNMP
  - HTTP
- **Schutz gegen Angriffe**
  - Denial of Service (DoS)
  - IP Spoofing
  - Flood Management
  - Routing-Attacken
  - NBAR

Interaktiver Zugang

Zugang sichern und protokollieren

- Zugriff auf Router über “log-input” Einträge einschränken und protokollieren
  - Erstes Paket wird “geloggt”, dann alle 5 Minuten die neue Gesamtzahl

```
access-list 101 permit tcp host 10.185.208.189 any eq telnet log-input
access-list 101 permit tcp host 10.185.208.189 any eq 22 log-input
access-list 101 permit tcp host 10.185.208.175 any eq telnet log-input
access-list 101 permit tcp host 10.185.208.175 any eq 22 log-input
access-list 101 deny   ip any any log-input
line vty 0 4
  access-class 101 in
```

- Angriff im LAN über ARP Cache Poisoning und IP Address Spoofing
  - Umgeht definierte Zugriffsliste
- Schutzmechanismen
  - Statische ARP-Einträge für zugelassenen Management-Stationen auf den Routern
  - ARP Inspection (Cat 6500) oder Sticky ARP (Cat6500 mit MSFC als Router)
  - Eigenes Management VLAN

Verbindung zum Router ist nicht sicher !!!!!

- ***Password Sniffing* ist einfach !!!!!!!!!!**
  - z.B. DSNIFF Tool

```
attack# dsniff -cn
dsniff: listening on eth0
-----------------
10/28/02 13:16:15 tcp 10.185.210.127.2137 -> 10.185.208.190.23 (telnet)
andreas
c
ena
c
exit
```

- Schutz bietet nur **Verschlüsselung der Verbindung**
  - **SSHv1** (Secure Shell; Feature Set mit DES oder 3DES Unterstützung)
  - **SSHv2** (Für Ende des Jahres geplant)
  - **Kerberized Telnet** (Enterprise Feature Set)
  - **IPSec** (Feature Set mit IPSec Unterstützung)

Verschlüsselung: Secure Shell (SSH)

- RSA-Schlüsselpaar generieren
  - **Verschlüsselung** und **Host-Authentifizierung**

rtr(config)# hostname *sissy*

rtr(config)# ip domain-name *frs-lab.de*

rtr(config)# crypto key generate rsa

rtr# show crypto key mypubkey rsa

```
% Key pair was generated at: 12:06:54 MET-DST Sep 30 2002
Key name: sissy.frs-lab.de
 Usage: General Purpose Key
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081
  …   …   …
  0001
% Key pair was generated at: 13:36:53 MET-DST Oct 18 2002
Key name: sissy.frs-lab.de.server
 Usage: Encryption Key
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261
  …   …   …
  67237538 B659E97E 379CC4A0 670418D9 64ACFF8B 2B5639DF
```

SSH Host Key

SSH Server Key

Verschlüsselung: SSH Authentifizierung

- Passwort-Authentifizierung des Benutzers
  - *AAA login authentication* der VTY Line

```
aaa authentication login SSH local
username andreas secret xxx
line vty 0 4
 login authentication SSH
 transport input ssh
 transport output ssh
```

  - **IOS SSH-Server unterstützt keine RSA-Authentifizierung**
- Keine Überprüfung des Server-Host-Key beim IOS SSH-Client
  - Anfällig für MitM-Attacke
- SSH Malformed Packet Vulnerabilities (Fix ab Januar 2003)
  - Routercrash; DoS-Angriff
  - http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

Verschlüsselung: SSH und SCP Kommandos

- SSH-Verbindung vom Host zum Router aufbauen

```
unix# ssh -c des -l andreas sissy
The authenticity of host '10.185.208.190 (10.185.208.190)' can't be established
RSA1 key fingerprint is 18:9c:32:7c:56:ec:b5:ec:f1:d6:d1:d6:52:49:50:9e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.185.208.190' (RSA1) to the list of known hosts.
Warning: use of DES is strongly discouraged due to cryptographic weaknesses
andreas@10.185.208.190's password:
```

```
sissy> show ssh
Connection      Version Encryption      State                   Username
 1      1.5     DES                     Session started         andreas
```

- Konfiguration über SSH sichern

```
# copy running-config scp:
Address or name of remote host []? 10.185.208.189
Destination username [andreas]?
Destination filename [sissy-confg]?
Writing sissy-confg
Password:
5432 bytes copied in 12.408 secs (452 bytes/sec)
```

Übertragung der Konfiguration sichern

- **Enable Password** wird als MD5-Prüfsumme übertragen
  - **Nicht reversibel**
- Entschlüsseln über *Dictionary* und *Brute Force*
  - *Dictionary*-Attacke auf das Passwort “winterzeit”: **15 Minuten**
  - *Dictionary*-Attacke auf das Passwort “winterzeit02”: **ca. 6 Stunden**

Services

Syslog

HTTP

NTP

Unnötige Services ausschalten

Systemmeldungen protokollieren

- Auf **Console**
  - **logging console**
- Auf **VTYs** und **TTYs**
  - **logging monitor** und **terminal monitor**
- In **lokalen Puffer**
  - **logging buffered**
- Auf **SYSLOG Server**
  - **logging ip-address** und **logging trap**
- Korrekte Zeit wichtig
  - **service timestamps log datetime msecs**
- Sequence Number um verlorene Meldungen zu erkennen
  - **service sequence-numbers**

Syslog-Konfiguration

```
service timestamps log datetime msec
service  sequence-numbers
!
logging buffered 20000 debugging
logging trap notifications
logging facility local6
logging rate-limit all 10
logging source-interface Loopback0
logging 10.185.208.189
```

Vermeidet Performanceprobleme durch zu viele SYSLOG-Meldungen

Beim Crash Coredump auf Server schreiben

- Falls Router crashen sollte, kann Auswertung erfolgen
  - Konfiguration testen mit **write core**

```
ip ftp source-interface Loopback0
ip ftp username crashusr
ip ftp password Crash$Pw
exception core-file permiter.dmp
exception protocol ftp
exception dump 10.185.208.189
```


NTP (Network Time Protocol)

- Zum Nachvollziehen eines Angriffs ist korrekte Zeit auf wichtig
  - NTP gegen **DoS**-Angriffe schützen
    - NTP-Pakete authentifizieren
    - Kein NTP auf Internet-Interface
  - ACL für NTP-Server definieren
    - Angriff über *ARP* und *IP Address Spoofing* möglich

```
ntp authentication-key 33 md5 xxxntpxxx
ntp authentication-key 44 md5 yyyntpyyy
ntp authenticate
ntp trusted-key 33
ntp trusted-key 44
ntp source Loopback0
ntp access-group peer 50
ntp max-associations 2
ntp server 10.185.208.175 key 44 prefer
ntp server 10.185.208.189 key 33
```

```
interface FastEthernet0
 description -- Inside Interface zum lokalen Netzwerk --
 ip address 10.185.208.190 255.255.255.0

interface Serial0
 description -- Outside Interface zum Internet --
 ip address 192.168.3.1 255.255.255.252
 ntp disable

access-list 50 permit 10.185.208.175
access-list 50 permit 10.185.208.189
```

SNMPv1 und v2c Management Services

- Authentifizierung über Community String
  - Klartext
  - Durch SNMP Polling wird Community String relativ häufig gesendet
- **Community String wie Passwort behandeln**
  - Öfters ändern und “schwieriges” Passwort verwenden

```
snmp-server community gansgehaim RO 11
snmp-server trap-source Ethernet0
snmp-server host 10.185.208.189 version 1 gansgehaim tty config snmp
```

  - Access-Liste für snmp-server community konfigurieren
    - Angriff über *ARP* und *IP Address Spoofing* möglich

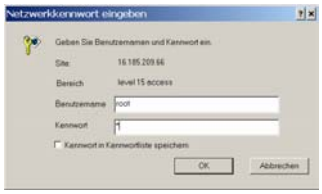
```
access-list 11 permit 10.176.208.0 0.0.0.255 log
access-list 11 permit 10.176.211.0 0.0.0.255 log
access-list 11 deny   any log
```


HTTP Management Service

- HTTP auf den Router ausschalten (**no ip http server**)
  - DoS-Angriffe auf den HTTP Server (Router Crash)
    - http://<router-ip>/%%
    - http://router-ip/anytext?/
- Falls HTTP notwendig, Zugriff kontrollieren (z.B. wegen QDM)

```
username root privilege 15 secret c
!
ip http authentication local
ip http server
ip http port 8089
ip http access-class 11
!
access-list 11 permit host 10.185.208.189 log
access-list 11 permit host 10.185.208.175 log
```

aaa, enable, local, tacacs



HTTP Management Service

- HTTPS ab IOS V12.2(15)T verfügbar

```
username root privilege 15 secret c

no ip http server
ip http authentication local
ip http secure-server
ip http secure-port 9099
[ ip http secure-client-auth ]
ip http secure-trustpoint FRS-LAB
ip http access-class 11

access-list 11 permit host 10.185.208.189 log
access-list 11 permit host 10.185.208.175 log
```

```
crypto ca trustpoint FRS-LAB
enrollment mode ra
  enrollment url http://192.168.1.210:80/certsrv/mscep/mscep.dll
  ip-address none
  password cisco
  crl optional

crypto key generate rsa
crypto ca authenticate FRS-LAB
crypto ca enroll FRS-LAB
```


Unnötige globale Services

- Jeder **offene Service** kann Ziel eines **Angriffs** sein
  - Unberechtigter Zugang zum Router
    - Z.B. Remote Cisco IOS TFTP-Server Exploit
  - DoS-Attacke (Router Crash)
    - Z.B. über das Senden von vielen CDP Neighbor Announcements
- Folgende globalen Services sollte man ausschalten

```
no service tcp-small-servers
no service udp-small-servers
no service pad
no service dhcp
no service finger
```

```
no ip finger
no ip domain-lookup
no ip bootp server
no ip http server
no ip source-route

no cdp run
```

Unnötige Services auf Schnittstellen

- Folgende Services auf Schnittstellen zum Internet ausschalten
  - ICMP Services

```
interface outside
  no ip mask-reply
  no ip redirects
  no ip unreachables
```

  - ARP Services

```
interface outside
  no ip local-proxy-arp
  no ip proxy-arp
  no ip rarp-server
```

  - Sonstige Services

```
interface outside
  no cdp enable
  ntp disable
```

Ab IOS V12.0 Standard: Schutz gegen „Smurf"-Attacke

```
interface inside
  no ip directed-broadcast
```


Unnötige Services auf Schnittstellen

- Ein ***show ip interface*** zeigt die Services an

```
router#show ip int s0
Serial0 is up, line protocol is up
  …  …  …
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is disabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are never sent
  ICMP unreachables are never sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  …  …  …
  Router Discovery is disabled
  …  …  …
```

TCP Port Scan

- **OS Detection** über TCP Port Scan

```
# nmap -P0 -O 10.120.208.66
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Initiating SYN Stealth Scan against  (10.120.208.66)
Adding open port 23/tcp
Adding open port 80/tcp
Adding open port 22/tcp
The SYN Stealth Scan took 21 seconds to scan 1601 ports.
For OSScan assuming that port 22 is open and port 1 is closed and
neither are firewalled
Interesting ports on  (10.120.208.66):
(The 1598 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
23/tcp     open        telnet
80/tcp     open        http
Remote operating system guess: Cisco router running IOS 12.1.5-12.2(6a)
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: All zeros
Nmap run completed -- 1 IP address (1 host up) scanned in 21 seconds
```


UDP Port Scan

- UDP Port Scans

```
attack# nmap -P0 -sU -pU:1-1023 10.120.208.66
Interesting ports on  (10.185.208.66):
(The 1017 ports scanned but not shown below are in state: closed)
Port       State       Service
49/udp     open        tacacs
67/udp     open        dhcpserver
69/udp     open        tftp
123/udp    open        ntp
161/udp    open        snmp
162/udp    open        snmptrap
```

- UDP Port Scan benötigt ICMP Unreachable Pakete
  - ***no ip unreachable*** auf dem Outside Interface

```
attack# nmap -P0 -sU -pU:1-1023 10.120.208.66
All 1023 scanned ports on  (16.185.209.66) are: filtered
Nmap run completed -- 1 IP address (1 host up) scanned in 1238 seconds
```

  - Nachteil: kein ***Path MTU Discovery*** möglich

Schutz gegen Angriffe

Denial of Service

IP Spoofing

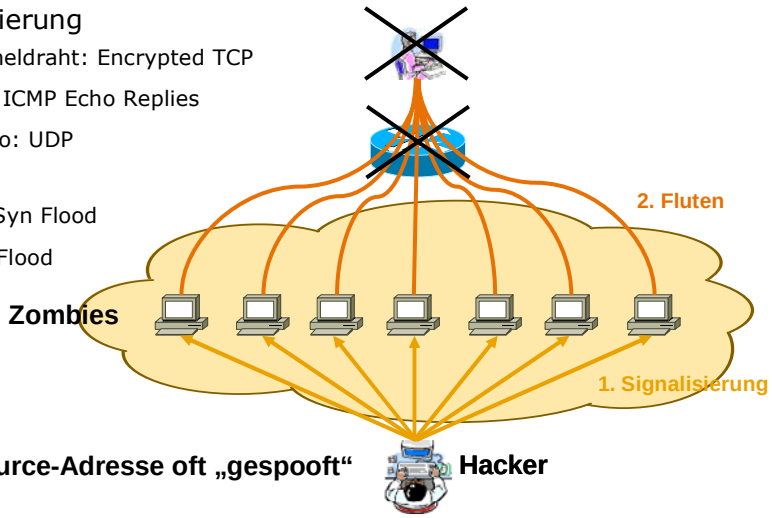
Flood Management

Routing Attacken

NBAR

Distributed Denial of Service (DDoS)

- Signalisierung
  - Stacheldraht: Encrypted TCP
  - TFN: ICMP Echo Replies
  - Trinoo: UDP
- Fluten
  - TCP Syn Flood
  - UDP Flood



ACL auf Outside Interface erweitern

- Alle Pakete können über ICMP, UDP oder TCP getunnel werden
  - **ICMP blocken**
  - UDP blocken
  - TCP so spezifisch wie möglich
  - **oder CBAC (IOS FW) verwenden**

```
access-list 2010 deny icmp any any log-input
access-list 2010 deny udp any any log-input
access-list 2010 permit tcp  ...
access-list 2010 permit tcp  ...
```


IP Spoofing

- Viele DoS-Attacken verwenden falsche IP-Quelladresse
  - **IP Spoofing**
  - Bestimmte Bereiche des IP-Adressbereichs sind nicht vergeben
    - http://www.iana.org/assignments/ipv4-address-space
    - RFC 3330 – Special-Use IPv4 Addresses
- Anti-IP-Spoofing-Mechanismen
  - 1.) Filtern von ankommenden IP-Paketen über **Access-Listen**
  - 2.) **Unicast Reverse Path Forwarding**
- Anti-Spoofing auf Inside und Outside Interface
  - IP-Spoofing-Attacken von internen Benutzern verhindern
  - Erkennen von infizierten Systemen

Anti IP Spoofing mit Access-Listen

- Log-Mechanismus der ACLs verwenden
  - Protokolliert Quelle und Ziel des Pakets
  - Erkennt Angriffe und infizierte Systeme

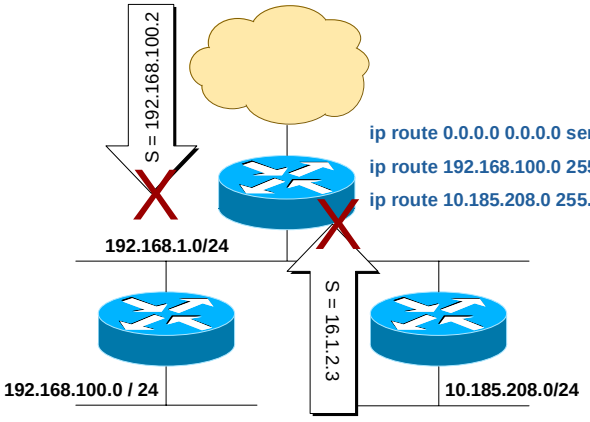
Erkennt infizierte Systeme, die nur den Hostanteil der Quelladresse verändern (z.B. Stacheldraht DDoS)

```
! # Ungültige IP-Quelladressen
access-list 2010 deny ip 0.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 224.0.0.0 31.255.255.255 any log-input
! # Privater IP-Adressbereich
access-list 2010 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 2010 deny ip 192.168.0.0 0.0.255.255 any log-input
! # Nicht vergebener IP-Adressbereich
access-list 2010 deny ip 1.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 2.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 5.0.0.0 0.255.255.255 any log-input
...
access-list 2010 permit …
!
Interface Serial0
  description – Outside Interface –
  ip access-group 2010 in
```

```
! # Freie Adressen aus dem lokalen Netzwerk sperren
access-list 2020 deny ip host 192.168.1.200 any log-input
access-list 2020 deny ip host 192.168.1.201 any log-input
access-list 2020 deny ip host 192.168.1.220 any log-input
! # Nur lokale Systeme dürfen Verbindung aufbauen
access-list 2020 permit ip 192.168.1.0 0.0.0.255 any
! # Sperren aller anderen IP-Adressen
access-list 2020 deny ip any any log-input
!
Interface Ethernet0
  description – Inside Interface –
  ip address 192.168.1.1 255.255.255.0
  ip access-group 2020 in
```


Anti IP Spoofing mit Unicast RPF

- Router leitet Paket nur weiter, wenn er es über die Schnittstelle empfängt, die er auch benutzt, um die Quelladresse des Pakets zu erreichen.



Anti IP Spoofing mit Unicast RPF

```
interface Serial0
  description -- Outside Interface --
  ip address negotiated
  ip access-group 2010 in
  ip verify unicast source reachable-via rx allow-default
!
ip route 1.0.0.0 255.0.0.0 null0
ip route 2.0.0.0 255.0.0.0 null0
ip route 5.0.0.0 255.0.0.0 null0
ip route 7.0.0.0 255.0.0.0 null0
ip route 10.0.0.0 255.0.0.0 null0
…  …  …
access-list 2010 deny ip 0.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 127.0.0.0 0.255.255.255 any log-input
access-list 2010 deny ip 224.0.0.0 31.255.255.255 any log-input
access-list 2010 permit …
```

Für ungültige Quell-Adressen weiterhin ACL notwendig

```
# show ip interface Serial0
IP verify source reachable-via RX, allow default
  58 verification drops
  0 suppressed verification drops
```


Flood Management

- DoS-Angriffe basieren oft auf Fluten von vielen unnötigen Paketen
  - Router verarbeitet nur noch Netzwerkinterrupts
  - Schutz durch Scheduler-Definition
    - Alt: **scheduler interval 500**
    - Neu: **scheduler allocate 30000 2000**

Microsekunden in denen der Router mit maskierten Interrupts läuft

Microsekunden in denen der Router mit eingeschalteten Interrupts läuft

- **Verwendung von *Quality of Service***
  - Rate Limiting für Multicast, UDP und ICMP
- **TCP Syn Flooding**
  - TCP Intercept und TCP Inspect
  - Bestandteil des IOS Firewall Feature Sets

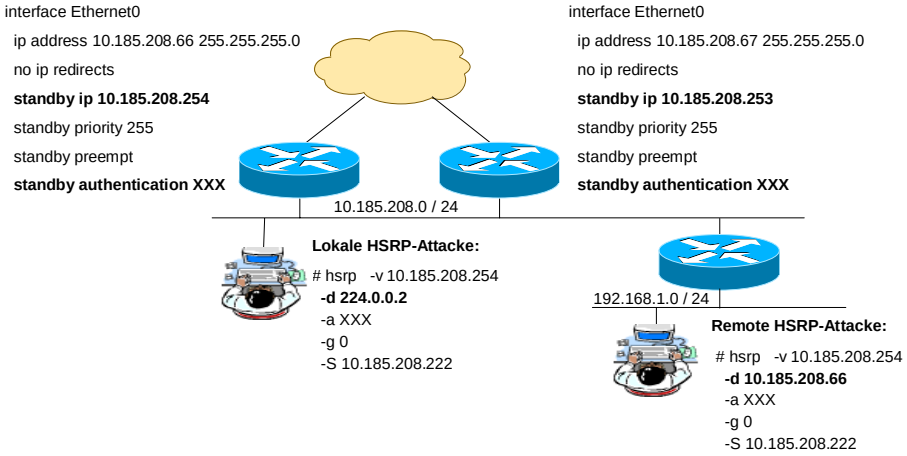
Angriffe auf Routing-Infrastruktur vermeiden

- **IP Source Routing ausschalten**
  - Sender des IP-Pakets kann Pfad zum Zielsystem vorgeben
    - **no ip source-route** (globles Kommando)
- **Authentifizierung der Routing-Pakete**
  - Attacken auf Routing-Infrastruktur und falsch konfigurierte Router
    - BGP, EIGRP, IS-IS, OSPF, RIPv2
  - Klartext- und MD5-Authentifizierung
- **Distribute-Listen**
  - Verhindern Annahme von falschen Routen
    - **distribute-list # in** (Router Kommando)

Warum Routing-Pakete authentifizieren ?

- IOS EIGRP Network DoS (alle IOS-Versionen betroffen)
  - http://www.cisco.com/warp/customer/707/eigrp_issue.html
    - Wenn der Router mit “gespooften” EIGRP Neighbor Announcements überflutet wird, kommt es zu einem ARP-Sturm, der die gesamte Bandbreite Netzwerksegement des Netzwerksegments in Anspruch nimmt.
  - Schutz durch MD5-Authentifizierung der EIGRP-Pakete
- IOS Memory Exploit (nur alte IOS Versionen < 12.1)
  - Bei mehr als 255 OSPF Neighbors kommt es zu einem Buffer Overflow in der I/O Memorystruktur.
    - Kann ausgenutzt werden, um Befehle auf dem Router auszuführen, die eine eigene Konfiguration in das NVRAM schreibt.
  - Schutz durch MD5-Authentifizierung der OSPF-Pakete

HSRP-Attacke



- Remote HSRP-Attacke mit Unicast-Paketen funktioniert nur in älteren IOS Versionen

HSRP-Attacke

- Router mit der höchsten Priorität wird Active Router
  - Bei gleicher Priorität ist höhere IP-Adresse entscheidend
    - Priorität für Active Router: 255
    - IP-Adresse für Active Router: …254
- HSRP unterstützt nur Klartext-Authentifizierung
  - Kein Schutz gegen Attacken, Passwort ist auf dem Netz sichtbar
- Filtern von HSRP-Multicasts auf den HSRP-Routern (IP Spoofing möglich)

```
ip access-list extended HSRPFilter
 permit udp host 10.185.208.66 host 224.0.0.2 eq 1985
 permit udp host 10.185.208.67 host 224.0.0.2 eq 1985
 deny   udp any any eq 1985
```

- Filtern von HSRP-Multicasts auf dem Switch

```
set igmp filter enable
set igmp filter profile 1 match-action deny
set igmp filter profile 1 224.0.0.2
set igmp filter map 1 3/3-3/48
```

NBAR

- **Network-Based Application Recognition**
  - Erweiterter Klassifizierungsmechnismus, der Applikationsprotokolle erkennt
    - Kann Inhalt von HTTP-Paketen überprüfen
    - Angriffe, die durch ein Paket identifizierbar sind, können verhindert werden
    - Ab IOS V12.1(5) für 7200, 7100, 36xx, 26xx, V12.2(5) für 17xx
    - Pro untersuchtem Flow werden 150 Byte Memory benötigt
- NBAR wird zusammen mit ***Quality of Service*** (QoS) eingesetzt
  - Paket markieren
  - Paket verwerfen
  - Übertragungsrate limitieren

NBAR Konfiguration

```
ip cef

ip nbar port-map custom-02 udp 445
ip nbar port-map custom-02 tcp 445
ip nbar port-map custom-01 udp 1434

class-map match-all SQLSlammer
   match protocol custom-01
   match packet length min 404 max 404
class-map match-any NetBIOS
   match protocol netbios
   match protocol custom-02
class-map match-any HTTP-Attacks
   match protocol http url "*.ida*"
   match protocol http url "*cmd.exe*"
   match protocol http url "*root.exe*"
   match protocol http url "*readme.eml*"
   match protocol http mime "application/octet-stream"
   match protocol http mime "application/x-msdownload"
   match protocol http mime "application/x-javascript"
   match protocol http host "badguy*"
```

Länge des IP Pakets (wie im IP Header eingetragen)

```
policy-map AttackProtection
  class HTTP-Attacks
    drop
  class SQLSlammer
    drop
  class NetBIOS
    drop

interface FastEthernet0
   ip address 192.168.1.1 255.255.255.0
   ip nbar protocol-discovery
  service-policy input AttackProtection

interface Serial0
   ip address negotiated
   ip nbar protocol-discovery
  service-policy input AttackProtection
```

NBAR und QoS Informationen

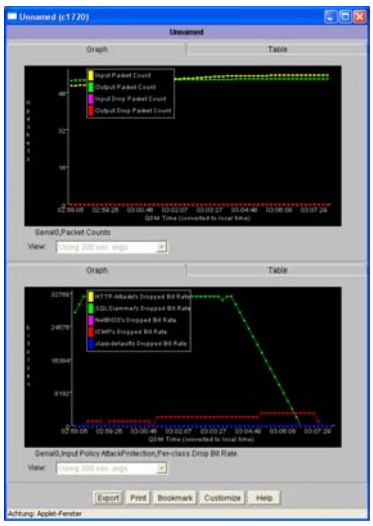
router# show policy-map interface s0

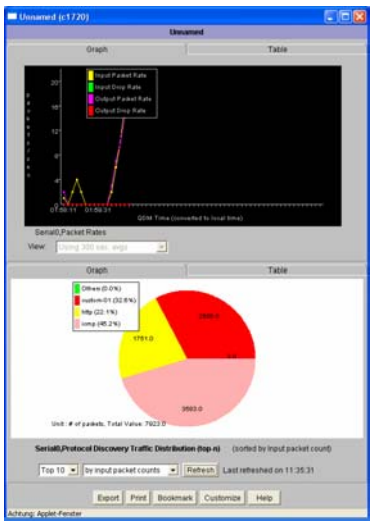
```
Serial0
 Service-policy input: AttackProtection
   Class-map: HTTP-Attacks (match-any)
     5 packets, 1892 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: protocol http url "*.ida*"
       0 packets, 0 bytes
       5 minute rate 0 bps
     Match: protocol http url "*cmd.exe*"
       0 packets, 0 bytes
       5 minute rate 0 bps
     Match: protocol http url "*root.exe*"
       5 packets, 1892 bytes
       5 minute rate 0 bps
     …    …    …
   Class-map: SQLSlammer (match-all)
     1 packets, 408 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: protocol custom-01
     Match: packet length min 404 max 404
     drop
```

router# show ip nbar port-map

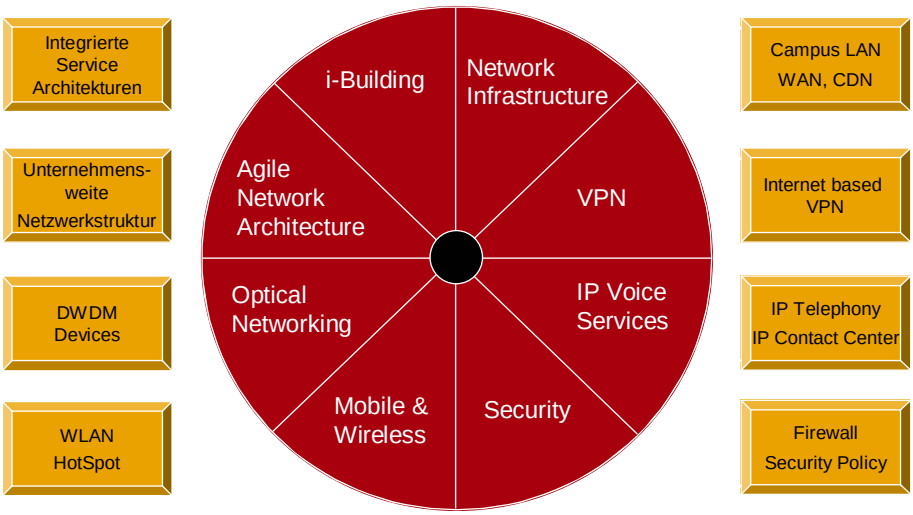
```
port-map bgp          udp 179
port-map bgp          tcp 179
port-map citrix       udp 1604
port-map citrix       tcp 1494
port-map cuseeme      udp 7648 7649 24032
…    …    …
```


QDM – Quality Device Manager





NSG Fokusthemen



Interessante Links

- Cisco Internet Security Advisories
  - http://www.cisco.com/go/psirt
- Improving Security on Cisco Routers
  - http://www.cisco.com/warp/public/707/21.html
- Secure IOS Template
  - http://www.cymru.com/Documents/secure-ios-template.html
- IOS QoS Device Manager (QDM)
  - http://www.cisco.com/warp/public/477/QDM_faq.shtml
- Virus Protection mit NBAR
  - http://www.cisco.com/warp/public/63/nimda.shtml