Demilitarisierte Zonen und Firewalls

Kars Ohrenberg
IT

Gliederung

- IP-Adressen, Netze, Ports, etc.
- IT-Sicherheit
- Warum Packetfilter/Firewalls?
- Packtfilter/Firewalls im DESY Netzwerk
- Konzept einer Demilitarisierten Zone (DMZ)
- Zusammenfassung

Adressen, Netzwerke Protokolle und Ports

- Was ist eine IP-Adresse?
  - Adressiert System im Netzwerk (131.169.40.200)
- Was ist eine Netzwerkadresse?
  - Bereich von IP-Adressen (z. B. 131.169.0.0/16)
  - Netzwerke werden über Router verbunden
- Was ist ein Protokoll?
  - IP-Paket speziellen Typs (TCP, UDP, ICMP, RIP, ...)
- Was ist ein TCP/UDP-Port?
  - Adressiert den auf einem Netzwerkgerät verfügbaren Dienst, z.B. Port 80 = http, 22 = ssh

Sicherheit in Netzwerken

- Im allgemeinen kann jedes an einem Netzwerk angeschlossene Gerät jedes andere System ohne Einschränkung erreichen
- Software ist selten fehlerfrei, daher gibt es zahlreiche Bedrohungen die einen reibungslosen Betrieb gefährden:
  - Denial of Service Attacken (DoS), Würmer, Viren, Hacker, ...
- Ein ungepatchtes und ungeschütztes System wird heutzutage innerhalb von Minuten aus dem Internet angegriffen und in weniger als 15 Minuten infiziert oder gehackt

Sicherheit auf Rechnerebene

- Neben Sicherheitsmechanismen die im Netzwerk realisiert werden können, gibt es eine Vielzahl von Möglichkeiten die Sicherheit auf den Endsystemen selber zu erhöhen:
  - Patches
  - Personal Firewall
  - Virenscanner
  - ...

‚Probleme' mit Sicherheit auf Rechnerebene

- Das System muss regelmäßig modifiziert werden, dies ist nicht unbedingt erwünscht (Server, Kontrollsysteme, Spezialhardware, ...)
- Es ist vergleichsweise schwer ein zentrales Management zu implementieren, insbesondere bei Beteiligung vieler Interessengruppen
- Insbesondere mobile Geräte (Laptops, ...) sind üblicherweise mit vielen individuellen Einstellungen und Komponenten stark personalisiert

Sicherheitsfunktionen in Netzwerken – Paketfilter

- Router können Verkehr aufgrund von IP-Adressen, Netzwerkadressen, Protokollen oder auch Ports filtern
- Relativ einfach und günstig einsetzbar da auf jedem Router verfügbar
- ABER: Keine Unterstützung zustandsbasierender, dynamischer Protokolle (z.B. FTP, H.323, ...)

Welche Adressen, Ports, etc. sind freizuschalten?

- Ein häufiges Problem beim Einsatz von Paketfiltern ist die Unkenntnis der freizuschaltenden Adressen und Ports
- Router liefern bei entsprechender Einstellung ausführliches Protokoll der blockierten Pakete
  - Es resultiert ein besseres Verständnis des Dienstes
  - Analyse der Log-Dateien erlaubt Rückschlüsse auf Auffälligkeiten im Netzwerk (z.B. Würmer)

Beispiel eines einfachen Paketfilters


```
RT-197-3#sh access-lists ipt-server-out
Extended IP access list ipt-server-out
    10 permit tcp any any established (1 match)
    20 permit tcp any eq ftp-data any
    30 permit icmp any any echo (23 matches)
    40 permit icmp any any echo-reply
    50 permit icmp any any unreachable (1 match)
    60 permit icmp any any time-exceeded
    70 permit icmp any any parameter-problem
    80 permit udp host 131.169.40.200 eq domain any range 1024 65535
    90 permit tcp host 131.169.40.200 eq domain any range 1024 65535
    100 permit udp host 131.169.194.200 eq domain any range 1024 65535
    110 permit tcp host 131.169.194.200 eq domain any range 1024 65535
    120 permit udp host 131.169.40.65 eq ntp any eq ntp (9 matches)
    130 permit udp host 131.169.194.85 eq ntp any eq ntp (11 matches)
    140 permit udp host 131.169.194.86 eq ntp any eq ntp (27 matches)
    150 permit udp host 131.169.56.32 range 1024 65535 any eq snmp
    160 permit udp host 131.169.56.46 range 1024 65535 any eq snmp (79 matches)
```


Beispiel für Log-Einträge


```
…
Sep 19 21:41:59 rt-197-3 389240: Sep 19 21:41:58.490 MEST: %SEC-6-IPACCESSLOGP:
  list 123 permitted tcp 131.169.40.200(50144) (Vlan40 0030.482c.226c) -> 131.169.56.37(53),
  1 packet
Sep 19 21:42:00 rt-197-3 389241: Sep 19 21:41:59.778 MEST: %SEC-6-IPACCESSLOGP:
  list 123 permitted tcp 131.169.40.200(50145) (Vlan40 0030.482c.226c) -> 131.169.56.37(53),
  1 packet
Sep 19 21:42:04 rt-197-3 389242: Sep 19 21:42:03.046 MEST: %SEC-6-IPACCESSLOGP:
  list 123 denied tcp 131.169.40.77(44836) (Vlan40 0002.5533.7441) -> 131.169.56.33(1757),
  1 packet
…
```

Paketfilter im DESY-Netz

- Einige Subnetze sind schon seit vielen Jahren mit Paketfiltern versehen:
  - Büronetze: Gebanis, IP-Phones, V1/V3, V4, V2, SAP-HR
  - Servernetze: SAP, WLAN-Admin, RZ-Admin, 51er, IT-Server (40er und 56er), IPT-Server
  - Freischaltung erfolgt in Absprache zwischen Dienstbetreibern, Segmentadministratoren und NOC
  - Dokumentiert unter http://www-it.desy.de/network/intranet/services/dns/beauftragte.html

Sicherheitsfunktionen in Netzwerken - Firewalls

- Führen eine Statustabelle aller aktuell aktiven Verbindungen und erlauben ‚Statefull Inspection'
- Analysieren den Kommunikationstrom der Applikationen:
  - Einhaltung des Applikationsprotokolls
  - Dynamisch benötigte Ports können automatisch geöffnet werden
    - H.323, FTP, ICMP, DNS, ...
  - Systeminformationen innerhalb der Datenpakete können ‚versteckt' werden

Die ‚Internet Firewall' am DESY

- Aktuell über eine Cisco PIX 535 in redundanter Konfiguration realisiert
- Maximaler möglicher Durchsatz liegt bei 1 GBit/s
  - 10 GBit/s heutzutage noch eine große technische Herausforderung
- Aktuelle Filterliste enthält z. Zt. ~1500 Einträge
- Freischaltungen werden von D4 genehmigt und durch NOC technisch realisiert

Firewalls im DESY-LAN

- Firewall Service Modul
  - Einschubkarte für zentrale Router
  - Nahtlose Integration in VLAN-Struktur
  - Maximaler Durchsatz 5 GBit/s
  - Erste Tests im VoIP-Umfeld
  - 2 Modi Transparent/Routed
  - Mandantenfähig

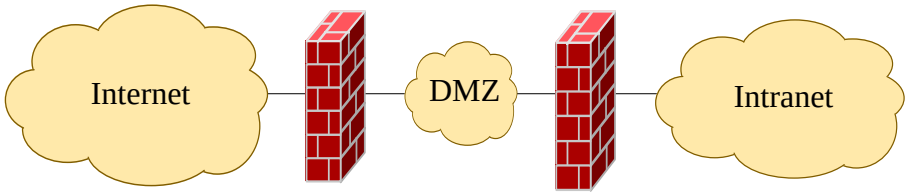
Beispielkonfiguration

```
…
class-map inspection_default
 match default-inspection-traffic
class-map http-map1
 match access-list acl-http1
!
!
policy-map global_policy
 class inspection_default
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect icmp
  inspect icmp error
 class http-map1
  set connection advanced-options mss-map
!
service-policy global_policy global
…
```


Demilitarisierte Zone

- Demilitarisierte Zone (DMZ): Eine demilitarisierte Zone entspricht einem Rechner oder Rechnerverbund zwischen einem internen und einem externen Netz. In der DMZ werden die Dienste angeboten, die sowohl vom LAN als auch vom Internet zugänglich sein müssen, zum Beispiel ein Mailserver. Die DMZ ist sowohl zum lokalen Netz als auch zum Internet durch eine Firewall geschützt.

DMZ Layout



Vorteil einer DMZ

- Vorteil einer solchen Lösung ist es, dass im Falle einer Kompromittierung eines Servers in der DMZ das interne Netz trotzdem noch geschützt bleibt. Wären die Server nicht in einer DMZ, sondern direkt im internen Netz, so wäre auch das gesamte interne Netz durch eine Kompromittierung betroffen

DMZ im DESY-LAN

- Ein Subnetz als DMZ aufgebaut (131.169.5.0), innerhalb der WAN-Firewall realisiert
- Folgende Server sind bereits in der DMZ angesiedelt: bastion, wof, srm-dcache, h1web01, it-ftp, smtp, ..
- Generell sollte jeder Rechner der einen externen Dienst anbietet in der DMZ stehen!
- Freischaltungen des Internet zur DMZ über D4, Freischaltungen von der DMZ ins Intranet über NOC
- Das Netz für das LHC Computing Grid (131.169.98.0) kann als DMZ-2 betrachtet werden, ist aber über Paketfilter aus WAN-Router realisiert

Ausblick

- Die Nachfrage und der Bedarf an geschützten Netzwerkbereichen wächst
- Die aktuell eingesetzten Paketfilter werden in den kommenden Monaten durch Firewalls ersetzt
- Bei jedem zum Internet freigeschalteten Dienst sollte der mögliche Einsatz in der DMZ geprüft werden