Westfälische Wilhelms-Universität Münster

Zentrum für Informationsverarbeitung

Sicherheit und Netze
- Firewalls -

Westfälische Wilhelms-Universität Münster
Zentrum für Informationsverarbeitung
Abteilung Kommunikationssysteme

Guido Wessendorf
wessend@uni-muenster.de

ZIV-Vorlesung
WS 2008/09 - Veranstaltungsnummer 260040
Münster, 20. November 2008

wissen.leben WWU Münster

Themen

- Einführung in IV-Sicherheit
- Grundlagen
- Was ist eine Firewall?
- Firewall-Techniken
- Firewall-Toplogien
- Personal-Firewalls
- Vorführung

Einführung in IV-Sicherheit

Grundwerte der Informationsverarbeitung

- Verfügbarkeit (Availability)
  - Daten, Dienstleistungen, Ressourcen
- Vertraulichkeit (Confidentiality, Privacy)
  - Informationen, Daten
- Unversehrtheit, Korrektheit (Integrity)
  - Daten, Systeme
- Verbindlichkeit – Authentizität, Nicht-Abstreitbarkeit (Non-Repudiation)
  - Daten, Dienstleistungen (Transaktionen)

Grundwerte der Informationsverarbeitung

Verletzung der Grundwerte der IV führt zu

- Verletzung der Rechte von Personen, Organisationen, Unternehmen, Staat
- materiellen Schäden
- ideellen Schäden

und ist häufig Verstoß gegen Gesetze

Bedrohungen

- prinzipielle Bedrohungen
  - Verlust von Grundwerten
- spezifische, unmittelbare Bedrohungen
  - Virenbefall, Stromausfall, Einbruch, Passwort-Kompromittierung, ...
- mittelbare Bedrohungen
  - schädliche Auswirkungen auf die IV-Dienstleistung des Unternehmens (Arbeitsplatzausfall, Service-Einschränkungen, Produktionsausfall)
- Folgewirkungen
  - Gewinnausfall, Ansehensverlust, Geschäftsschädigung
- beabsichtigte Bedrohungen
  - Spionage, Sabotage, Vandalismus
- unbeabsichtigte Bedrohungen
  - höhere Gewalt, technisches Versagen, menschliches Versagen

Sicherheitsrisiko Netz?

„Neue“ allgegenwärtige IV-Sicherheitsrisiken durch

- Anbindung von IV-Strukturen an das Internet
- insbesondere in Verbindung mit dem Aufkommen von LANs

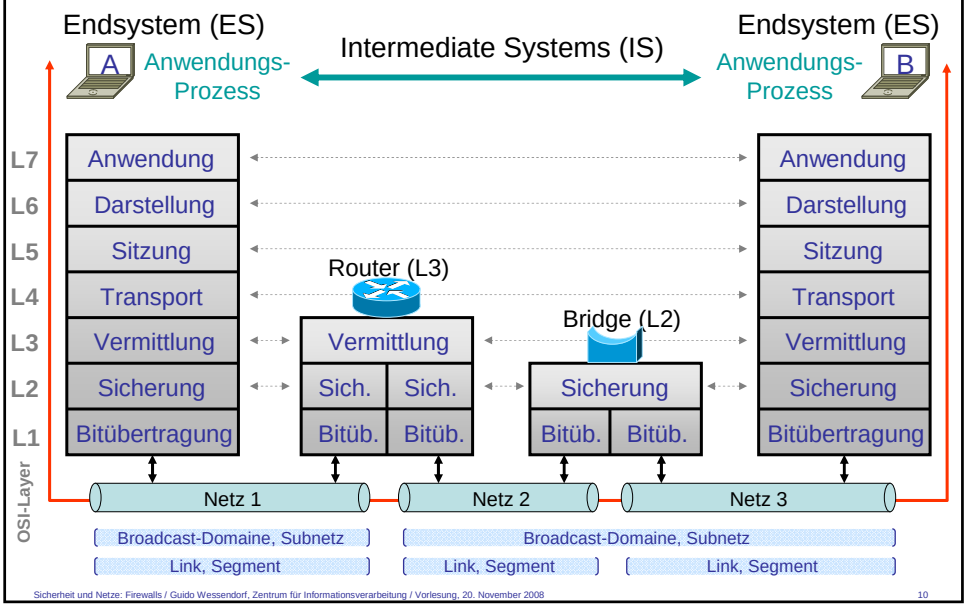
Bedrohungen *über* oder *durch* das Netz/Internet?

Sicherheit in (großen) Netzen

- wie kann man in (großen komplexen) Netzen IV-seitige Sicherheit verbessern?
  - Endsystem-Sicherheit *(vorrangig!)*
    - skalierend
    - nutzernah
    - anwendungsbezogen
    - Methoden (u.A.):
      - Anti-Virus-Scan
      - Personal-Firewall
      - Update-Services
      - Host-Intrusion-Prevention
      - Policy-Orchestrierung
  - Netzwerk-Sicherheit
  - natürliche Aufgabenteilung
    - Systemadministration:
      - Sicherheit in IT-Endsystemen
      - Sicherheit in IT-Anwendungen
      - Ende-zu-Ende-Sicherheit
    - Netzadministration:
      - Sicherheit im Übermittlungssystem (L1-3, L4)

Grundlagen

Rückblick: das OSI-Modell



Rückblick: das OSI-Modell

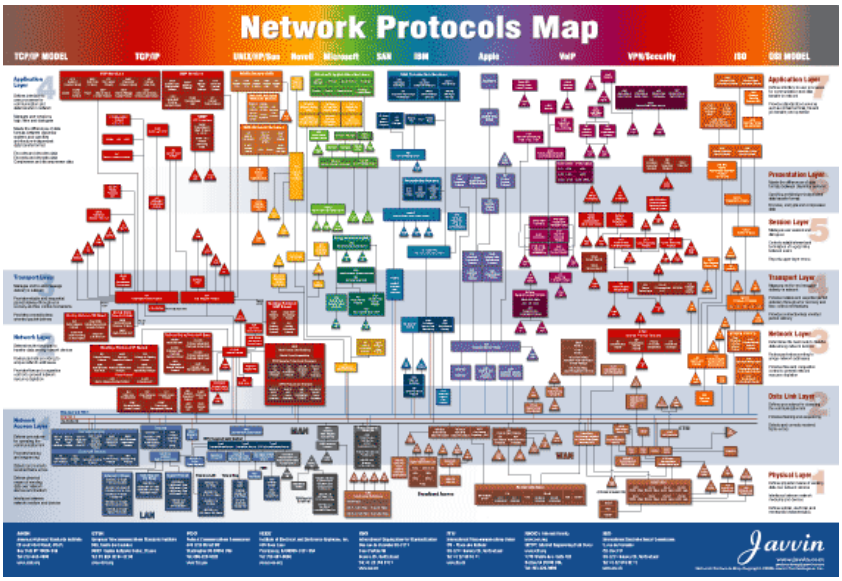
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- zugehörige Dienste und Medien (Beispiele)

Anwendungs-System (L5–L7)	FTP	SMTP	Telnet	HTTP	DNS	RPC	NFS
Transport-System (L2–L4)	TCP				UDP		
	IP				ICMP	ARP	
	Ethernet, Token-Ring, FDDI, ATM, PPP						
Übertragungs-medium (L1)	Twisted-Pair, LWL, Koaxialkabel, Funk, Laser						

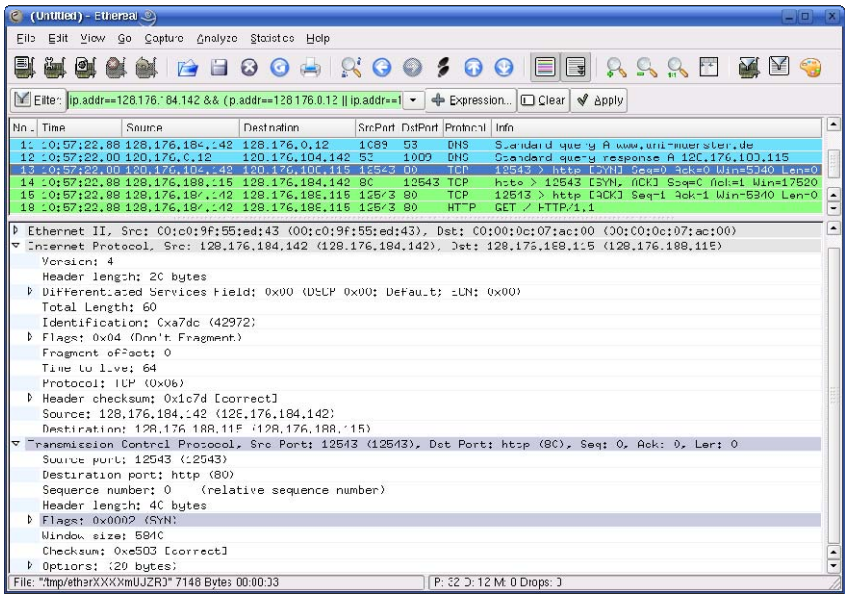
Komplexe Protokollwelten...

ZENTRUM FÜR INFORMATIONS VERARBEITUNG



Quelle: http://www.javvin.com/

Protokoll-Header (snapshot)



Was ist eine Firewall?

- sie ist eine „Brandschutzmauer“ (Firewall);
  soll trennen, einschränken und analysieren
- sie ist zwischen zwei (oder mehr) Netzen installiert und soll nur „erlaubte“ Kommunikation durchlassen
- sie weist unzulässige Kommunikation ab und kann erkannte Missbrauchsversuche protokollieren
- sie setzt *zuvor* definierte Sicherheitskonzepte (Security-Policies) technisch durch
- sie ist selber „sicher“ (gegen Angriffe)

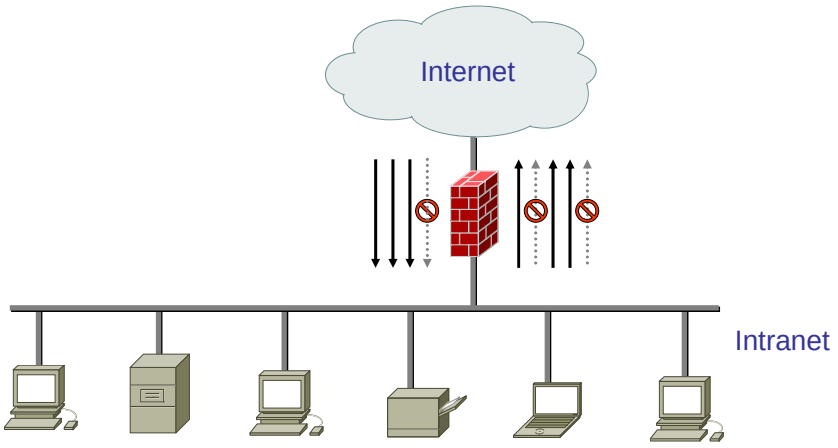
Was kann eine Firewall nicht?

- vor bösartigen Insidern schützen
- vor Verbindungen schützen, die nicht durch sie hindurchführen
- vor neuen Gefahren schützen
- im Allgemeinen nicht vor Viren und Verkehrs-Anomalien schützen (⇨IPS)
- Endgeräte-Sicherheit ersetzen
- sichere Kommunikationsverfahren (Ende-zu-Ende) ersetzen
  - Verschlüsselung, Authentifizierung, digitale Signaturen
- sich selber richtig konfigurieren ;-)

Firewall-Techniken

- Paketfilter
  - stateless Packet-Screen („ACL“)
  - stateful Packet-Inspection („Firewall“)
- Application-Gateways (ALG) und Proxies
- Network-Adress-Translation (NAT)
  - eigentlich keine Firewall-Technik, aber mit ähnlicher Wirkung

Paketfilter



Paketfilter

realisiert in

- L2-Switches (Access-Bereich)
  - MAC-Adress-Filterung, CoS-Filterung, VLAN-Tag-Filterung, 802.1X-Zugangskontrolle, Protokoll-Filterung („Ethertype“, z.B. IPv4, IPv6, IPX, ARP)
- L3-Switches (Backbone-Bereich)
  - Quell/Ziel-IP-Adress-Filterung, Protokoll-Filterung (z.B. TCP, UDP, GRE, ICMP, IGMP), Paketgröße
  - L4-Protokoll-Filterung
    - TCP-Port
      - Beispiele: HTTP [80], Telnet [23], FTP [21], SSH [22], SMTP [25], Netnews [119]
    - TCP-Verbindungsaufbau: SYN-Flag
    - UDP-Port
      - Beispiele: DNS [53], NTP [123], SNMP [161], Syslog [514]
    - ICMP-Typ
      - Beispiele: echo request [8], echo reply [0], destination unreachable [3], redirect [5]

Paketfilter

realisiert in

- dedizierten Firewall-Lösungen (zentralisierter Ansatz)
  - großer Funktionsumfang
  - höhere Performance
  - (mandantenfähiges) Management
- Personal-Firewalls (dezentralisierter Ansatz)
  - FW-Software auf Endsystemen
  - skalierend und anwendungsbezogen
  - Administration?

Leistungsdaten stark produktabhängig

Stateless Packet-Screens

- analysieren und kontrollieren Pakete ohne Veränderung der Pakete
  - bzgl. Inhalte der L2-, L3- und L4-Felder (Header-Felder)
  - bzgl. dem Quell- bzw. Ziel-Interface (an dem das Paket empfangen bzw. weitergeleitet wird)
  - durch sequentielle Abarbeitung von „Access-Control-Lists“ (ACL): „*interface, in/out, source, destination, service, permit/deny*“
  - ohne Berücksichtigung früherer Pakete (zustandslos, „stateless“)
    - Möglichkeiten begrenzt (s.u.)

Stateless Packet-Screens

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Vorteile:
  - oft in Hardware implementiert, d.h. ohne Performance-Einbußen zu betreiben: „wirespeed“
    - im Uni-Core zur Zeit bis zu n×10 Gbit/s vollduplex
  - oft Mehrwert bereits vorhandener Systeme
- Nachteile:
  - unterstützen keine „portagilen“ Anwendungen
    - komplexe Protokolle wie z.B. FTP, H.323 oder SIP handeln dynamisch weitere Übertragungskanäle aus. Nur mit Protokollanalyse und Zustandsverwaltung zu handhaben
  - unterstützen keine IP-Fragmentierung
  - Regelwerke zumeist „offener“ als notwendig um mangelhafte Möglichkeiten zu umgehen
    - z.B. Rückkanäle (bzw. mögliche Rückkanal-Bereiche) dauerhaft freigegeben
  - Regelwerke unübersichtlicher

Stateful Packet-Inspection

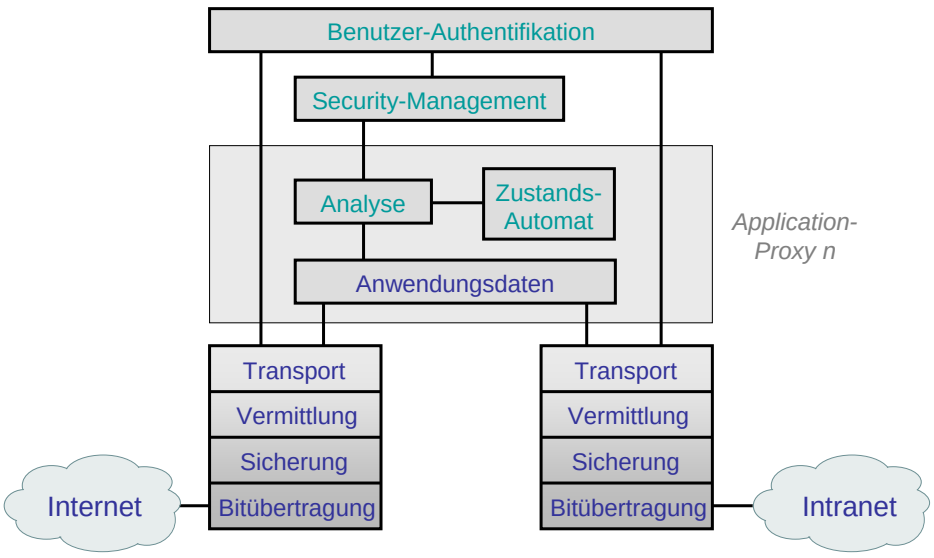
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- wie stateless Packet-Screens, jedoch zusätzlich:
  - Connection-Tracking: Firewall merkt sich Zustände (States) von Kommunikationsverbindungen in Session-Tables
    - typische State-Informationen:
      Quell-/Ziel-IP, Protokoll, Ports, Session-Dauer, Protokoll-Phase (TCP)
  - signifikante Vorteile
    - leichter zu konfigurieren, weniger Regeln notwendig
    - Rückkanäle sind nur bei Bedarf geöffnet
    - Unterstützung komplexer Protokolle
  - häufig auch weitere Mehrwerte implementiert
    - Überprüfung auf protokollkonforme Kommunikation (Application-Inspection)
    - Denial-of-Service (DoS) Inspection
    - Nutzer-Authentification
- Nachteil:
  - limitierter Durchsatz (im Vgl. zu stateless-ACLs)

Vorteile und Grenzen von Paketfiltern

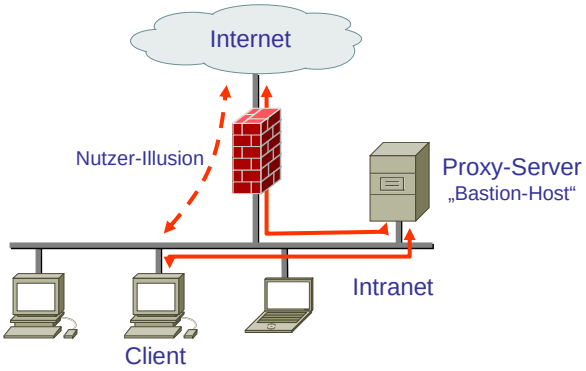
- Transparenz
  - \+ kein Eingriff in Kommunikationsverfahren
  - – Schutz der Intranets abhängig von Sicherheit der erreichbaren Anwendungssysteme
  - – Strukturinformationen des Intranets (IP-Adressen) nicht verborgen
- breite Einsetzbarkeit
  - \+ z.T. hohe Performance
  - \+ „natürlich“ integrierbar ins LAN, d.h. ACLs auf vorhandenen Backbone-Interfacen oder dedizierte FW-Systeme als Bridge oder Router in Verkehr eingebunden oder als Add-On-Software-Installation auf Endsystemen
- kombinierbar mit Proxy-Diensten und Application-Gateways (s.u.)

Application-Gateways und Proxies



Application-Gateways und Proxies

- Proxy-Server führen stellvertretend die Verbindung innerer Systeme nach „Außen“ durch
- bei Bedarf: Firewall erlaubt nur Kommunikation der Proxy-Server mit „Außen“
- Proxy-Server für viele Dienste (HTTP, SMTP, NTP, FTP, ...)



Application-Gateways und Proxies

- konzentrieren die Sicherheitsfunktionen auf einen Übergang
- entkoppeln die Netze (mit Vor- und Nachteilen, s.u.)
- auch „Standard-Server“ können Application-Gateway mit Sicherheitsfunktionen sein, z.B.
  - Terminal-, SMTP-, POP3/IMAP-Server
- können Inhaltsfilterung zentral durchführen und massiv in Anwendungsprotokolle eingreifen

Application-Gateways und Proxies

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

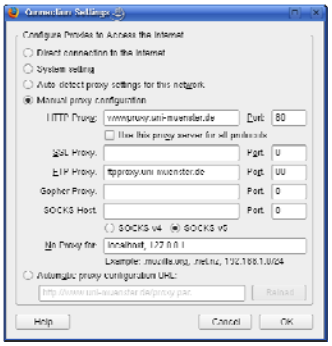
- Vorteile
  - Logging, Accounting
  - oft User-Level Authentifizierung möglich
  - oft Caching möglich
  - (unsichere) Endnutzer-Systeme kommunizieren nicht direkt mit „Außen“
  - verbergen der Intranet-Struktur
- Nachteile
  - nicht alle Dienste haben Proxy-Versionen
  - ggf. eigener Proxy-Server für jeden Dienst
  - ggf. Modifikationen an Endsystemen (Clients) nötig
  - eingeschränkte Flexibilität
  - ggf. eingeschränkte Performance
  - Aufwand

Proxy-Szenarien

ZENTRUM FÜR INFORMATIONSVERARBEITUNG

- Proxy-taugliche Anwendungssoftware
  - die Anwendungen auf den End-systemen enthalten Proxy-Clienten, die die Proxy-Server (automatisch) anstatt der eigentlichen Ziele ansprechen

Beispiel: Mozilla-Firefox Web-Browser:



- Proxy-taugliche Betriebssysteme
- Proxy-taugliche Router oder Firewall
  - der Router oder die Firewall blockiert direkte Verbindungen und führt Redirects auf zugehörige Proxy-Server durch
  - für Nutzer transparent (keine Änderung an Endsystemen)

Varianten und Begriffe

- Circuit-Level-Proxies
  - Port-Relays (TCP-Wrapper), Port-Proxies – NAPT
  - keine Analyse auf Applikations-Ebene (Nutzdaten)
  - bis Layer 4
- Application-Level-Proxies
  - „verstehen“ Applikation, Analyse bis in die Nutzdaten
  - komplexe anwendungsspezifische Sicherheitsziele umsetzbar
  - bis Layer 7
- Permit-Proxies
  - in Verbindung mit Circuit- oder Application-Proxies: Authentifizierung *vor* benutzerspezifischer Port-Freischaltung (z.B. über HTTPS-GUI)

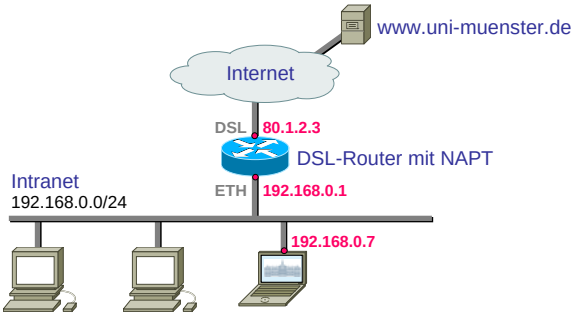
Hybride Systeme

- Kombination von Funktionen in einem Produkt
  - Router
  - stateful Packet-Inspection
  - Application-Gateways und Proxies
  - zusätzliche Funktionalitäten (s.u.)
- manche komplexe Firewall-Produkte und -Lösungen beinhalten einige zusätzliche Funktionalitäten, z.B.
  - VPN-Einwahl
  - Content-Filterung
  - Authentifizierung
    - in Kopplung mit lokalen Authentifizierungs-Servern
  - Virenscanner
  - Denial-of-Service (DoS) Schutz
  - Überwachung von Protokoll- und Anwendungs-Konformität

Network-Address-Translation (NAT)

in aller Kürze:

- NAT (NAPT, PAT) erlaubt intern die Verwendung anderer (privater) IP-Adressen als am externen Internet-Zugang
- NAPT ist notwendig, wenn mehr interne Systeme als zur Verfügung stehende „öffentliche“ IP-Adressen mit dem Internet gleichzeitig kommunizieren sollen
- einfaches Beispiel (Heim-Netz mit DSL-Router):



Network-Address-Translation (NAT)

- NAT, NAPT bzw. PAT sind im eigentlichen Sinne keine Firewall-Techniken, haben jedoch ähnliche Wirkung:
  - verbergen interne IP-Adressstruktur
  - unterbinden Verkehr von außen, wenn er kein Rückverkehr bzgl. von innen aufgebauter Verbindungen ist
  - erlauben Rückverkehr nur in bestimmten Zeitfenstern
- Nachteile:
  - Ende-zu-Ende Konnektivität nicht gegeben
    - Verbindungsaufbau von „Außen“ eingeschränkt
  - eingebettete IP-Adressen und portagile Applikationen problematisch
    - spezieller Support für solche Anwendungen nötig (z.B. FTP)
  - Verschlüsselung und Integritäts-Überprüfung kann durch notwendige IP-Header-Veränderungen fehl schlagen
    - IPsec: NAT-Traversal um Problem zu umgehen (einpacken der originalen IPsec-Pakete in UDP-Pakete)

Firewall-Topologien

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

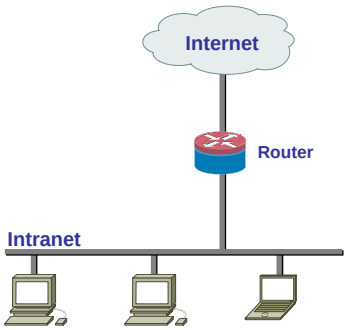
Beispiele von Basis-Topologien:

- Screening-Router
- Dual-homed Bastion-Host
- Screening-Router mit Application-Gateway
- Screened Subnet (DMZ)

Screening-Router

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

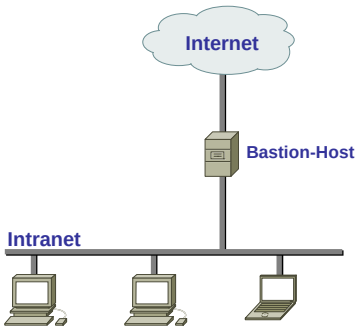
- Router mit Firewall-Funktionalität
  - stateless Packet-Screens (ACL)
  - statefull Packet-Inspection
  - NAT / NAPT



- einfachstes Szenario
- Application-Layer-Gateway (ALG) fehlt
- preiswert
- unflexible
- typisch für Heim-Netz

Dual-homed Bastion-Host

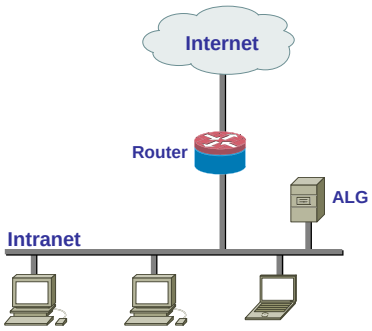
- Bastion-Host *(absichtlich außen und somit Angriffen besonders ausgesetzter Rechner = Vorwerk = Bastion*) mit zwei Anschlüssen in unterschiedlichen Netzen (dual-homed) als Application-Gateway und/oder Paketfilter



- mögliche Szenarien:
  - Bastion-Host routet nicht, sondern nur ALG
  - Bastion-Host ist ALG und Router mit Firewall-Funktionen zugleich
- oft in SW auf Standard-PCs realisiert
- preiswertes Feature-reiches Szenario
- SPoF, Performance

Screening-Router mit ALG

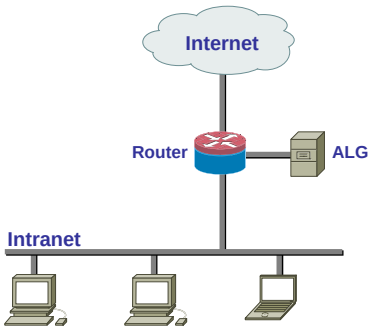
- Router und Bastion-Host (ALG) getrennt
- ALG im Intranet installiert
- Router erlaubt bestimmte Verbindungen nur via ALG



- kombiniert (preiswerten) (performanten) Router mit erweiterter Sicherheit über ALG
- falls Bastion-Host (ALG) gehackt wird, ist Angreifer schon im Intranet

Screening-Router mit ALG

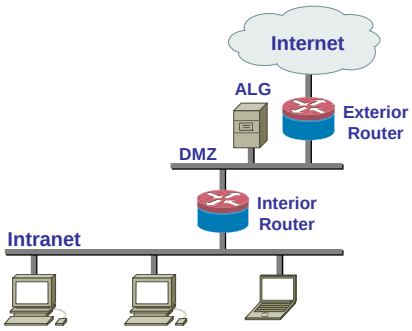
- Variante: ALG direkt am Router an Extra-Interface angeschlossen



- bessere Lösung als ALG im Intranet
  - besserer Schutz vom/zum Intranet
  - eigene Interface-ACLs
- aufwendiger: mehr geroutete Interface am Router nötig (teurer)

Screened-Subnet (DMZ)

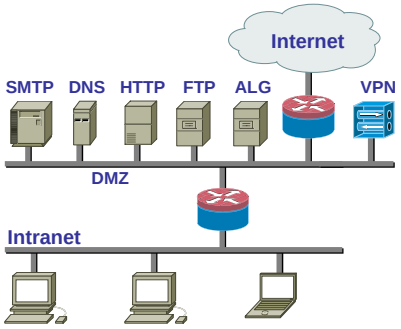
- eigenes überwachtes Teilnetz (Screened Subnet) für Server und Gateways für Kommunikation mit draußen
- auch DMZ (De-Militarized-Zone) genannt



- für Angriffe aufs Intranet müssen beide Router überwunden werden
- DMZ leicht erweiterbar (s.u.)

Screened-Subnet (DMZ)

- viele Gateways und Server für externe Dienste in DMZ-LAN vereint
- „Standard“-Szenario vieler kleinerer bis mittlerer Unternehmens-Netze
- VPN-Gateways für verschlüsselte authentifizierte Einwahl



- flexibel
- relativ aufwendig
- viele Variationen denkbar
  - mehrere DMZ-LANs
  - Dual-homed Bastion-Hosts (z.B. zwischen äußerem und innerem Router)
- Vorsicht: VPN erweitert das zu schützende Netzwerk

Verteilte Firewalls

- in größeren komplexeren Netzen macht es Sinn Firewalls zu verteilen:
  - mehrfache Auslegung eines Firewall-Systems aufgrund
    - Performance
    - Redundanz
  - Absicherung nicht nur zum Internet hin
    - Durchsetzung von Sicherheitsregeln auch im Intranet
    - Absicherung von Intranet-Schutzzonen gegeneinander
  - je nach Anwendungsschwerpunkt Einsatz unterschiedlicher Systeme
    - Features
    - Performance
    - Kosten
    - Managebarkeit
    - Virtualisierbarkeit
    - Netzwerkanbindung (Router/Transparent Bridge)

Personal-Firewalls

- sind auf dem (eigenen) Computer installiert und sollen ihn gegen ungewollten Zugriff schützen
  - von Außen: Einbruchsversuche, Ausnutzung von System-Schwächen, DoS-Angriffen, etc.
  - von Innen: ungewollte offene Ports (Dienste, Services), Abschottung lokaler Schädlinge (Viren), Empfang ungewollter Werbung und Fenster-Popups, etc.
- Beispiele:
  - McAfee Personal Firewall, Norman Personal Firewall, ZoneAlarm, Norton Personal Firewall, ...
  - Betriebssystemeigene Firewalls: Windows XP Firewall, Linux iptables, ...

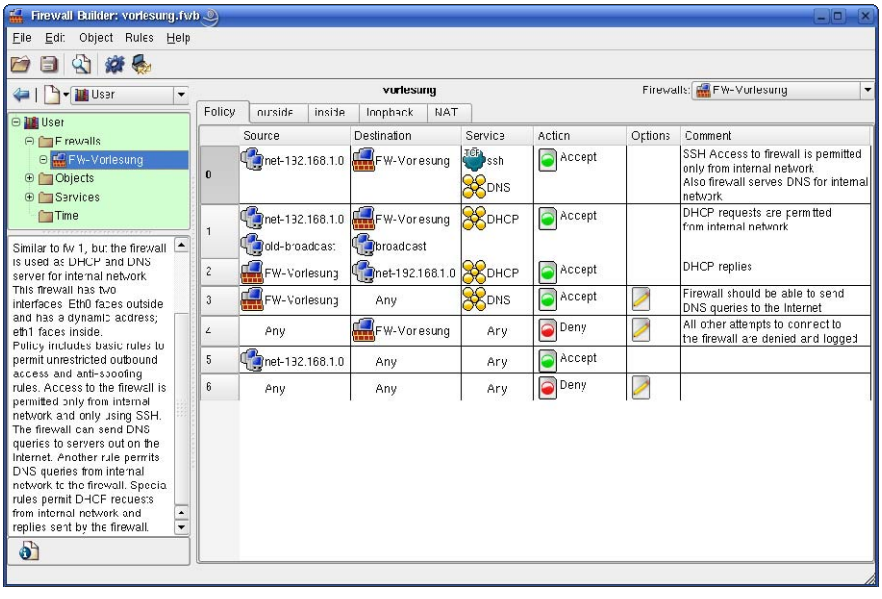
Personal-Firewalls

- Vorteile
  - skalieren
  - anwendungsnah
  - Ausbreitung von Viren kann an der „Quelle“ bekämpft werden
  - Standardkonfiguration bietet Grundschutz: von Innen alles erlaubt, von Außen nur „Rückverkehr“ (ähnlich NAT-Router-Verhalten (s.o.))
- Nachteile
  - häufigstes Problem: Unkenntnis der Nutzer
    - zu Recht: was sind Ports, Dienste, RTP, SMTP, ...?
  - ohne klar definierte Sicherheitskonzepte (Security-Policies) oft untauglich
    - Beispiel: Firewall popt Fenster auf und fragt Nutzer ob „*diese Verbindung*“ erlaubt ist... Damit es weiter geht, werden diese (häufigen) Fragen schnell ungelesen bestätigt
  - prinzipiell unsicher
    - Schutz läuft auf zu schützendem System
    - Fehler im Betriebssystem, Fehler in FW-Software, Bedienungsfehler oder Viren hebeln Firewall aus

Beispiel einer Linux-Firewall

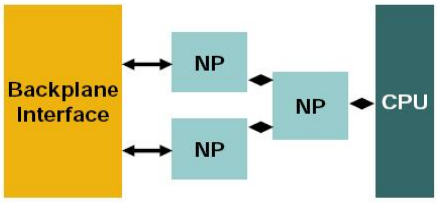
- Software:
  - iptables (www.netfilter.org) Linux-Kernel-Firewall, konfiguriert mit
  - fwbuilder (www.fwbuilder.org) GUI
- fwbuilder liefert mit einer komfortablen GUI gute knappe Regelsätze für verschiedene Systeme, z.B.
  - iptables (Linux), ipfw (FreeBSD), pf (OpenBSD), ipfilter, PIX/FWSM (Cisco)
- generierte Skripte sind ein guter Einstieg in low-level Filterung (z.B. iptables)
- fwbuilder unterstützt zentrales Management vieler verteilter Firewalls

fwbuilder



Firewall Services Module
Quick Recap...

Cisco.com



THE WS-SVC-FWM-1-K9 SUPPORTS THE FOLLOWING...

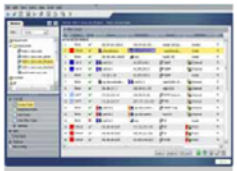
- Fabric line card
- Supported in Cisco IOS and Catalyst OS
- Network-processor based hardware
- Up to 5Gb aggregate throughput
- Up to 3Mpps aggregate performance
- Up to 1M TCP concurrent connections
- Supports dynamic routing (OSPF)
- Up to 100K new connections per second for HTTP, DNS and enhanced SMTP
- Support for 100 Virtual Firewalls
- Transparent Firewall support
- Intra and Inter chassis failover in Active/Standby mode
- Dynamic Routing with RIP and OSPF

RST-2504
9794 05 2004 c2

30

Quelle: http://www.cisco.com/ 45

Cisco Security Manager
Integrated Security Configuration Management

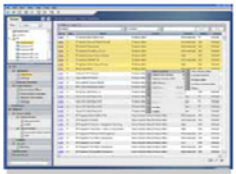


Firewall Management

- Support for Cisco® PIX® Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Firewall Services Module (FWSM), and Cisco IOS® Software Routers
- Rich firewall rule definition: shared objects, rule grouping, and inheritance
- Powerful analysis tools: conflict detection, rule combiner, hit counts, …

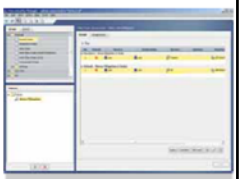
VPN Management

- Support for Cisco PIX Firewall, Cisco ASA, VPN services module (VPNSM), VPN shared port adapter (SPA), and Cisco IOS Software routers
- Support for wide array of VPN technolgies, such as DMVPN, Easy VPN, and SSL VPN
- VPN wizard for 3-step point-and-click VPN creation



IPS Management

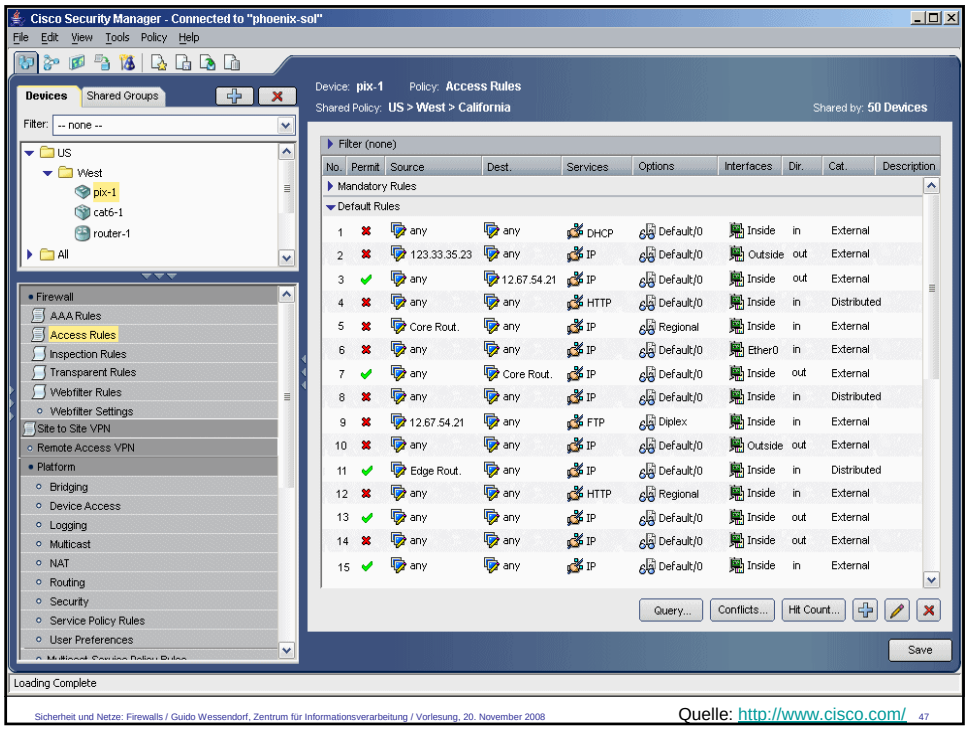
- Support for IPS sensors and Cisco IOS IPS
- Automatic policy-based IPS sensor software and signature updates
- Signature update wizard allowing easy review and editing prior to deployment



Productivity

- Unified security management for Cisco devices supporting firewall, VPN, and IPS
- Efficient management of up to 5000 devices per server
- Multiple views for task optimization
  - Device view
  - Policy view
  - Topology view

Quelle: http://www.cisco.com/ 46

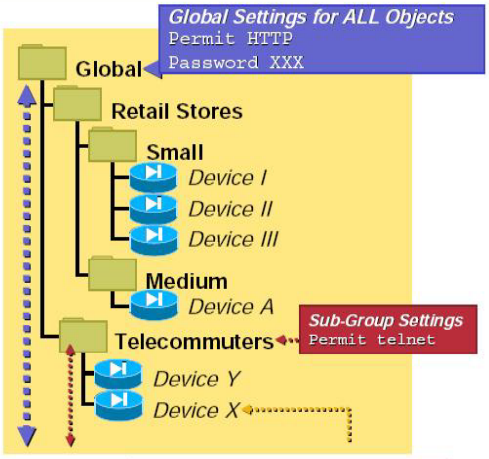


Quelle: http://www.cisco.com/ 47

Flexible Inheritance

Cisco.com

- Grouping reflects organizational structure or common setup
- Parents can MANDATE or DEFAULT Rules/Settings on children objects
- Children objects can
  - Inherit parents' DEFAULT settings/rules
  - Override parents' DEFAULT settings/rules
- Children MUST inherit MANDATED Settings/Rules from parent groups



Device/Net X Settings
Permit FTP
Permit Telnet (inherited)
Permit HTTP (inherited)
Password XXX (inherited)

SEC-2006
9860_05_2004_c1

22

Quelle: http://www.cisco.com/ 48

Workflow

"Enable different management teams to work together"

What Is It?

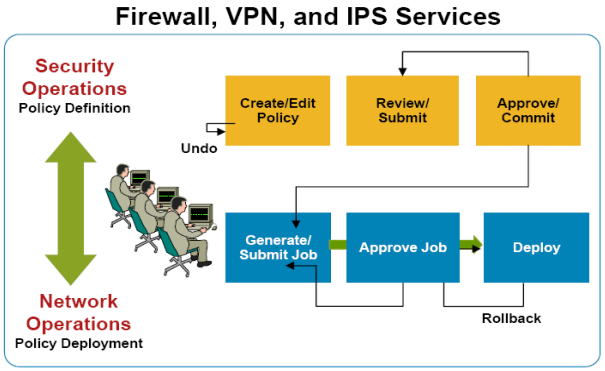
- Structured process for change management that complements your operational environment

Example

- Who can set policies
- Who can approve them
- Who can approve deployment and when
- Who can deploy them

Benefit

- Enables teamwork and collaboration between NetOps and SecOps
- Provides scope of control



Quelle: http://www.cisco.com/

Literatur und Links

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

- Building Internet Firewalls / Chapman, Cooper, Zwicky O´Reilly
- Firewalls and Internet Security / Bellovin, Cheswick, Rubin Addison-Wesley
  - http://www.wilyhacker.com/1e/ (1. Auflage online)
- Guidelines on Firewalls and Firewall Policy National Institute of Standards and Technology (NIST)
  - http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  - http://www.bsi.de/
  - Sicherheitsgateway (Firewall) http://www.bsi.de/fachthem/sinet/loesungen_netze/loesungen_firewall.htm
- Internet Firewalls: Frequently Asked Questions
  - http://www.interhack.net/pubs/fwfaq/
- Wikipedia – Firewall
  - http://de.wikipedia.org/wiki/Firewall