Gibraltar Firewall

Rene Mayrhofer

Linuxday

Klagenfurt, 22. Februar 2005

12:15-13:30

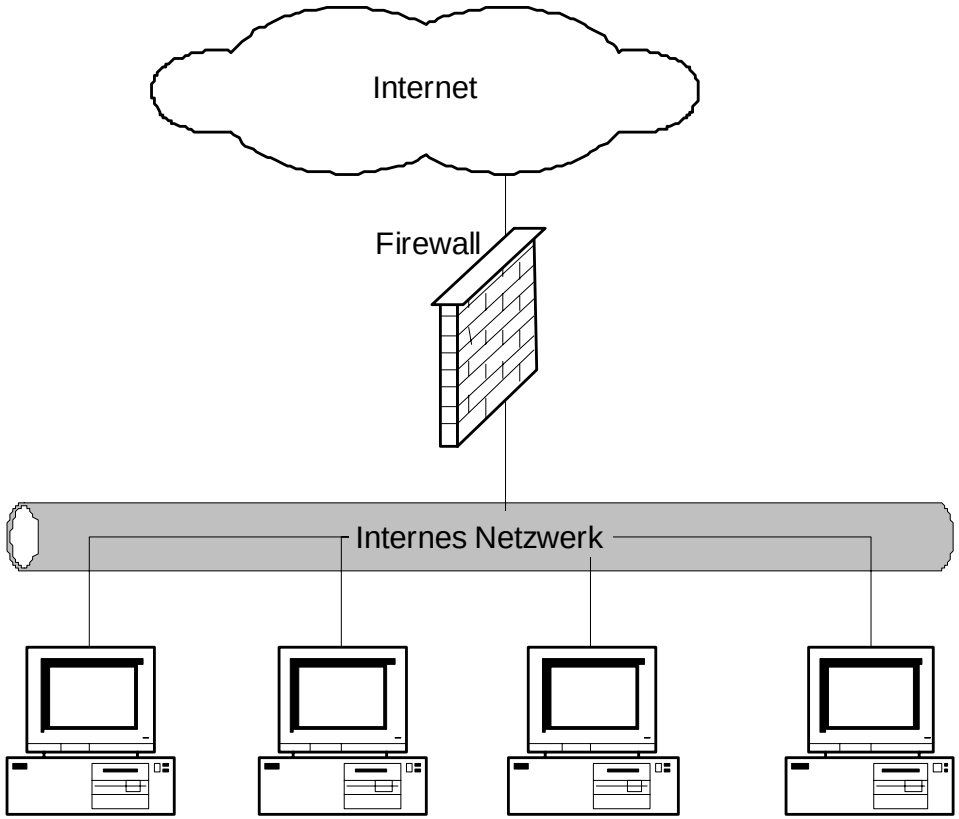
Vortragsinhalt

- Prinzipielle Firewalltechniken und Netzwerktopologien
- Gibraltar
- Praxisbeispiel
- Erweiterte Firewalltechniken
- Diskussion

Einführung in Firewalltechnologien

Firewall, Paketfilter, Proxy-Server, NAT, VPN

Was ist eine Firewall?



Firewall - Grundlagen

- Eine Firewall ist der Schwerpunkt der Sicherheitsmaßnahmen
  - gesamter Verkehr muss Kontrollpunkt passieren
  - Verkehr kann überwacht werden
- Durchsetzen der Sicherheitspolitik
  - verhindert, dass Daten nach außen gelangen
- Protokollierung
  - protokolliert den laufenden Netzwerkverkehr
- Verkleinerung der Angriffsfläche
  - trennt verschiedene Bereiche des Firmennetzwerks
  - DMZ (Demilitarisierte Zonen)

- **schützt nur Verbindungen, die durch sie hindurchgehen**
- schützt nicht / nur bedingt gegen Angriffe von innen
- bietet keinen vollständigen Virenschutz
- kann sich nicht selbst einrichten

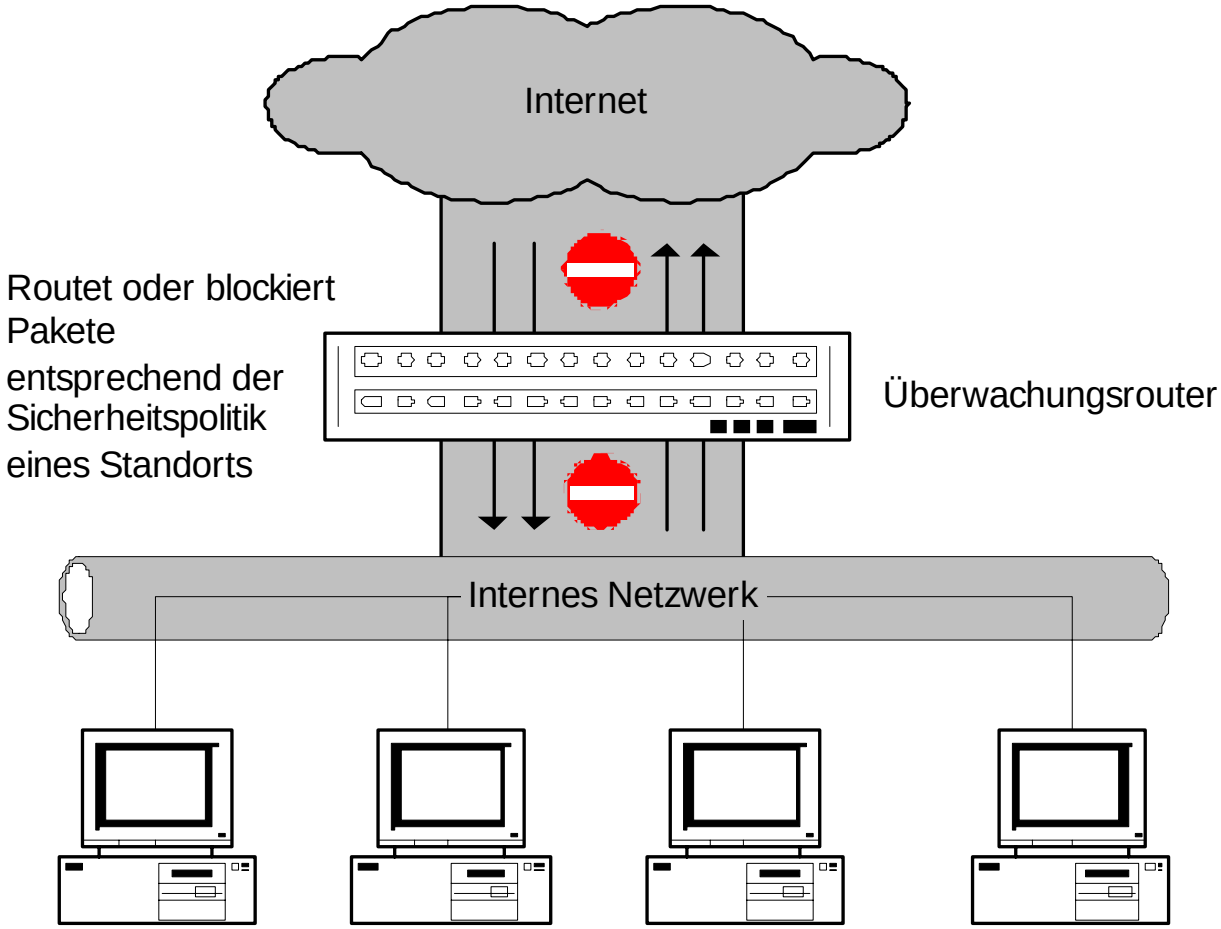
Firewall - Techniken

- **Paketfilterung**: Kern einer jeden Firewall, Umsetzung der Sicherheitsrichtlinien und Überwachung des Netzwerktraffics
- **Proxy-Dienste**: Sicherheits- und Performancefunktion. Application-Level-Inspection, Deep Inspection
- **NAT** (Network – Adress – Translation): Adressübersetzung
- **VPN** (Virtuelle Private Netzwerke): **IPSec**

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations-Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations-Steuerungsschicht		
4	Transportschicht	Transport-Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork-Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network-Access-Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Paketfilterung



Paketfilter

- Paketfilter arbeiten auf Ebenen 3 und 4 des ISO/OSI Schichtenmodells
- routen Pakete zwischen internen und externen Hosts
- arbeiten selektiv
- erlauben und blockieren Pakete

- Paket-Header für IPv4:
  - IP-Quelladresse
  - IP-Zieladresse
  - Protokoll
  - TCP oder UDP-Quellport
  - TCP oder UDP-Zielport
  - ICMP-Meldungstyp
  - Paketgröße
  - ...

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations-Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations-Steuerungsschicht		
4	Transportschicht	Transport-Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork-Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network-Access-Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

Paketfilter

- prinzipielle Unterscheidung in stateless und stateful inspection
- Stateless
  - statische Paketfilterung
  - unabhängig von bereits eingetroffenen Paketen
  - Entscheidung über Aktion (Durchlassen oder Blockieren) für jedes einzelne Paket
- Stateful
  - dynamische Paketfilterung
  - zustandsabhängig
  - untersucht nicht nur den Header eines Pakets, sondern auch den Inhalt
  - beobachtet den Status der Verbindung
  - Kontext-Analyse der Verbindung

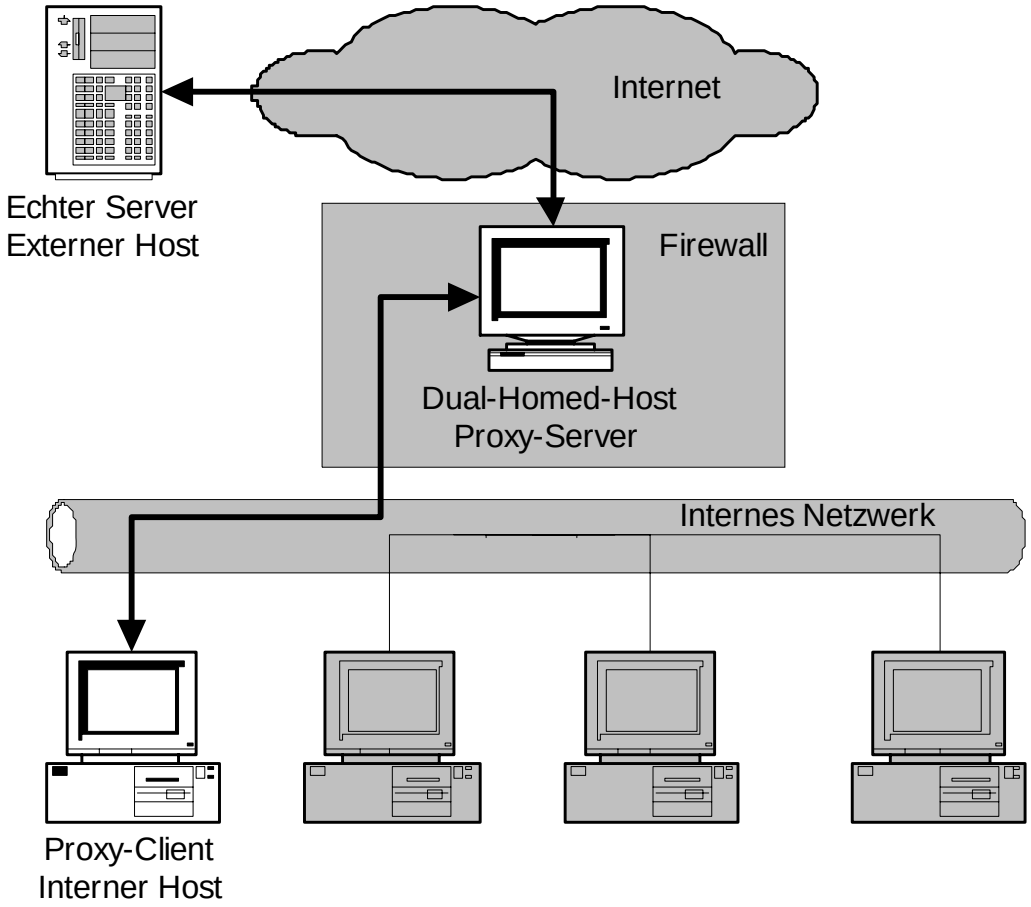
Paketfilter

- bekannte Daten
  - Schnittstelle, an der das Paket empfangen wurde.
  - Schnittstelle, an die das Paket weitergeleitet werden soll.
  - ob das Paket eine Antwort auf ein anderes Paket war **(stateful)**
  - wie viele andere Pakete zuvor zu oder von dem gleichen Host übertragen wurden **(stateful)**.
  - ob das Paket identisch mit einem zuvor gesendeten Paket ist.
  - ob das Paket Teil eines größeren Pakets ist, das in einzelne Teile zerlegt (fragmentiert) wurde (deshalb sehr oft Defragmentierung auf Firewalls, weil die weiteren Fragmente außer dem ersten keinen IP-Header mehr haben).

Paketfilter - Aktionen

- Standard
  - Paket schicken (ACCEPT)
  - Paket verwerfen (DROP)
  - Paket mit Fehlermeldung zurückweisen (REJECT)
  - Informationen über Paket aufzeichnen (LOG)
- Erweitert
  - einen Alarm auslösen
  - Bei stateful: neue Verbindung in Verbindungstabelle eintragen
  - Optionale Zusatzfunktionen: Paket in bestimmter Klasse zählen, Paketgröße zu Quota addieren, Paket in Liste von kürzlich gesehenen Hosts eintragen, ...
  - Paket vor dem Weitersenden verändern !
  - Paket an einen lokalen, transparenten Proxy weitergeben

Proxy - Dienste



Proxy - Dienste

- Proxys arbeiten auf den Ebenen 5 bis 7
- Stellvertreter
- spezielle Anwendungen oder Server-Programme, die Benutzeranfragen an Internet-Dienste entgegennehmen und sie an den eigentlichen Dienst weiterleiten.
- Application-Level-Gateways
- Erhöhung der Sicherheit
- höhere Effektivität des Netzwerks bei caching Proxys
- transparent oder nicht transparent
- Kann für bestimmte Protokolle nötig sein, da Eingriff auf Ebenen 5 bis 7 bei NAT nötig sind (z.B. FTP, H.323)

ISO/OSI – 7-Schichtenmodell

Schicht	ISO/OSI-Modell		TCP/IP-Modell
7	Applikationsschicht	Applikations-Protokolle	telnet, ftp, nfs rlogin, DNS smtp, snmp X-Windows Socket library
6	Präsentationsschicht		
5	Kommunikations-Steuerungsschicht		
4	Transportschicht	Transport-Protokolle	TCP UDP
3	Netzwerkschicht	Internetwork-Protokolle	IP EGP, RIP ICMP ARP, RARP
2	Sicherungsschicht	Network-Access-Protokolle	Ethernet CSMA/CD Token Ring FDDI
1	Bitübertragungsschicht		

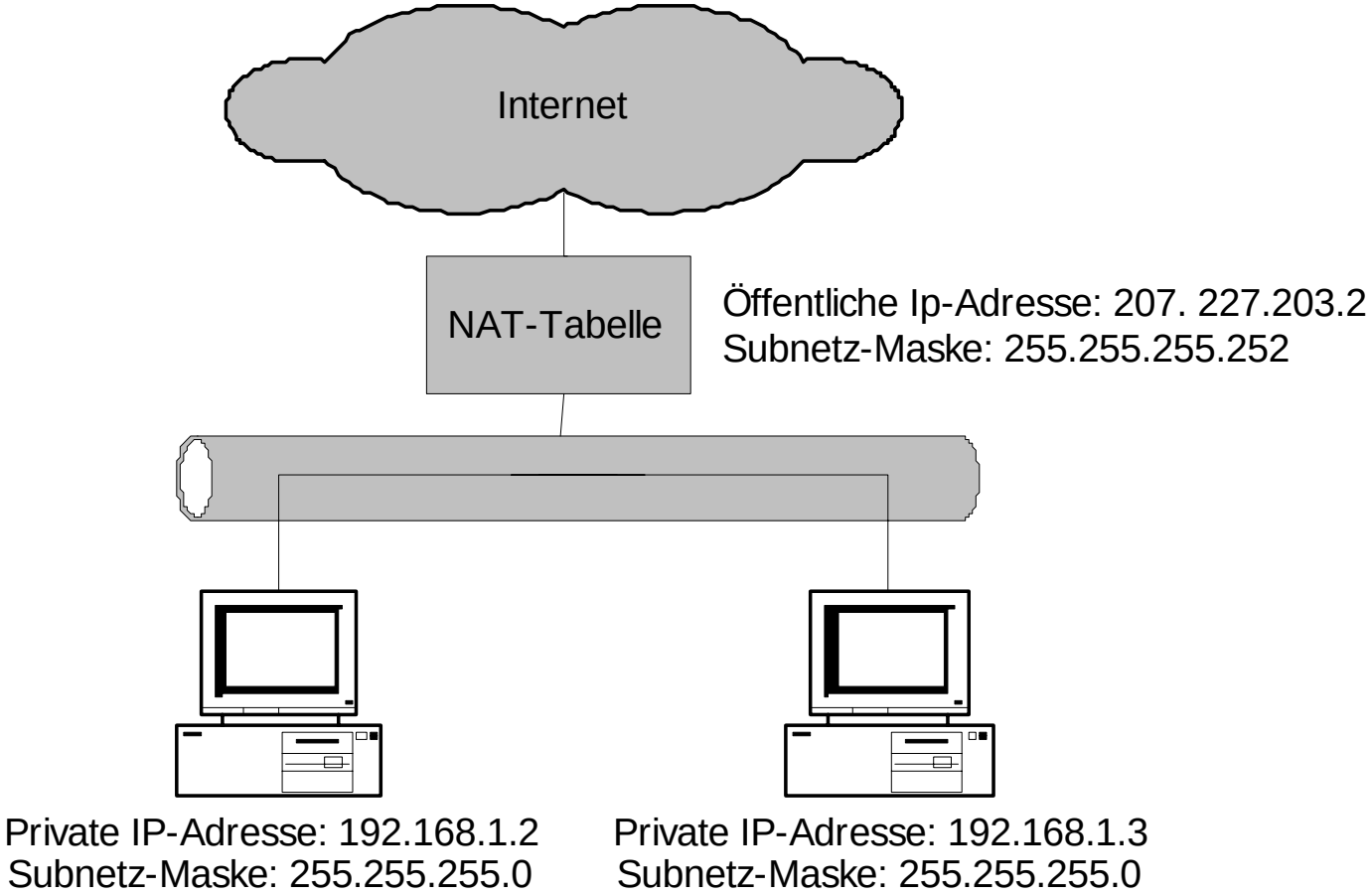
NAT – Network – Address Translation

- Veränderung von Netzwerkadressen
- Router verändert Pakete
  - nach außen: Quelladresse wird verändert
  - nach innen: Zieladresse wird verändert
- Häufigste Anwendung: Masquerading / Maskierung:
  - Problem: Durch IPv4-Adressknappheit wird von Providern oft nur eine einzige IP-Adresse zur Verfügung gestellt, obwohl mehrere Computer angebunden werden sollen
  - Lösung: Interne Rechner bekommen private, im Internet nicht verwendbare Adressen. Bei der Weiterleitung ins Internet ersetzt die Firewall die Quelladresse aller Pakete durch ihre eigene, Antwortpakete gehen daher direkt an die Firewall. Durch interne Zuordnungstabellen können die Antwortpakete an die richtigen internen Rechner weitergeleitet werden.

NAT (2)

- Vorteile
  - NAT unterstützt die Kontrolle der Firewall über nach außen gerichtete Verbindungen
  - eingehender Verkehr kann eingeschränkt werden
  - interne Konfiguration des Netzwerks wird verborgen
- Nachteile
  - ev. Problem mit eingebetteten IP-Adressen
  - Verschlüsselung und Authentifizierung erschwert
  - Protokollierung bei dynamischer Adresszuweisung
  - Dynamische Zuweisung von Ports stört Paketfilterung
  - Diverse Protokolle übertragen IP-Adressen der Clients auf Anwendungsebene (z.B. FTP, H.323) ↯ spezielle Unterstützung muss in NAT eingebaut werden

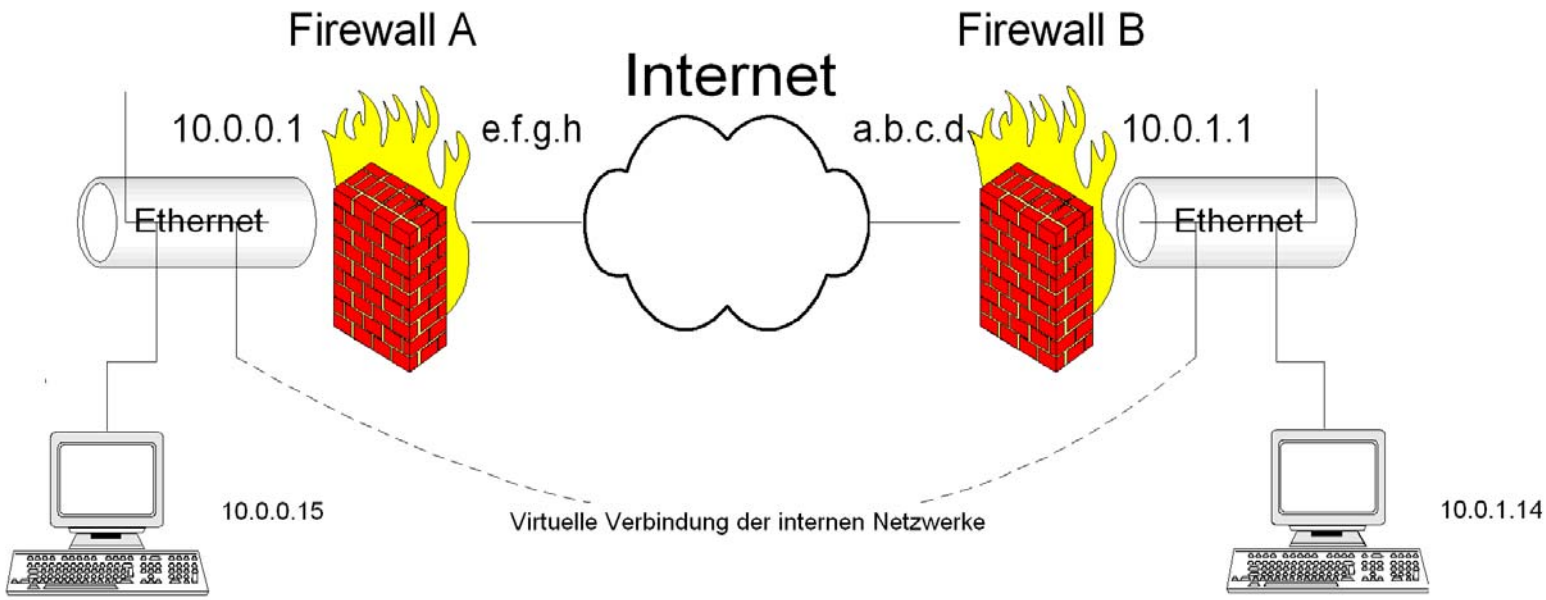
NAT - Beispiel



Virtuelle Private Netzwerke (VPN)

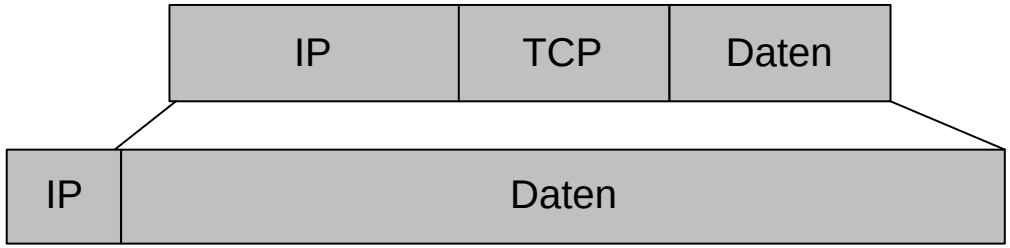
- öffentliches Netz wird privat genutzt
- Verschlüsselung
- Integrität wird geschützt
- Authentizität wird sichergestellt
- Daten werden gekapselt
- Methoden
  - End-zu-End Verschlüsselung
  - Tunnel
- Zeitpunkt der Ver- bzw. Entschlüsselung
  - Behandlung durch den Paketfilter

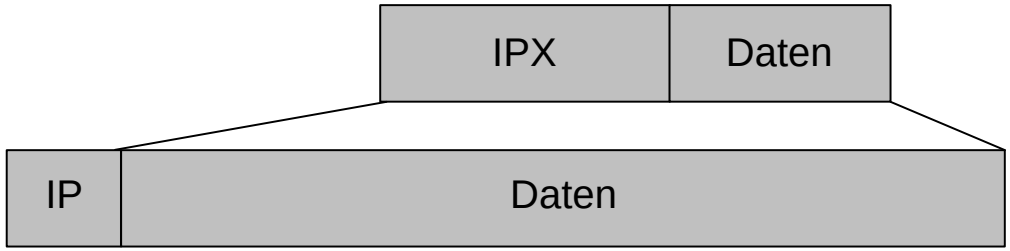
VPN - Prinzip


Firewall A
Internet
Firewall B
10.0.0.1
e.f.g.h
a.b.c.d
10.0.1.1
Ethernet
Ethernet
10.0.0.15
Virtuelle Verbindung der internen Netzwerke
10.0.1.14

VPNs

- Meist im Tunnel-Modus betrieben: Rechner hinter den jeweiligen Gateways können transparent miteinander kommunizieren, obwohl die Gateways keine direkte Verbindung haben
- Methode: „Verpacken“ der Pakete, die zwischen den internen Rechnern ausgetauscht werden sollen in IPv4-Pakete



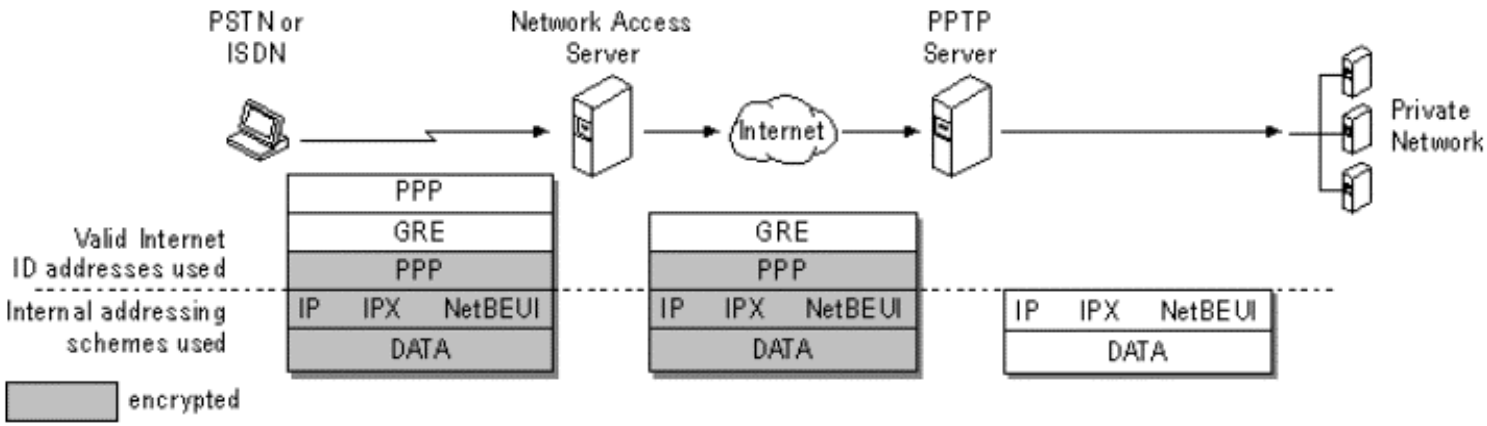


Tunneling

- Verschiedene Implementierungen von Tunneling (Beispiele):
  - GRE (unverschlüsselt)
  - IPv6-in-IPv4 (unverschlüsselt, Übergangsmaßnahme zu IPv6)
  - PPP-over-Ethernet (unverschlüsselt)
  - PPP-over-ATM (unverschlüsselt)
  - L2TP (**unverschlüsselt!**)
  - PPTP
  - **IPSec**
  - OpenVPN
  - VTun
  - CIPE
  - Tinc
  - ....

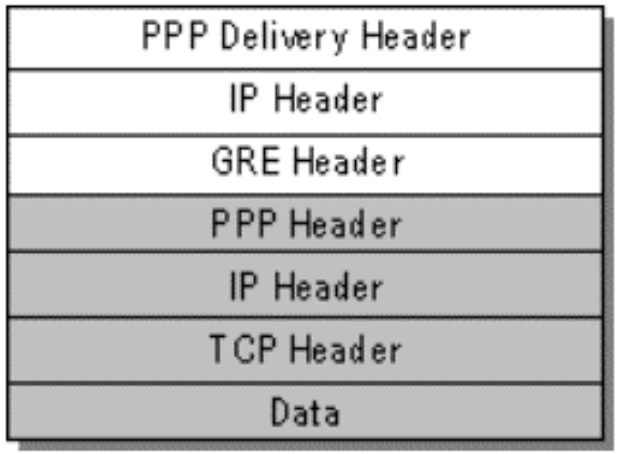
PPTP

- Von Microsoft entwickelt, zur IETF-Standardisierung eingereicht
- Kombiniert GRE-Tunneling mit PPP, um beliebige Protokolle (nicht nur IP) im Tunnel transportieren zu können
- Authentifizierung durch PPP (typisch Benutzername/Passwort)
- Optionale Verschlüsselung auf GRE-Paketebene



PPTP (2)

- Signifikanter Overhead wenn IP im Tunnel transportiert werden soll: Beispiel PPP-Dialin mit PPTP-Tunnel



- UNSICHER !

IPSec

- IETF-Standard (International Engineering Task Force)
- Garantiert Interoperabilität zwischen Herstellern (zumindest theoretisch)
- Gilt in der Wissenschaft als sehr sicher, **keine bekannten Angriffe**
- Ursprünglich für IPv6 entwickelt, dann für IPv4 adaptiert
- Für IPv6 Implementierungen ist IPSec-Unterstützung „vorgeschrieben“
- Allerdings: komplex !

- IPSec
  - definiert in 12 verschiedenen RFCs, Erweiterungen in eigenen RFCs (z.B. NAT Traversal, Dead Peer Detection, etc.)
  - entwickelt 1998

IPSec - Modes

- Protokolle: AH und ESP
- Modes: Tunnel und Transport-Mode
- Kombination aus Protokoll und Mode
- Transport-Mode:
  - AH und ESP schützen den Transport-Header. Pakete werden zwischen Netzwerkschicht und Transportschicht abgefangen
- Tunnel-Mode
  - wird verwendet, wenn Endziel des Pakets nicht dem Ende der gesicherten Verbindung entspricht
  - VPNs
  - IPSec kapselt IP Pakete mit IPSec Headern

IPSec - Modes

Transport Mode IPSec	**Tunnel Mode IPSec**
Applikation	Applikation
TCP, UDP oder anderes IP Protokol	TCP, UDP oder anderes IP Protokol
IPSec Security Layer	Innere IP Addresse (das wirkliche Ziel das Pakets nach dem IPSec Gateway)
IP Addresse	IP Security Layer
Data Layer	Äußere IP Addresse (IPSec gateway or firewall)
Physical Layer (Hardware)	Data Layer
	Physical Layer (Hardware)

IPSec

- Authentifizierung zwischen Hosts anstatt Benutzerauthentifizierung wie bei PPTP
- Authentifizierung über:
  - Preshared Keys (PSK)
  - X.509 Zertifikate
- X.509 Zertifikate bieten viele Vorteile:
  - Bessere Skalierbarkeit für viele Tunnel (bei N Teilnehmern nur N Zertifikate anstatt N * (N-1) Keys)
  - Integration in PKI (z.B. CRL)
  - Sehr gute Unterstützung von „Road-Warriors“, da Zertifikate nicht auf Gateway installiert werden müssen, CA-Zertifikat genügt ❥ Einrichtung neuer Zugänge ohne Umkonfiguration des IPSec-Gateways
- Aber: oft problematisch bei verschiedenen Implementierungen

IPSec - Kompatibilität

	PSK	RSA	X.509	NAT-Traversal	Manual keying
Gibraltar Firewall (FreeS/WAN)					
FreeS/WAN					
Open BSD					
Kame (FreeBSD, NetBSD, MacOSX)					
McAffee VPN was PGPnet					
Microsoft Windows 2000 / XP					
CheckPoint FW					
Cisco with 3DES					
F-Secure					
Gauntlet GVPN					
IBM AIX					
IBM AS/400					
SonicWall					
Symantec					
Watchguard Firwall					

Vortragsinhalt

- Prinzipielle Firewalltechniken und Netzwerktopologien
- Gibraltar
- Praxisbeispiel
- Erweiterte Firewalltechniken
- Diskussion

Gibraltar Firewall

Geschichte, Prinzip, Vor-/Nachteile

Gibraltar - Entstehung

- Projektbeginn Juli 2000 von Rene Mayrhofer
- 2000 – 2002: permanente Weiterentwicklung, gestützt auf Verbesserungsvorschläge aus der wachsenden Community
- 2002: erste Ideen zu einer kommerziellen Version
- 2/2003: Partnerschaft von Rene Mayrhofer mit der eSYS Informationssysteme GmbH. Start der kommerziellen Entwicklung
- 11/2003: Präsentation der Version 1.0. Erste Version mit Webinterface
- 5/2004: Gibraltar v2
- 11/2004: Gibraltar v2.1
- ca. 03/2005: Gibraltar v2.2

Gibraltar – Zahlen und Fakten

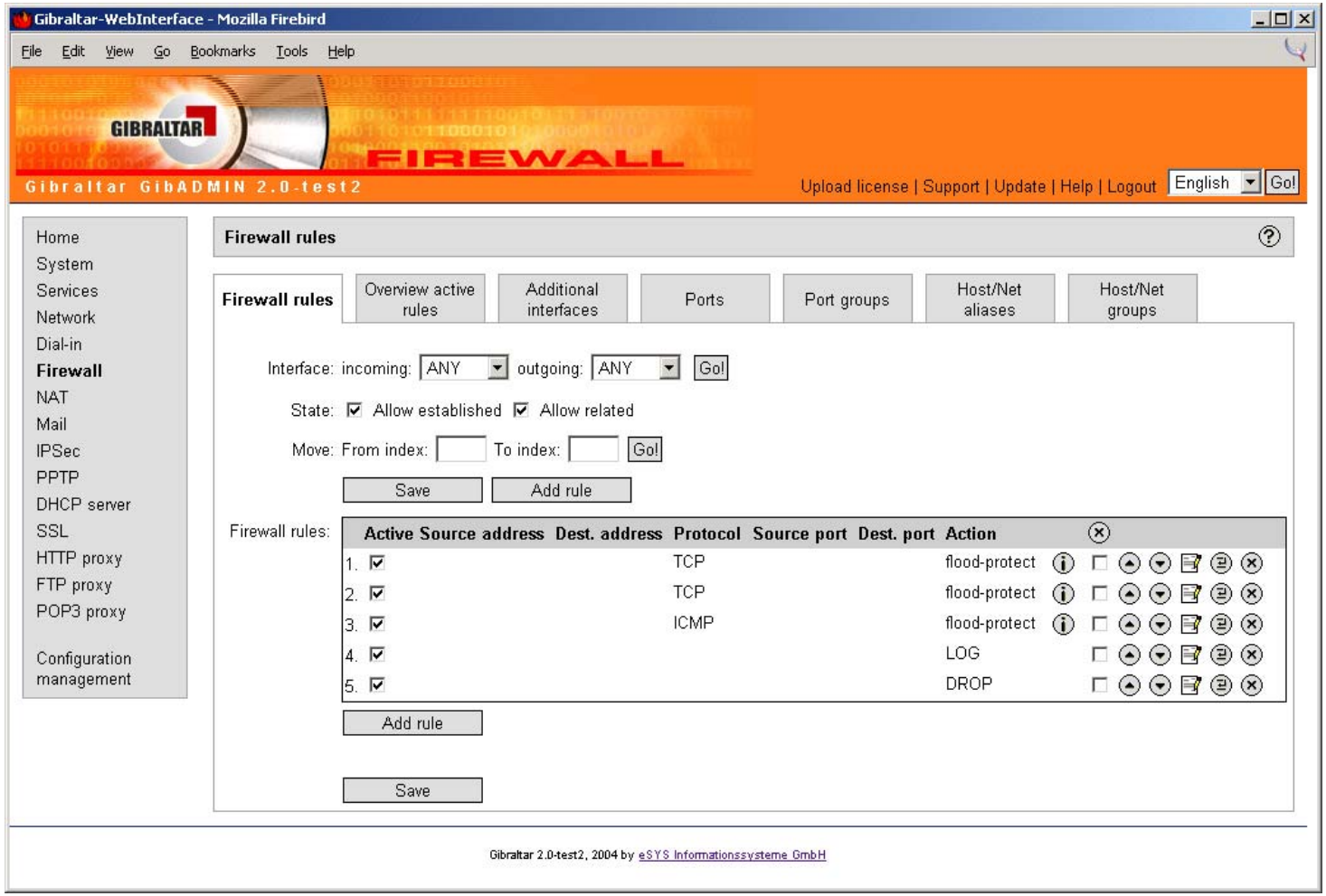
- geschätzte Installationen der freien Version: über 1000
- kommerzielle Installationen (eigene Kunden): ca. 50
- Testinstallationen (Testlizenzen) seit 11/2003: ca. 3000
- tägliche Anzahl von Zugriffen auf Homepage: 600-1000
- Mailingliste: knapp 500 Mitglieder

- seit 11/2004: ca. 20 Vertriebs- und Supportpartner in
  - Österreich
  - Deutschland
  - Schweiz
  - Italien
  - USA
  - Finnland
  - Griechenland

Grundprinzipien

- basierend auf Debian GNU/Linux 3.0 (woody++, demnächst sarge)
- bootet und läuft vollständig von CD-ROM
- minimale Hardwareanforderungen
- vollständig mittels Webinterface konfigurierbar
- sicher durch Verwendung von gängigen Open-Source-Komponenten und Live CD Technology
- Extras
  - Virtuelle Private Netzwerke
  - Kaspersky Antivirus Engine
  - State-of-the-art Spamschutz
  - ab Version 2.3: Failover mit Hot-Standby für hohe Verfügbarkeit
  - ab Version 2.4: Traffic Shaping

Das Webinterface



System

- Live CD Technology: bootet und läuft vollständig von CD ROM
- Keine Festplatteninstallation notwendig
- Speziell gehärteter Linux Kernel
- Sprachen: Deutsch, Englisch, *Finnisch*
- Fernkonfiguration mittels Webinterface oder remote login
- Einfaches Konfigurationsmanagement
- Automatische Live Updates
- Minimale Hardwareanforderungen

Netzwerkunterstützung

- Ethernet 10/100/1000 MBit/s: statisch oder DHCP, virtuelle IP Adressen
- ADSL Ethernet Modems: PPP over Ethernet, PPTP
- ADSL USB Modems: PPP over ATM
- Modem Dial In: Seriell, USB
- Unbegrenzte Anzahl von Netzwerkschnittstellen

Stateful Packet Inspection

- Protokollunterstützung: ICMP, TCP, UDP, GRE, ESP, AH, IPv6-over-IPv4
- Flexibler Paketfilter: Schnittstelle, MAC-Adresse, IP-Adresse, Service, Port,...
- NAT: Network Address Translation
- PAT: Port Address Translation
- Freie Definition von Aliases und Gruppen: Adressen und Ports
- DoS/Flood-Protection: vordefiniert, erweiterbar
- Randomized IP Sequencing
- Gezielte TTL Manipulation
- Protokoll Pass Through: PPTP, FTP, H.323, IRC

VPN (Virtuelle Private Netzwerke)

- IPSec Gateway
- PPTP Server: MPPE 128 Bit Encryption
- Network-to-Network VPN (IPSec)
- Network-to-Client VPN: Kompatibel mit MS Windows 2000/XP (IPSec, IPSec/L2TP, PPTP)
- Unbeschränkte Anzahl von VPN Tunneln
- Authentifizierung mit PSK (Private Shared Key) und X.509 Zertifikaten
- Verschlüsselung: 3DES, Blowfish, Serpent, Twofish, CAST, AES
- Authentifizierung PPTP / L2TP: CHAP, MS-CHAPv1, MS-CHAPv2
- NAT traversal
- Perfect Forward Secrecy (PFS)

GIBRALTAR

Deep Inspection Firewall

- Secure SMTP Relay: eingehend, ausgehend, Attachment Blocking, Block Lists, Viren- und Spamschutz postfix (+TLS+IPv6+SASL++)
- Transparenter HTTP Proxy: keine Clientkonfiguration notwendig, Spamschutz squid (+erweiterte Filter-Patches)
- User Authentifizierung: Benutzerliste, Active Directory Integration, LDAP
- Content Caching
- Content Scanning: Antivirus, Cookies, JavaScript, Active X
- URL Filter
- FTP Proxy: transparent ausgehend, eingehend SuSE ftp-proxy + frox
- Transparenter POP3 Proxy: Antivirus, Spamschutz, und Schutz vor gefährlichen Attachments p3scan

Zusatzdienste

- DHCP Server dhcpd 3
- Secure DNS Resolver djbdns
- SSL Wrapper für beliebige TCP Dienste sslwrap
- Portscan Detection psad
- Anti Spam Filter: spamassassin über amavisd-new
  regelbasiert, Bayes, RBL, Razor und DCC, SPF
- ClamAV Virenscanner
- Kaspersky Virenscanner
- In Entwicklung: Failover mit Hot-Standby heartbeat mit Erweiterungen zur Replikation der Connection-State Tabelle

Vorteil gegenüber Hardware-Lösungen (Watchguard, Sonicwall, Cisco, Zyxel,...)

- Preis
- Skalierbarkeit
- Flexibilität
- Erweiterbarkeit
- Sicherheit durch Open Source
- Sicherheit durch Live-CD-Technology

Vorteile gegenüber Softwarepaketen (Astaro, Checkpoint, Smoothwall,...)

- Preis
- Einfache Installation
- Sicherheit durch Live-CD-Technology
- Keine Festplatte notwendig
- Höhere Ausfallsicherheit

Facts

- Gibraltar ist nicht dauerhaft angreifbar: durch physisch schreibgeschütztes System ist es nicht möglich, sogenannten „malicious code“ dauerhaft zu plazieren
- Gibraltar ist ausgereift: seit dem Jahr 2000 wird Gibraltar weltweit von Linux-Experten verwendet, getestet und weiterentwickelt. Gibraltar verwendet tausendfach getestete Komponenten, deren Quellcode frei verfügbar ist.
- Gibraltar reduziert das Spam-Aufkommen um ca. 95%: durch die Kombination mehrerer Anti-Spam-Maßnahmen (RBL-Listen, Inhaltsanalyse, Bayes-Filter, Razor, DCC, SPF, …) kann Gibraltar wirksam Spam-Mails erkennen und darauf reagieren.
- Gibraltar ist skalierbar und flexibel: je nach Anforderung kann geeignete Hardware verwendet und auch erweitert werden. Gibraltar unterstützt Load-Balancing und Fail-Over.

Gibraltar – Referenzen

- Universität Washington
- Universität Linz
- Fachhochschule Kufstein
- Technikum Wien
- Doubrava
- COPYright by Josef Schürz
- Kirsch – Muchitsch und Partner
- Finadvice Financial Adivsory GmbH
- Ebnerbau Mondsee
- Prävital
- HGS Unternehmensberatung
- Profactor Steyr
- Datacontact
- CARE Österreich
- …

Vortragsinhalt

- Prinzipielle Firewalltechniken und Netzwerktopologien
- Gibraltar
- Praxisbeispiel
- Erweiterte Firewalltechniken
- Diskussion

Gibraltar Firewall Praxisbeispiel

Einrichtung Netzwerk, Firewall-Regeln, VPN

Vortragsinhalt

- Prinzipielle Firewalltechniken und Netzwerktopologien
- Gibraltar
- Praxisbeispiel
- Erweiterte Firewalltechniken
- Diskussion

Erweiterte Firewall-Techniken

Layer2 vs. Layer3 vs. Layer7 Firewalls

Mögliche Ebenen für Filterung

- Erinnerung: ISO/OSI Schichtenmodell bietet verschiedene Punkte zum Filtern von Netzwerkverkehr

- Für Firewalls interessant sind:
  - Layer 2: sog. “Bridging” Firewalls, auch als “transparente” oder “unsichtbare” Firewalls beschrieben
  - Layer 3: “normale” Firewalls
  - Layer (5 –) 7: “Deep Inspection” / “Content Inspection” / “Intelligent” / “Smart” / (hier bitte das aktuelle Marketing Buzz-Word der Woche einsetzen) Firewalls

Layer 2 Firewalls

- Firewall funktioniert wie Bridge, d.h. die angeschlossenen Ethernet-Segmente sind transparent auf Ethernet-Ebene miteinander verbunden
- Allerdings: nicht jedes Paket wird weitergeleitet, sondern es wird nach üblichen Firewall-Regeln gefiltert (also z.B. Quell-/Ziel-MAC, -IP, -Port, etc.)

- Vorteile:
  - Kein Routing, also muss auch kein Gateway bei den angeschlossenen Computern eingetragen werden
  - Daher bei bestehenden Netzwerkstrukturen keinerlei Aufwand zur Rekonfiguration – eine Layer 2 Firewall kann als Ersatz für ein Netzwerkkabel „dazwischengesteckt“ werden
  - Firewall selbst benötigt keine IP-Adressen und ist daher über das Netzwerk auch nicht (zumindest nicht direkt!) angreifbar

Layer 3 Firewalls

- Übliche Firewalltechnik, d.h. die Firwall arbeitet wie ein Router
- Mindestens eine IP-Adresse pro Netzwerkschnittstelle
- Angeschlossene Computer verwenden die Firewall als Gateway

- Vorteil: bekannte Struktur

Layer 7 Firewalls

- Einbindung in Netzwerk entweder als Layer 2 oder Layer 3 Firewall
- Untersuchung der Pakete zusätzlich auf höheren ISO/OSI Schichten (Anwendungsschichten 5-7), also im Datenbereich aus Sicht von IP bzw. TCP/UDP ⇒ „Deep Inspection"
- Daher: mehr Information zur Entscheidung ob Paket weitergeleitet oder verworfen/zurückgewiesen werden soll

- Vorteile:
  - Applikationsprotokoll wird in Entscheidung mit einbezogen
    ⇒ mehr Freiraum und Sicherheit
  - Zusatzdienste auf Applikationsebene möglich, die direkt auf den übertragenen Daten arbeiten (applikationsabhängig!)
    z.B.: transparenter Virenschutz (HTTP, FTP, SMTP, POP3, IMAP4, ...), Blockieren von Cookies (HTTP), Blockieren von Javascript etc. (HTTP)
- Nachteile:
  - deutlich höherer Ressourcenbedarf (CPU, RAM, HDD)
  - erhöhte Latenz

Anwendungsbeispiel: transparenter HTTP Proxy

- Möglichkeiten für Layer 7-Transparenz:
  - Direkte Untersuchung der einzelnen Pakete im Kernel (äquivalent zur Prüfung der ISO/OSI Schichten 2 – 4)
    ⇒ Problem der Komplexität
  - Umleitung der Pakete an einen erweiterten HTTP Proxy
    ⇒ besser durch Modularisierung
- Verhält sich so als ob im Web-Client der HTTP Proxy eingetragen wäre, allerdings ohne den damit verbundenen administrativen Aufwand
- Erlaubt im Prinzip beliebige Änderungen an den in HTTP übertragenen Daten, z.B.:
  - Filterung nach erlaubten/unerwünschten URLs (wichtig für öffentliche Zugänge, Schulen, etc.)
  - Transparente Entfernung von Viren (on-the-fly)
  - Benutzerauthentifizierung
  - Entfernung ungewünschter HTML-Tags bzw. Inhalte (ActiveX, JavaScript, Cookies, Pop-Ups, etc.)
  - Beschleunigung durch Caching

Vortragsinhalt

- Prinzipielle Firewalltechniken und Netzwerktopologien
- Gibraltar
- Praxisbeispiel
- Erweiterte Firewalltechniken
- Diskussion

Diskussion

(Fast) jede Frage wird hier versucht zu beantworten...