Firewall

Kontrolliert den Zugriff auf und von einem geschützten Netzwerk

Inhalt

- Ziele
- Konzepte
- Arten von Firewalls
- Paketfilter
- Application Gateway
- Statefull Inspection
- Port Knocking
- Personal Firewall

Wovor gilt es zu schützen ?

- Ausspionieren von Daten auf Systemen durch Einbruch in diese Systeme
- Ausspionieren bei der Übertragung zwischen Systemen (Man in the middle)
- Manipulation von Verbindungen (Übernehmen einer Verbindung mit Hilfe gefälschter Adressen = Spoofing)
- Verhindern der normalen Funktion eines Rechners (Denial of Service Attacke z.B. SYN Flooding)
- ……

  Ransomware, durch Verschlüsselung von Daten

Allgemeine Ziele

- Blockieren unerwünschten Verkehrs
- Weiterleitung eingehenden Verkehrs an interne Systeme
- Verbergen verwundbarer Systeme, welche nicht auf einfache Art gesichert werden können — Portforwarding
- Protokollierung des Verkehrs Netzwerkverkehrs
- Verstecken von Informationen wie Systemnamen, Netzwerktopologie, Netzwerk-Gerätetypen usw.
- Zentrale robuste Authentifizierung — Radius-Server, Remote Authentication Dial-In User Service
- Netzwerkbandbreite beschränken
- Angriffe erkennen
- Verbinden von Standorten und Cloudlösungen — VPN Verbindung, Site2Site Verbindung
- Das Firewall-System muss selbst resistent gegen Angriffe sein — Backups, Shadowcopy, restriktive Schreibrechte gegen Ransomware

VPN - Virtual Private Network
- Administration von Servern, etc. sollte über VPN und nicht direkt über Portfreigaben gemacht werden. Angreifbar!

Firewall-Konzept

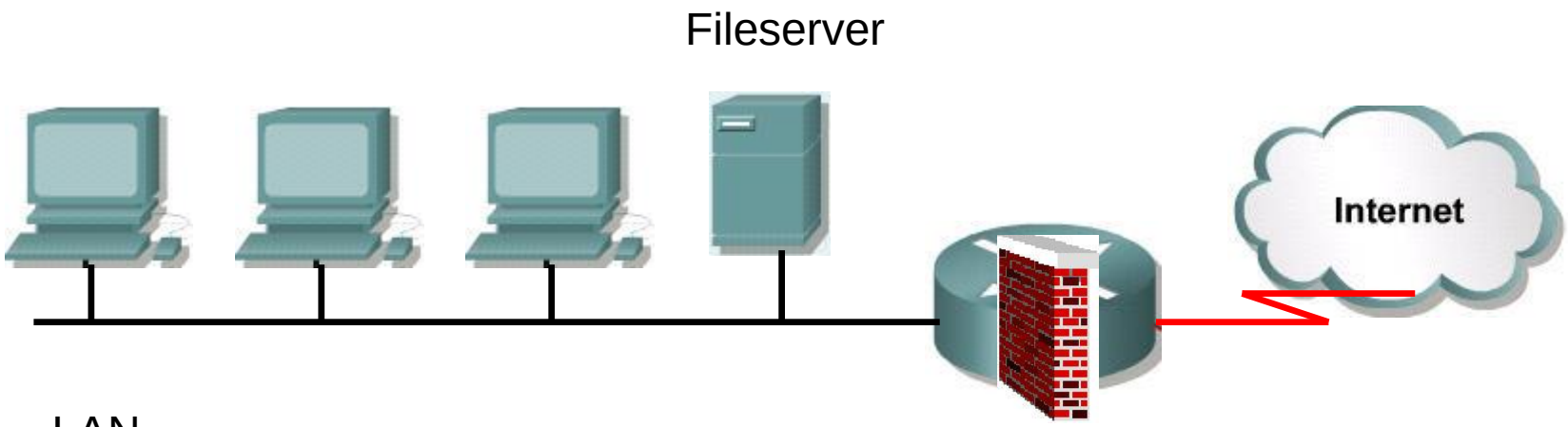
- Ein Firewall-Konzept ist nicht einfach ein Router oder eine Software
- Ein Firewall-Konzept besteht aus einer Reihe von Maßnahmen wie z.B.: SNMP
  - Netzwerkaufteilung mit Serverstandorten (DMZ) Unterteile in VLANs IP-Adresswahl!
  - Router, Server, Firewalls mit spezieller Filtersoftware L3-Switch mit ACLs
  - Sicherheitsrichtlinien AD Group Policy, auch für Admins (kein Internet, Arbeitsstation)!
  - Application-Gateway = Proxy Nicht mer letzter Stand der Technik => Firewall
  - Authentifizierungsmechanismen Radius Server, SSO, LDAP, Federation Service
  - ……. VPN, Standleitung zwischen Standorten, Site2Site-VPN
  - Principle of least privilege „Wenn ma nix duad, seit nix geht“, Wunsch => viel Arbeit

Zentrale Authentifizierung über AD, oder anderen Verzeichnisdienst (OpenLDAP, eDirectory, …)

Firewall Hard- & Software

- **Hardware Lösungen** (bei hohem Datendurchsatz):
  - Fortigate, Barracuda, Sonicwall, ……..
  - Cisco (ASA und FirePOWER)
  - Router mit Paketfilter
- **Softwarelösungen** (flexibel und kostengünstig):
  - oft Linux oder OpenBSD Rechner, auf denen nur das Betriebssystem und die Firewall läuft
  - Application Level Gateway (Proxy)
- **Personal- oder Desktop Firewall**
  - Firewallsoftware am Arbeitsrechner
- **Cloudkonzepte**
  - VPN Lösungen

Einfache Firewall z.B. mit Paketfilter

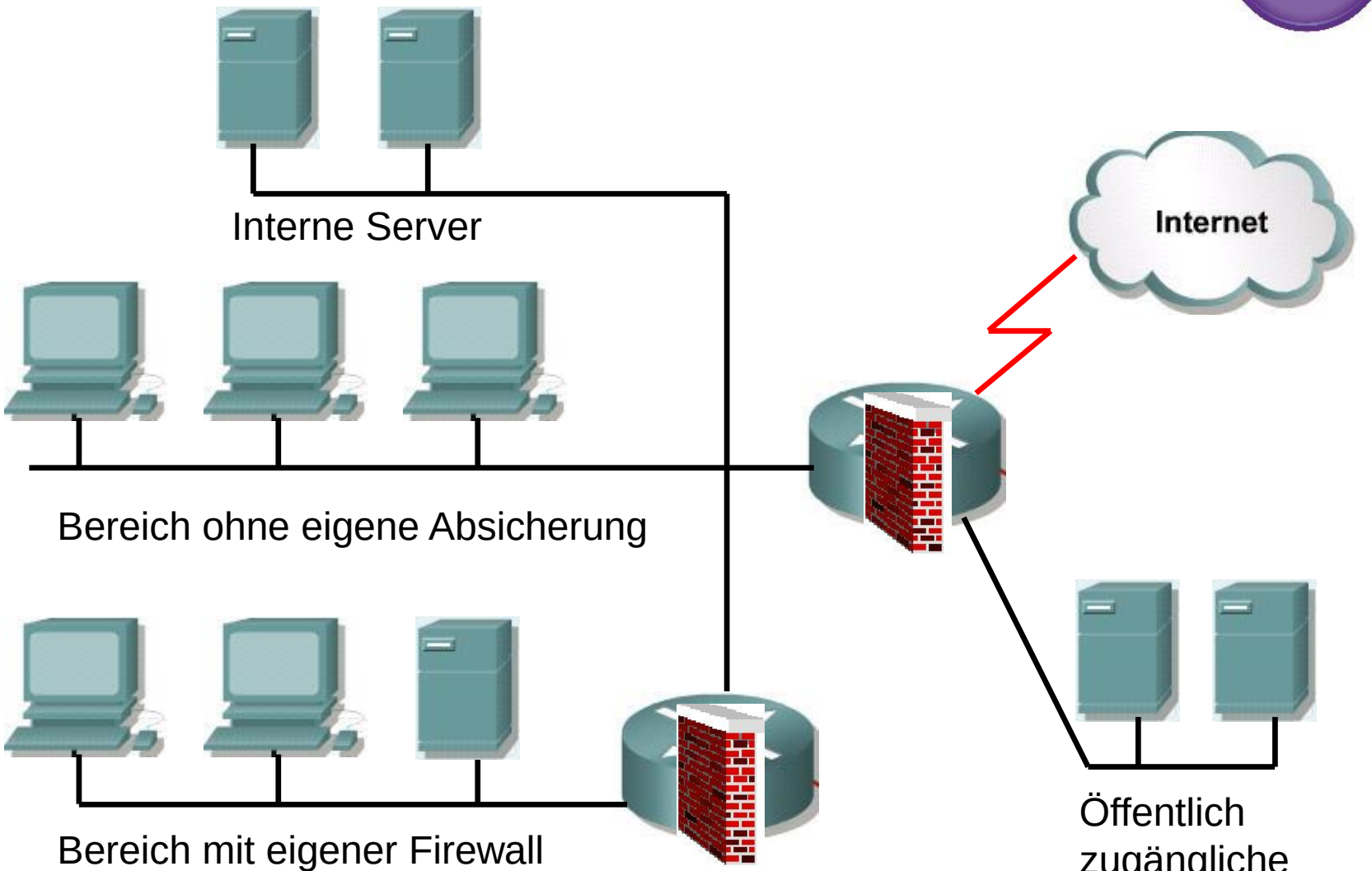


LAN

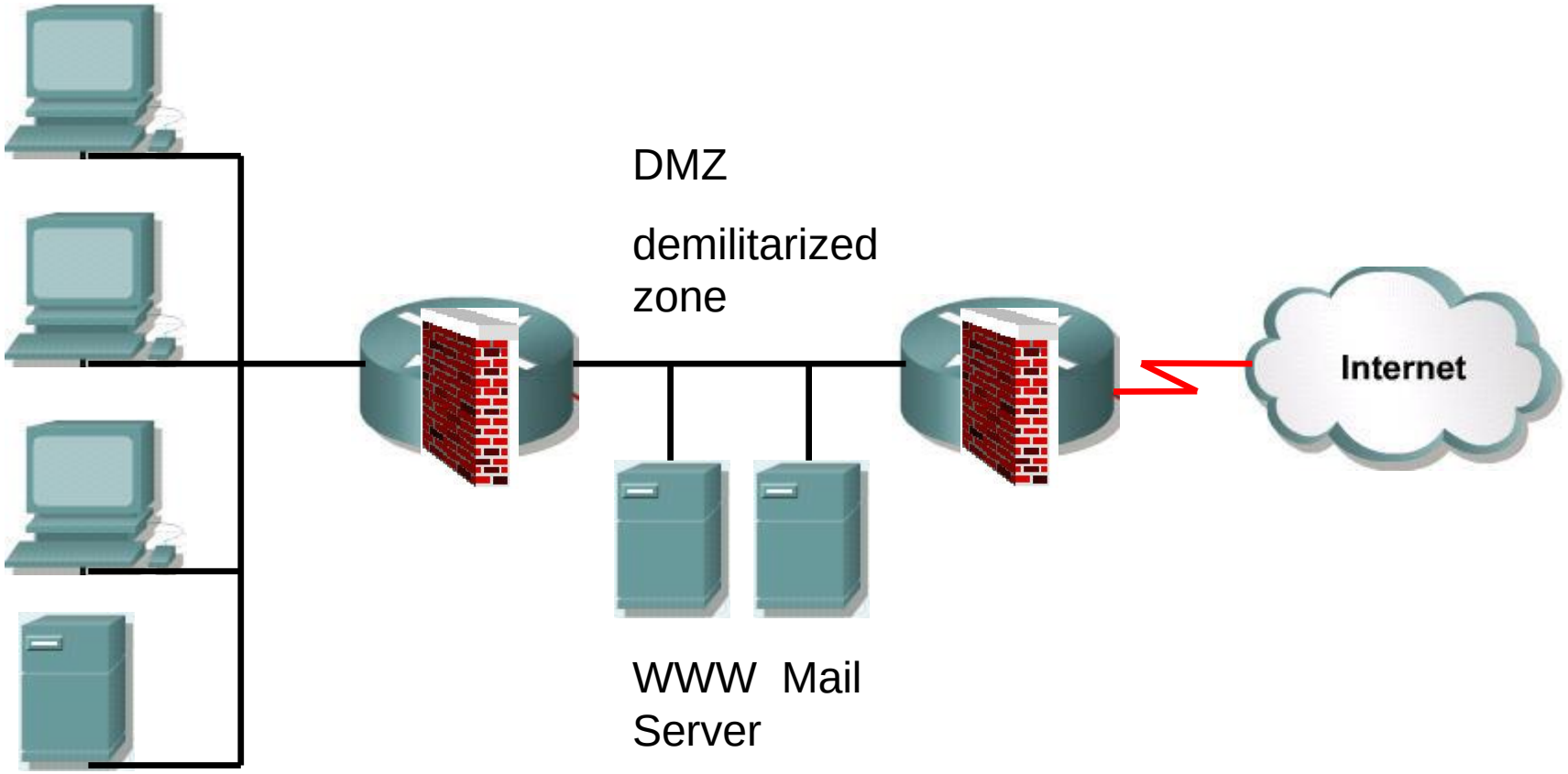
Public NetID (oder private NetID)

Router mit Paketfilter

Gestaffelte Firewall



Kaskadierte Firewall



Paketfilter Firewall

- Ist ein Router, der IP-Pakete zur Unterscheidung zwischen der erlaubten und unerlaubten Nutzung von Kommunikationsdiensten filtert.
- Einfachste und häufigste Lösung
- Der Router bestimmt, welche Pakete passieren dürfen
  - IP Adressen Quelle/Ziel
  - Ports Quelle/Ziel
  - MAC Adressen Quelle/Ziel
  - Protokoll (TCP, UDP, ICMP, ….)
  - Pakettyp siehe Ethernet-Frame
  - Paketlänge
  - Verbindungsaufbau und Zustand (SYN-/ACK-Flag)
  - ….. Frame-Typ, Frame, Protokolltyp, IPX-Frame
- Die Filterregeln sind an die Netzschnittstellen gebunden. Sie werden vom Packet Filter in der Reihenfolge abgearbeitet, in der sie angegeben sind.

Stärken von Paketfiltern

- Paketfilterung ist eine kostengünstige Technologie.
- Paketfilter ist heute auf fast allen Router-Produkten und L3 Switches standardmäßig implementiert.
- Wenig zusätzlicher Administrations- und Konfigurationsaufwand notwendig.
- Paketfiltertechnologie unterliegt keinen US-Exportbeschränkungen wie z.B. Kryptographie- Software
- Sie sind leicht erweiterbar, wenn neue Dienste oder Protokolle transportiert werden müssen (hinzufügen neuer Regeln reicht im Normalfall).

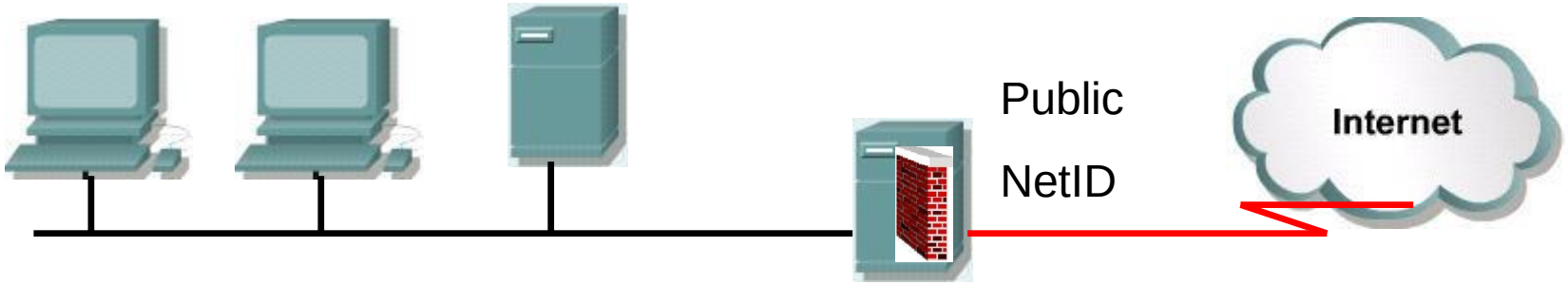
Schwächen von Paketfiltern

- Paketfilterregeln sind für den Durchschnittsbenutzer oft recht verwirrend
- Bei großen Netzen können Filterregeln sehr umfangreich und schwer nachvollziehbar werden
- Protokollmeldungen enthalten oft keine Informationen über Inhalt der übertragenen und verworfenen Pakete
- Einige Protokolle sind für Packet Filter ungeeignet, da variable Portnummern verwendet werden
- Unzureichende Integrität der Portnummern und IP-Adressen, da diese leicht gefälscht werden können (IP-Spoofing)
- Keine Benutzerauthentifizierung
- Keine Kontrolle der Inhalte der Datagramme

Application Level Gateway (Proxy)

- Ist ein speziell konfigurierbarer Rechner, über den die gesamte Kommunikation zwischen dem zu schützenden und dem unsicheren Netz stattfindet.
- Die Verbindung zwischen dem zu schützenden Netz und dem Internet wird völlig entkoppelt
- Ein Application Level Gateway mit zwei Netzschnittstellen wird **Dual-homed Gateway** genannt.

Dual-homed Gateway Firewall = Proxy mit 2 Netzwerkkarten



LAN

private NetID

PROXY

Application Level Gateway

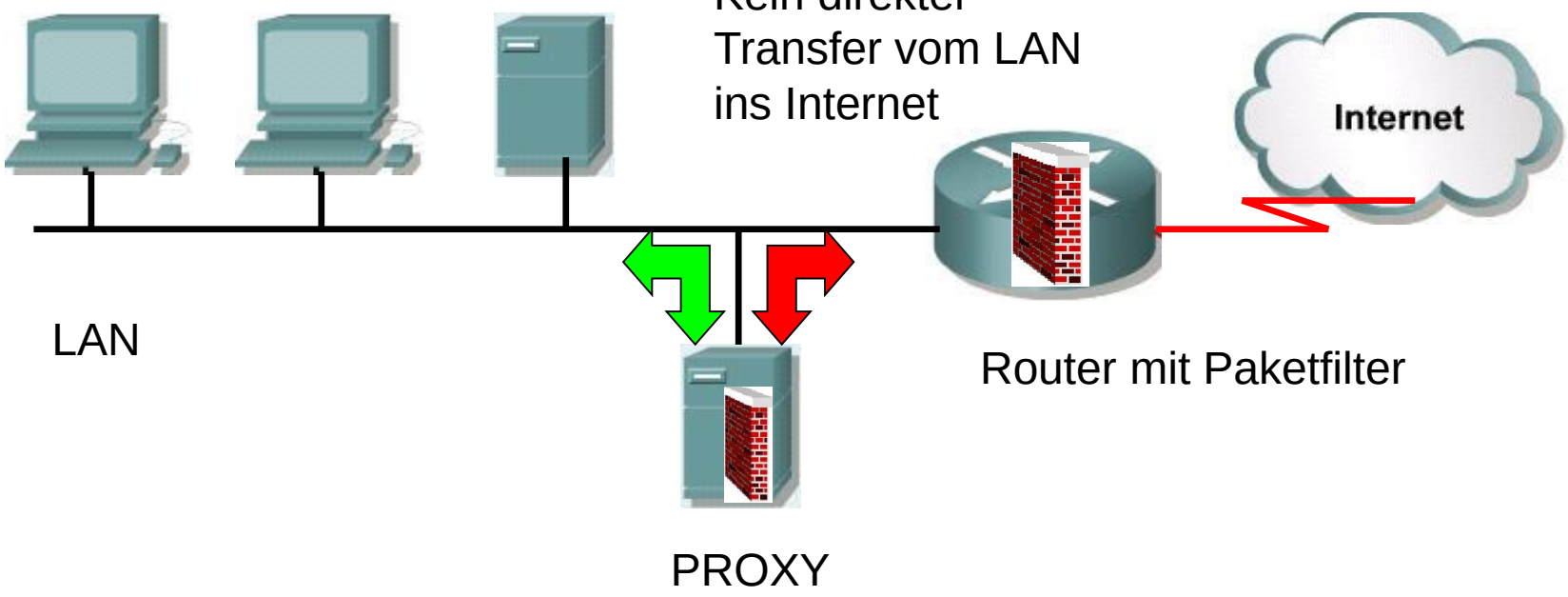
- Die Kontrolle der Kommunikationsbeziehungen findet auf Anwendungsebene statt.
- Für jeden Dienst (Telnet, FTP, WWW, E-Mail,...) werden **Security Proxys** eingeführt, die den direkten Zugriff auf den Dienst verhindern.
- Der gesamte Datenfluss für einen Dienst zwischen dem Firmennetzwerk und dem Internet kann so auf Applikations- und Benutzerbasis kontrolliert werden, z.B. nach bestimmten Schlüsselwörtern durchsucht werden (z.B. E-Mail, HTML-Seite)
- Authentisierung des Benutzers kann vorgenommen werden.
- Dienste können benutzerabhängig erlaubt werden.
- Möglichkeit einiger HTTP-Proxies, alle Zeilen innerhalb einer Seite, die zu Java-Applets gehören, zu löschen.
- Cache Funktionalität für Webseiten
- Genaue Aufzeichnung des ganzen Netzwerktransfers möglich

Screened Gateway

- Die Kombination von Packet Filter und Application Level Gateway wird auch als **Transparent Application Gateway** oder **Sandwich-System** bezeichnet
- Erhöht die Sicherheit der Firewall gegenüber den beiden Einzelkomponenten erheblich.
- Die Anordnung der beteiligten Komponenten kann variieren und erlaubt die individuelle Realisierung eines Firewall-Konzeptes.

Beispiel für Sreened Gateway

In diesem Fall sind z.B. Proxy und Paketfilter getrennt



Stateful Firewall (Inspection)

Beispiel: iptables

- Auch **Stateful Packet Filter** oder **Dynamic Packet Filter**
- Vereinigt die Schutzmöglichkeiten von Packet Filter und Application Level Gateway, so dass diese beiden Funktionen nicht in getrennten Komponenten realisiert werden müssen
- Arbeitet sowohl auf der Netz- als auch auf der Anwendungsschicht.
- Die IP-Pakete werden auf der Netzschicht entgegengenommen, von einem Analysemodul, das dynamisch im Betriebssystemkern geladen ist, zustandsabhängig inspiziert und gegenüber einer Zustandstabelle abgeglichen.
- Die Regeln, nach denen das Modul agiert, können sehr differenziert vorgegeben werden.
- Der Router unterhält eine dynamische Tabelle der aktiven Verbindungen

- Authentifizierung · Sicherungsschicht

Stateful Firewall (Inspection)

↳ NAT → Source- & Destination-NAT (ONAT)

- Für die Kommunikationspartner stellt sich eine Firewall mit Stateful Inspection als eine direkte Leitung dar, die nur für eine den Regeln entsprechende Kommunikation durchlässig ist.
- Für eine bidirektionale Verbindung reicht eine Regel auf Seite des Verbindungsherstellers
- Im Out-Of-Band-Betrieb erfolgt die Wartung und Konfiguration nicht über TCP/IP. Die Firewall besitzt dann keine eigene IP-Adresse, so daß keine Möglichkeit besteht, sie über TCP/IP direkt aus den angeschlossenen Netzen anzusprechen oder auf diesem Wege anzugreifen.
- Optional führt die Firewall ein Rewriting durch, d. h. Pakete werden vor dem Weitersenden nach vorgegebenen Regeln transformiert.

Port Knocking

- Die Firewall öffnet einen Port nur nach einem festgelegten Klopfzeichen (Sequenz von Zugriffsversuchen) durch den Client
- Der Port bleibt dann für eine gewisse Zeit zum Datentransfer offen
- Hilft gegen die meisten Portscans
- Nicht für öffentlich zugängliche Server wie http geeignet

Personal Firewall

- Sind Programme, die auf einem Einzelrechner, z.B für Windows Systeme, als Applikation laufen, der mit einem Netzwerk wie dem Internet verbunden ist.
- Hier ist die Firewall eine Software wie jedes andere Programm auch, die sich auf eine Teilfunktion eines Firewall-Konzepts reduziert, dem Paketscreen / Paketfilter.
- Ermöglicht den Internetzugang für einzelne Programme zu beschränken.
- Sie soll genau wie die normale Firewall den Rechner vor Angriffen von außen schützen.
- Verhindert, dass bestimmte Programme, zum Beispiel so genannte Spyware, Kontakt vom PC zum Internet aufnimmt.
- Kontrolliert dazu alle Verbindungen in andere Netzwerke und überprüft sowohl die Anfragen ins Internet als auch die Daten, die zum Rechner kommen.

Personal Firewall Nachteile

- Trügerische Sicherheit
- Applikationen können sich „tarnen“, z.B. eingebetteter Internet Explorer
- Firewall kann „ausgeschaltet“ werden
- Oft schlechtes Logging / schlechte Reports

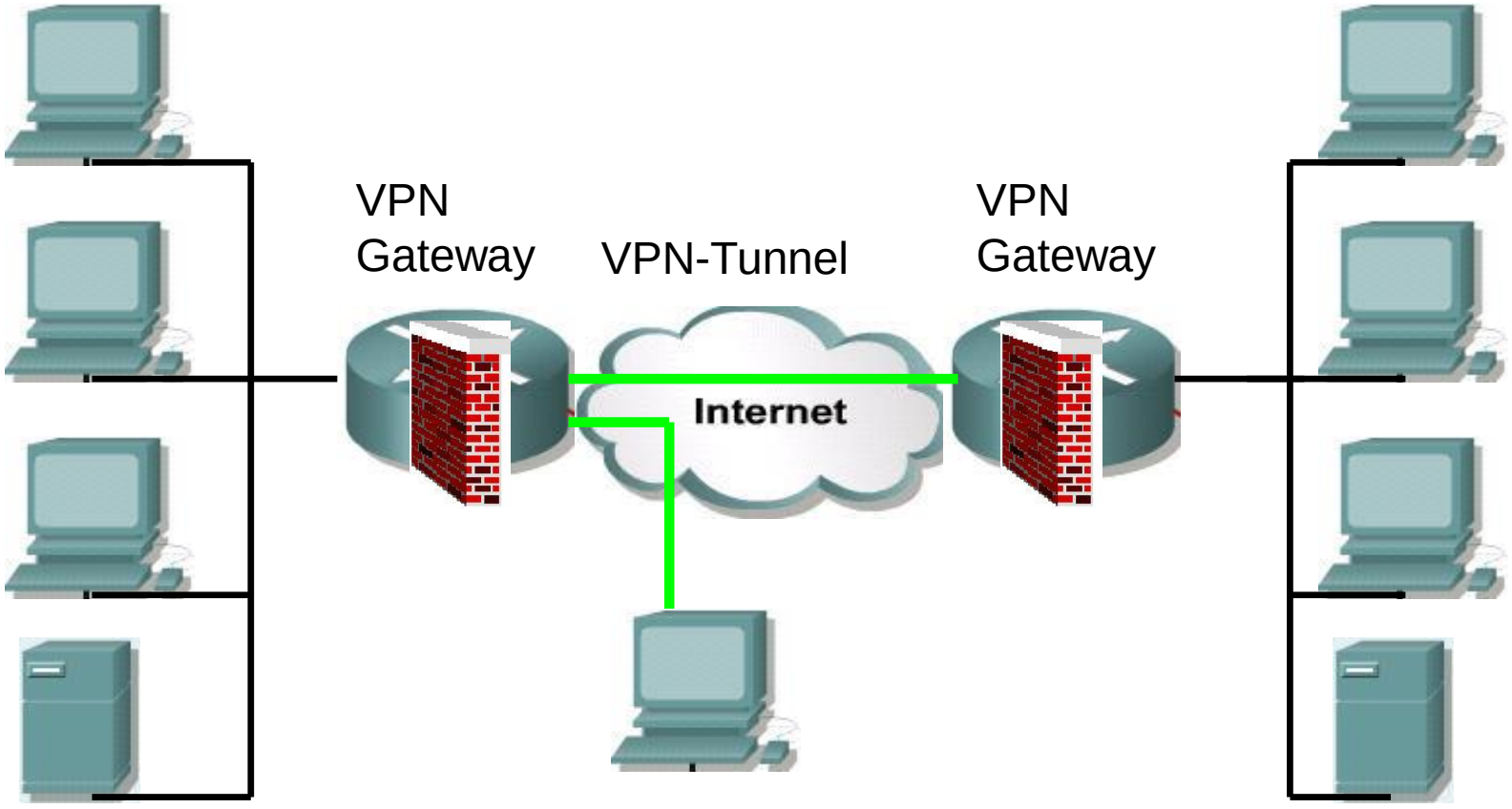
Personal Firewall Sandboxing

- Dabei werden einzelne Programme in eine eingeschränkte Umgebung "gesperrt". In diesem implementierten Schutzbereich werden Programme ausgeführt. Falls es sich dabei um Schadsoftware handeln sollte, kann sie aber keinen Schaden anrichten, da durch die Isolation der Rest des Systems davon nicht beeinflusst wird.

Personal - Firewall Software

- Windows Firewall (ab XP SP2) und Defender
- McAfee Desktop Firewall
- Avira
- Fsecure
- Kaspersky
- Norton / Symantec Personal Firewall
- Zone Alarm
- …..

Virtual Private Networt



Virtual Private Networt

- VPN, Virtual Private Network bedeutet, dass eine verschlüsselte und damit sichere Verbindung zwischen genau zwei Endpunkten hergestellt werden kann.
- VPN ermöglicht einem Benutzer von einer privaten Lokalität über das Internet eine sichere Verbindung zu anderen Benutzern oder Firmen und Organisationen in der Art herzustellen, als würde sich der Benutzer im Intranet einer Firma befinden oder er und ein weiterer Benutzer hätten ein eigenes Intranet aufgebaut und gehörten zum gleichen Netzwerk.
- Im Internet als Transportmedium wird für diese Verbindung ein virtuelles Netz (ein „verschlüsselter Kanal“ oder „Tunnel“) angelegt, durch den die Rechner zweier lokal getrennter Bereiche wie in einem Netz kommunizieren können.
- Für diese Verbindung werden spezielle Protokolle eingesetzt

VPN Gateways

- VPN Gateways koppeln komplette lokale Netze über das Internet.
- VPN Gateways können Standalone Geräte sein, aber es werden auch viele Router, Firewalls und Internet Server mit VPN Funktionalität geliefert.
- Standalone Gateways bieten sich insbesondere bei hohen Verschlüsselungsdurchsätzen (> 2 Mbps 3DES) an, da diese Geräte mit spezieller Verschlüsselungshardware oft preiswerter und flexibeler einzusetzen sind, als universelle Systeme.
- Im Bereich bis 2/4 Mbps arbeiten viele moderne Router und Firewalls auch ohne spezieller Verschlüsselungshardware komfortabel, schnell und preiswert.

VPN Remote Clients

- Ein Remote Client ist ein einzelner Rechner (oftmals ein Notebook), der sich in das Internet einwählt und dann über einen VPN Tunnel die Verbindung in das zentrale Netzwerk herstellt.
- Hierzu wird auf dem System ein VPN Client benötigt, der die Verschlüsselung durchführt.
- Microsoft liefert mit dem Windows Betriebssystem direkt einen PPTP VPN Client. Auf diese Weise können VPN's mit MS Windows Remote Systemen sehr bequem mit PPTP aufgebaut werden.

IPSec vs. PPTP In der Praxis werden im Moment hauptsächlich IPSec und PPTP VPN's eingesetzt.

- **PPTP** (Point to Point Tunneling Protocol)
  - ist ein von Microsoft initiiertes Protokoll
  - arbeitet auf Layer-2 sozusagen als "virtuelles Kabel".
  - PPTP ist multiprotokollfähig und kann zum Beispiel in IP und IPX Netzwerken genutzt werden.
  - PPTP ist insbesondere im Bereich Remote-User VPN interessant.
  - Alle Microsoft Betriebssysteme kommen bereits mit installierter PPTP Client Software und können auch problemlos mit alle Einwahltechniken incl. dynamischen IP Nummern eingesetzt werden.
  - PPTP ist durch einen Bug im Schlüsselaustausch als "relativ unsicheres" VPN Protokoll inzwischen etwas verrufen und wird bei neuen VPN's mit höherem Sicherheitsbedarf von IPSec fast komplett verdrängt.

IPSec vs. PPTP In der Praxis werden im Moment hauptsächlich IPSec und PPTP VPN's eingesetzt.

- **IPSec (IP Security)**
  - IPSec ist eine Layer-3 Tunneling Protokoll und arbeitet - wie der Namen IP Security bereits schließen läßt - auf IP Basis.
  - IPSec ist im Rahmen von IPv6 entwickelt worden und bereits vor der Umsetzung auf den IPv4 Standard aufgesetzt worden.
  - IPSec ist "sicherer" als PPTP bzw. andere Layer-2 Tunneling Protokolle.
  - Es bestehen allerdings noch Probleme in der Kompatibilität der Implementationen
  - ideal für Gateway-Gateway Kommunikation mit festen IP Nummern
  - problematischer bei Einsatz von Remote Usern mit dynamischen IP Adressen.
  - IPSec wird standardmäßig mit DES bzw. 3DES Verschlüsselung implementiert. Dies ist aber keine grundsätzliche Spezifikation des IPSec Protokolls.
  - speziell zu installierende Client Software benötigt

IPSec

- IPsec (Internet Protokol Security)-Protokoll, besteht aus
  - dem Encapsulating Security Payload (ESP), das die Art und Weise definiert, wie die eigentlichen Daten verschlüsselt zu übertragen sind :
    - Beim Tunnel Mode wird das gesamte IP-Paket inklusive IPHeader des eigentlichen Zielrechners verschlüsselt dem ESPHeader angehängt, der äußere Header trägt dabei die IP-Adresse eines Gatewayrechners, so dass die IP Pakete durch den Gateway zum Zielrechner wie durch einen verschlüsselten Tunnel übertragen werden.
    - Beim Transport Mode werden nur TCP,UDP und ICMP verschlüsselt dem Header angehängt
  - und dem Authenticated Header (AH) Protokoll, das definiert den Hash (kryptographisch gebildete Prüfsumme) des gesamten IP-Paketes zur Integritätskontrolle.

IPSec Funktionsweise

- Jede Datenübertragung oder Zugriffe auf Netzwerkressourcen, setzen eine erfolgreiche Legitimation des Computers oder Benutzers voraus.
- Verschlüsselung der übertragenen Daten.
- Jedes Datenpaket das übertragen werden soll, wird mit einer verschlüsselten Prüfsumme versehen.

Internet Key Exchange (IKE) Protokoll

- Legt fest, welche Algorithmen und Schlüssel zur wechselseitigen Authentifizierungs- und Schlüsselaustauschphase und zur anschließenden Verschlüsselung der zu übertragenden Nutzungsdaten verwendet werden