



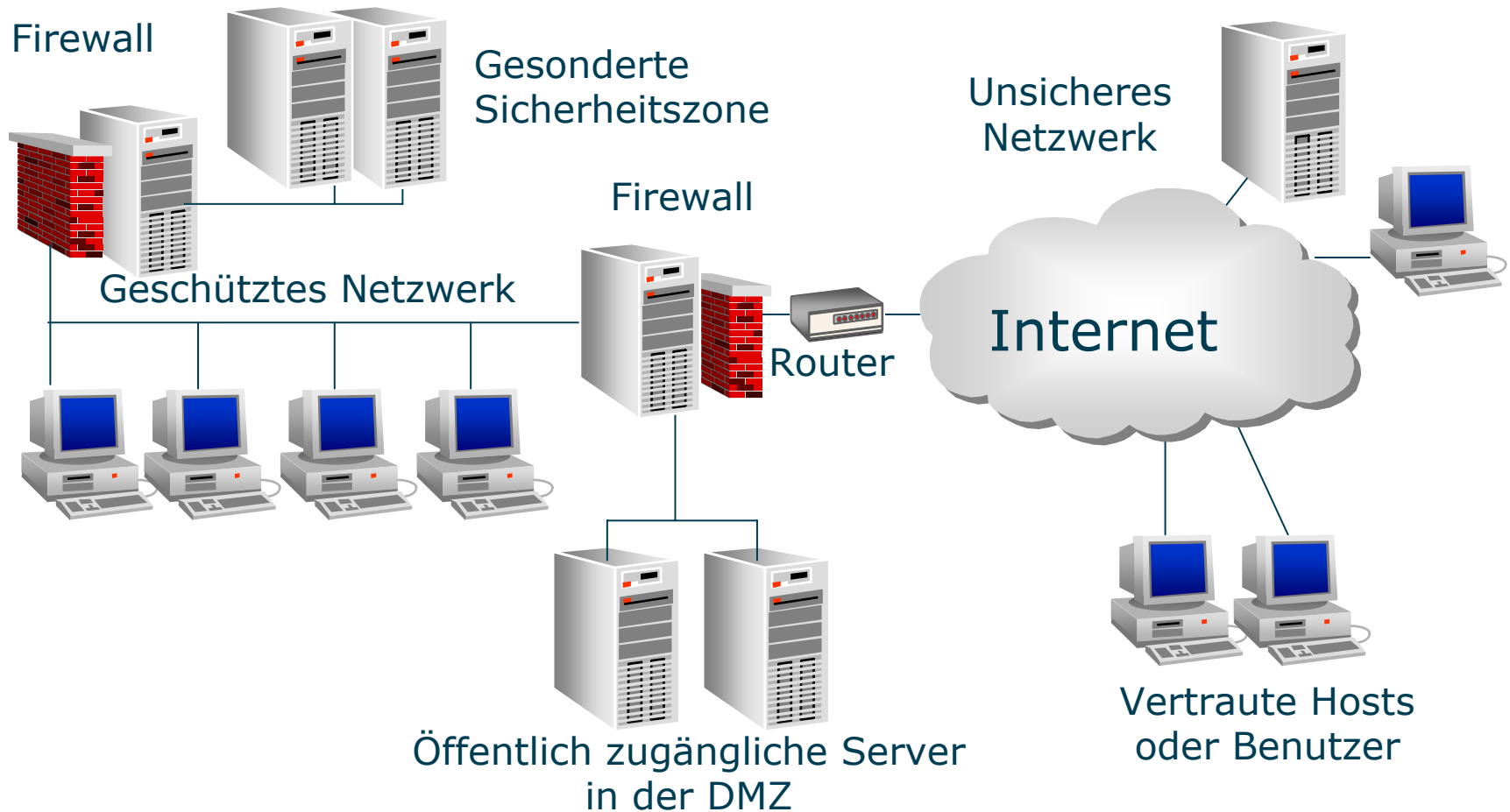
Welche Sicherheit bieten Firewalls?

Firewalls allgemein

- Aufgaben von Firewalls
 - Firewalls trennen gesicherte Netze von unsicheren Netzen, meist das interne Netz vom Internet.
 - Firewalls können aber auch eingesetzt werden, um das interne Netz zu strukturieren und unterschiedliche Sicherheitszonen zu schaffen.
 - Eine Firewall stellt einen „Common Point of Trust“ oder einen „Choke Point“ dar.

Firewalls allgemein

- Common Point of Trust



Firewalls allgemein

- Common Point of Trust
 - Das „Common Point of Trust“ oder „Choke Point“-Prinzip bietet einige Vorteile:
 - Ein zentraler Einstiegspunkt in das interne Netz kann leicht gewartet werden.
 - Die Sicherheitspolitik lässt sich effizient an diesem Punkt durchsetzen.
 - Die Daten und die Benutzerauthentisierung lassen sich bis zu diesem Punkt verschlüsselt über das unsichere Netz übertragen.

Firewalls allgemein

- Aufgaben einer Firewall
 - Eingehenden Netzwerkverkehr transparent zulassen oder blockieren
 - Ausgehenden Netzwerkverkehr transparent zulassen oder blockieren
 - Netzwerkverkehr aufgrund von Inhalten blockieren (meist mit 3rd Party-Software)
 - Interne Ressourcen mit Benutzerauthentifizierung zur Verfügung stellen
 - Sichere Verbindungen in das interne Netz ermöglichen (VPN)
 - Interne Strukturen verbergen (NAT)
 - Selbstschutz bei Angriffen
 - Protokollierung des Netzwerkverkehrs und der Firewall-Aktivitäten zur Beweissicherung

Firewalls allgemein

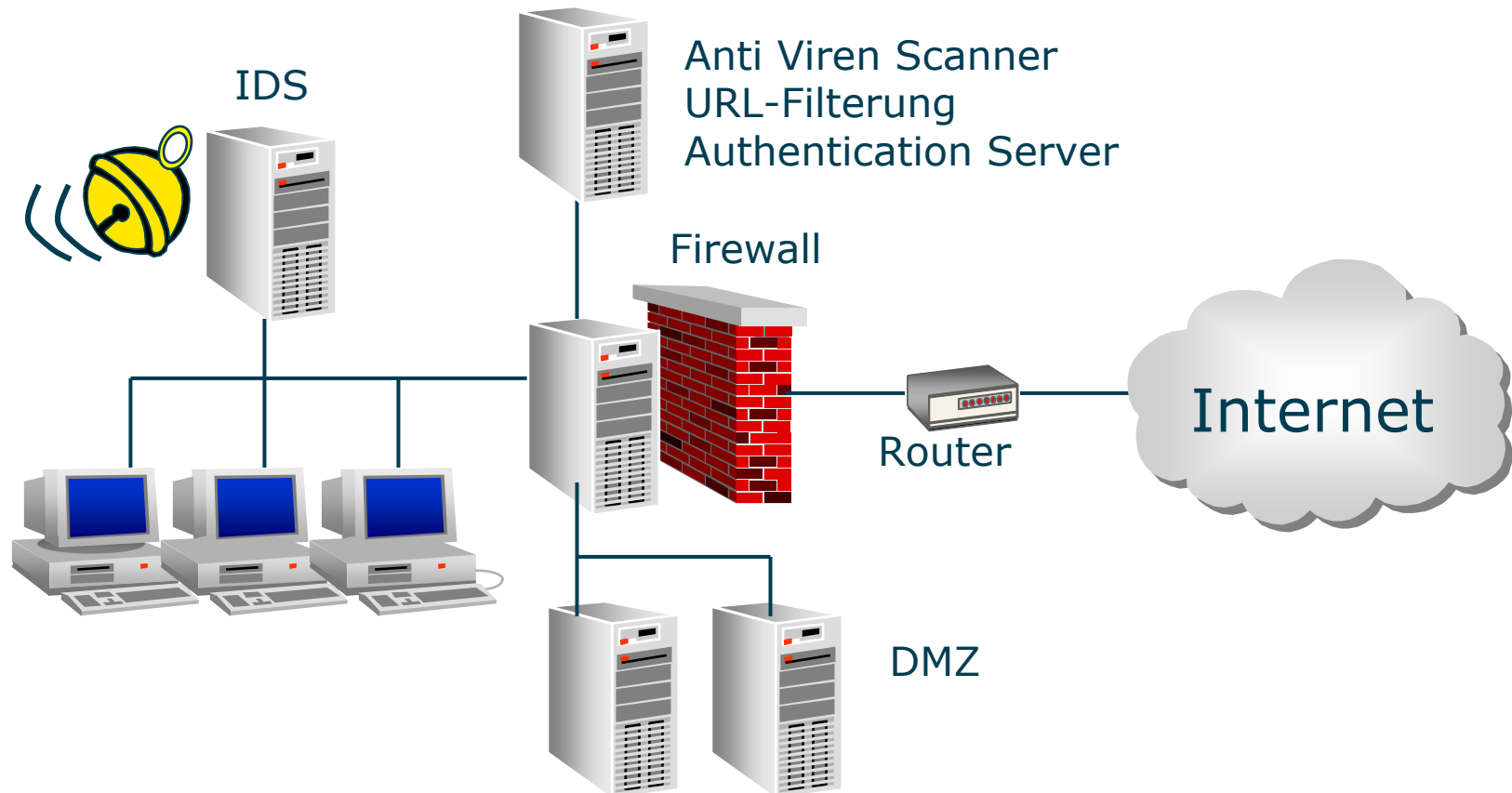
- Forderung an eine Firewall
 - Eine Firewall muss die Sicherheitspolitik des Unternehmens / der Institution umsetzen können.
 - Diese muss in einem Regelwerk (Security Policy) für die Firewall definiert werden können.

Firewalls allgemein

- Grenzen der Firewalls
 - Eine Firewall bietet keinen 100%igen Schutz.
 - Eine Firewall kann den Zugang zum geschützten Netz nur erschweren.
 - Deshalb sollte eine Firewall immer mit weiteren Sicherheitseinrichtungen, wie z.B. Intrusion Detection Systemen (IDS), kombiniert werden.
 - Eine Firewall kann mit dem Wächter an der Pforte, ein IDS mit einer Alarmanlage verglichen werden.

Firewalls allgemein

- Grundschatz mit Firewalls

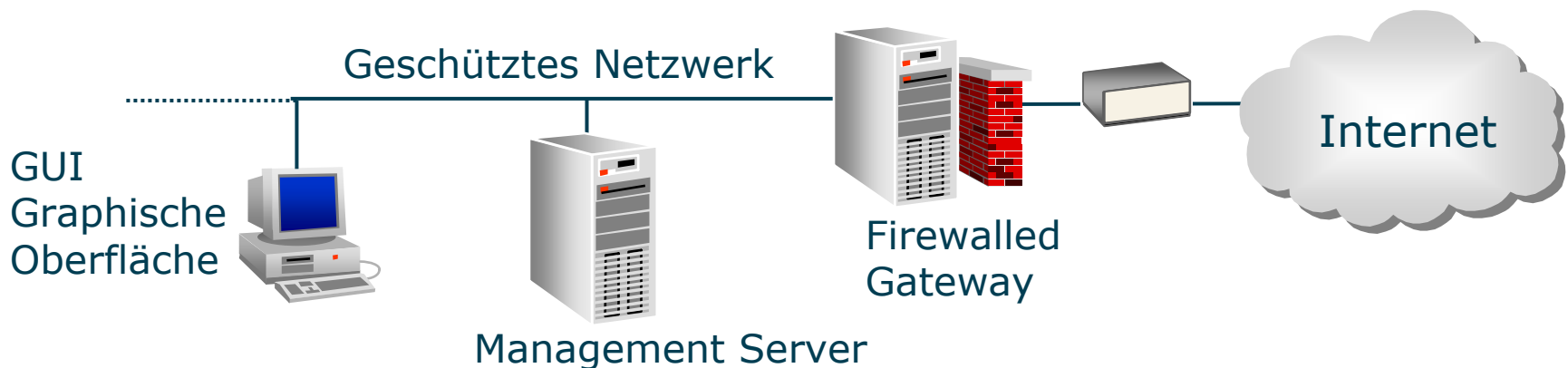


Aufbau und Philosophie von Firewalls

- Typen von Firewalls
 - Firewalls können anhand der Anforderungen aufgrund des Netzwerkverkehrs, der Kapazität und der Anzahl der Computer im zu schützenden Netzwerk in folgende Typen unterteilt werden:
 - Personal Firewall
 - Schützt einen Computer
 - Firewall für Außenstellen / kleine Organisationen
 - Schützt eine begrenzte Anzahl von Computern
 - Unternehmens-Firewall
 - Für tausende von Benutzern
 - Evtl. geographische Trennung der Benutzer
 - Mit komfortablen Administrator-Dienstprogrammen
 - Mit Protokollen für Vielfach-Firewalls

Aufbau und Philosophie von Firewalls NTC

- Aufteilung einer Unternehmens-Firewall
 - Eine Firewall für ein Unternehmensnetz wird meist in mehrere Teile gegliedert.
 - Jeder dieser Teile kann u.U. auf einer anderen Plattform und unter einem anderen Betriebssystem implementiert sein.
 - Z.B. Check Point FireWall-1



Aufbau und Philosophie von Firewalls

- Aufteilung einer Unternehmens-Firewall
 - Graphische Oberfläche (GUI-Client)
 - Dient zur komfortablen Erstellung des Regelwerkes
 - Management-Server
 - Speichert die Datenbank für das Regelwerk und die Benutzer
 - Sammelt die Log-Einträge
 - Firewalled Gateway
 - Setzt das Regelwerk zwischen den Netzwerken um
 - Besteht aus der Firewall Software
 - Die einzige Aufgabe der Software und des Betriebssystems ist das Prüfen der Pakete

Aufbau und Philosophie von Firewalls

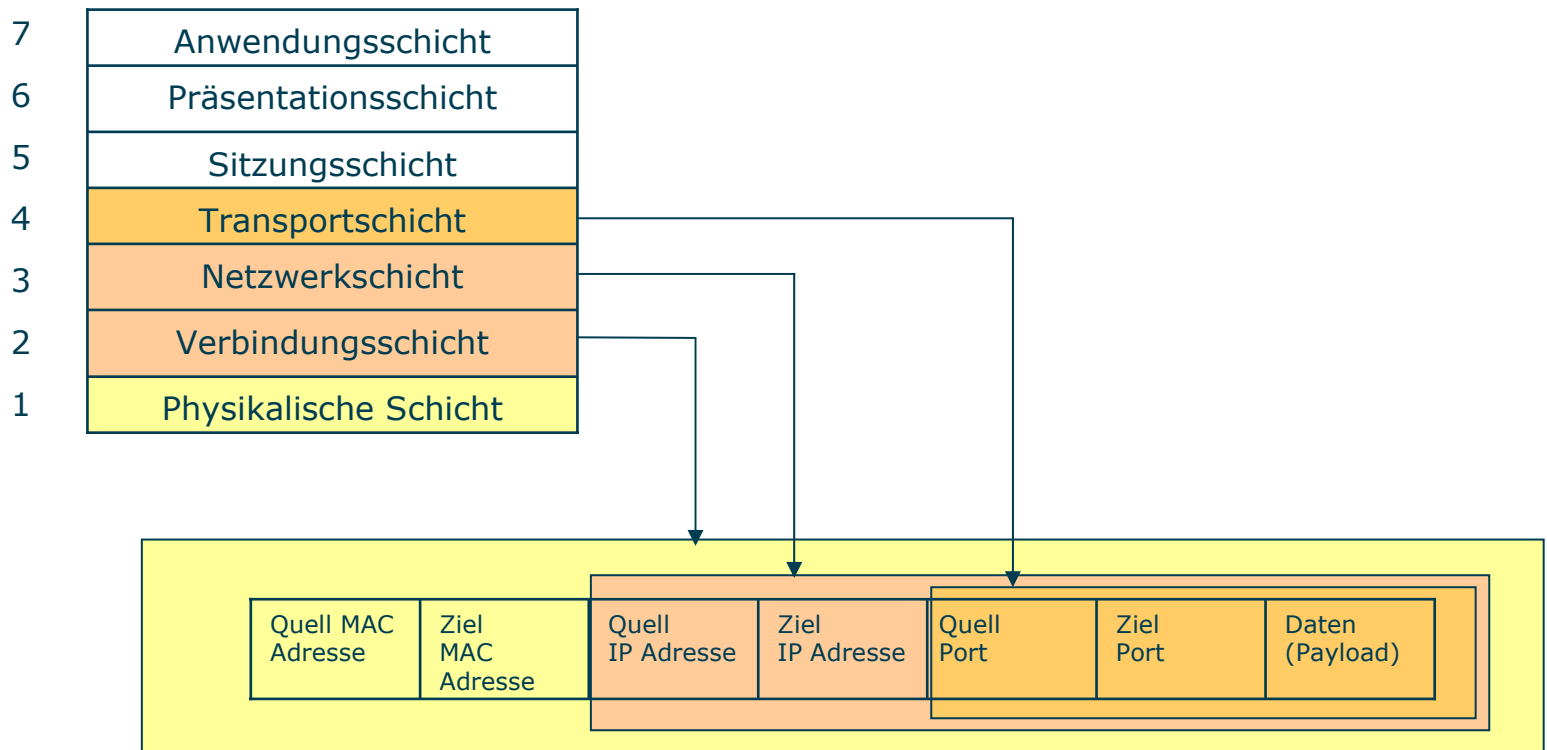
- Philosophie der Firewall-Hersteller
 - Netzwerkrouter
 - Beinhalten meist nur rudimentäre Firewall-Funktionen (Paketfilterung)
 - Hardware Firewalls
 - Bestehen aus einer Hardware-Blackbox
 - Verfügen über ein angepasstes, „gehärtetes“ Betriebssystem
 - Die Konfiguration erfolgt meist über Web-Browser
 - Software Firewalls
 - Setzen auf bestehende Hardware und Betriebssysteme auf
 - Das Betriebssystem wird durch Installationsroutinen oder den Administrator „gehärtet“

Aufbau und Philosophie von Firewalls

- Funktion der Firewalls
 - Jedes Paket, das an eine Firewall gelangt, wird aufgrund der Security Policy geprüft.
 - Anhand der Security Policy wird entschieden, ob das Paket:
 - Fallengelassen wird (Drop)
 - Zurückgewiesen wird (Reject)
 - Passieren darf (Accept)
 - Verschlüsselt wird (Encrypt)
 - Aufgezeichnet wird (Log)
 - Einen Alarm meldet (Alert)

Aufbau und Philosophie von Firewalls NTC

- Gruppierung von Firewalls
 - Die Firewalls werden aufgrund der Schicht des OSI-7-Schichten-Modells, auf der die Prüfung stattfindet, in Gruppen unterteilt.



Aufbau und Philosophie von Firewalls

- Es werden drei Hauptgruppierungen unterschieden

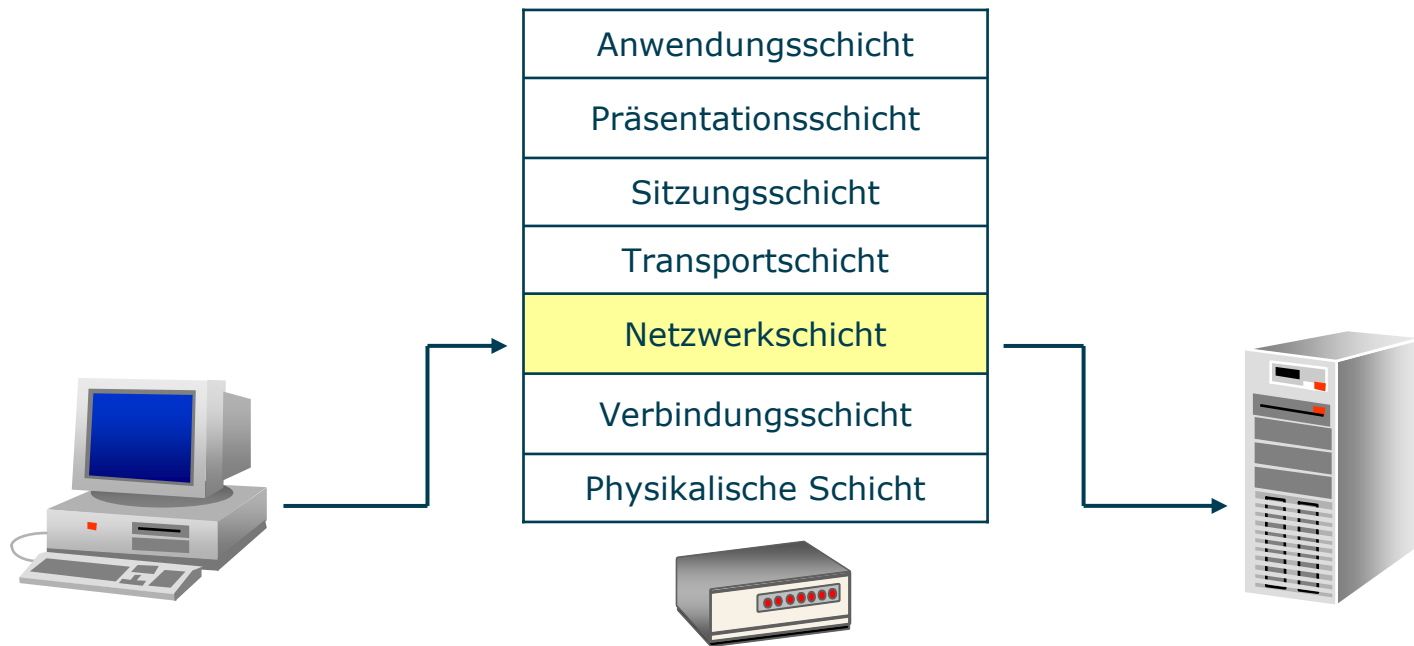
Anwendungsschicht	<i>Application Layer Gateway</i>
Präsentationsschicht	
Sitzungsschicht	
Transportschicht	
Netzwerkschicht	<i>Packet Filter</i>
<i>Zusatzschicht</i>	<i>Stateful Inspection Firewalls</i>
Verbindungsschicht	
Physikalische Schicht	

Aufbau und Philosophie von Firewalls

- Packet Filter
 - Die älteren Firewalls der ersten Generation oder einfache Firewalls (Router) sind meist schlichte Paketfilter.
 - Die Paketfilter prüfen den Netzwerkverkehr auf der Schicht 3, der Netzwerkschicht.
 - Die oberen Schichten bleiben unberücksichtigt.
 - Nur die Absender- und Empfängeradressen werden geprüft.
 - Die Pakete werden anhand eines benutzerdefinierten Regelwerkes weitergeleitet oder zurückgewiesen.

Aufbau und Philosophie von Firewalls NTC

- Packet Filter



Aufbau und Philosophie von Firewalls

- Packet Filter
- Vorteile:
 - Kostengünstig
 - Transparent für die Applikationen
 - Schnellere Prüfung der Pakete
- Nachteile:
 - Nur Teile des Headers werden geprüft
 - Kaum Überprüfung oberhalb der Netzwerkschicht
 - Kaum Veränderung der Informationen möglich
 - Schwierig zu konfigurieren
 - Unzureichende Log- und Alarmmechanismen

Aufbau und Philosophie von Firewalls

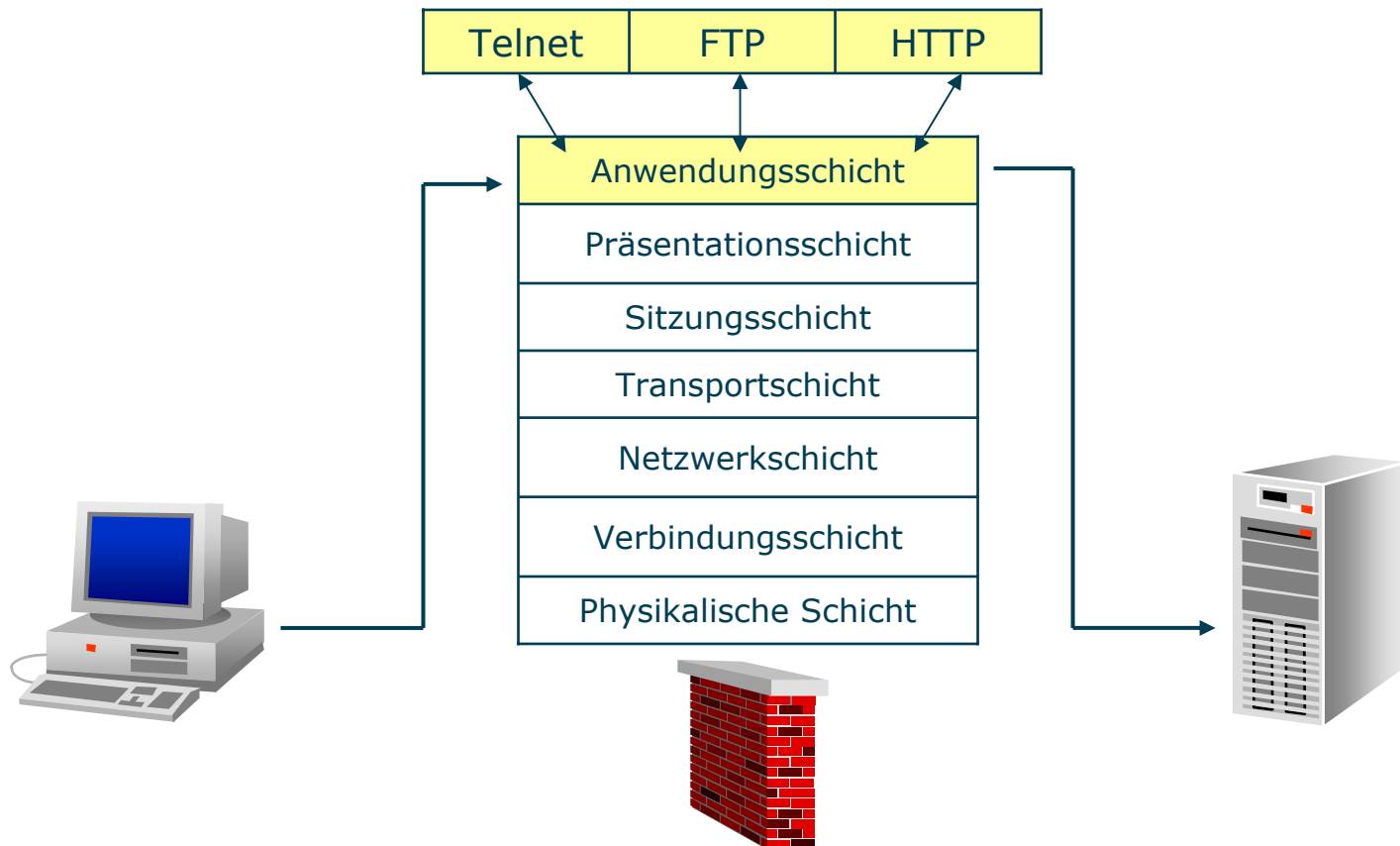
- Packet Filter
 - Um die Nachteile von ursprünglichen Paketfiltern zu umgehen, wurden diese mit zusätzlichen Leistungsmerkmalen ausgestattet.
 - Dynamische Paketfilter
 - Diese prüfen und speichern dynamisch zusätzlich zur Quell- und Zieladresse noch die Ports von UDP oder TCP.
 - Benutzerorientierte Paketfilter
 - Diese können Benutzer anhand eines Profils überprüfen und z.B. mittels Smart-Card verifizieren.
 - Stateful Packet Filtering
 - Diese lassen automatisch den Netzwerkverkehr zu, der als Antwort auf ein ausgehendes Paket zu sehen ist. Dabei kann auch auf höheren Ebenen geprüft werden (Firewall-Funktionalität).

Aufbau und Philosophie von Firewalls

- Application Layer Gateway
 - Die Application Layer Gateways oder Proxy sind Firewalls der zweiten Generation.
 - Diese prüfen den Netzwerkverkehr auf der Schicht 7, der Applikationsschicht.
 - Dabei wird das Client- / Server-Modell durchbrochen, also die direkte Verbindung eines Clients zu einem Server.
 - Es werden zwei Netzwerkverbindungen benötigt, eine vom Client zur Firewall und eine von der Firewall zum Server.
 - Zusätzlich wird für jede zu prüfende Netzwerkverbindung eine spezielle „Prüfapplikation“ benötigt.

Aufbau und Philosophie von Firewalls NTC

- Application Layer Gateway



Aufbau und Philosophie von Firewalls

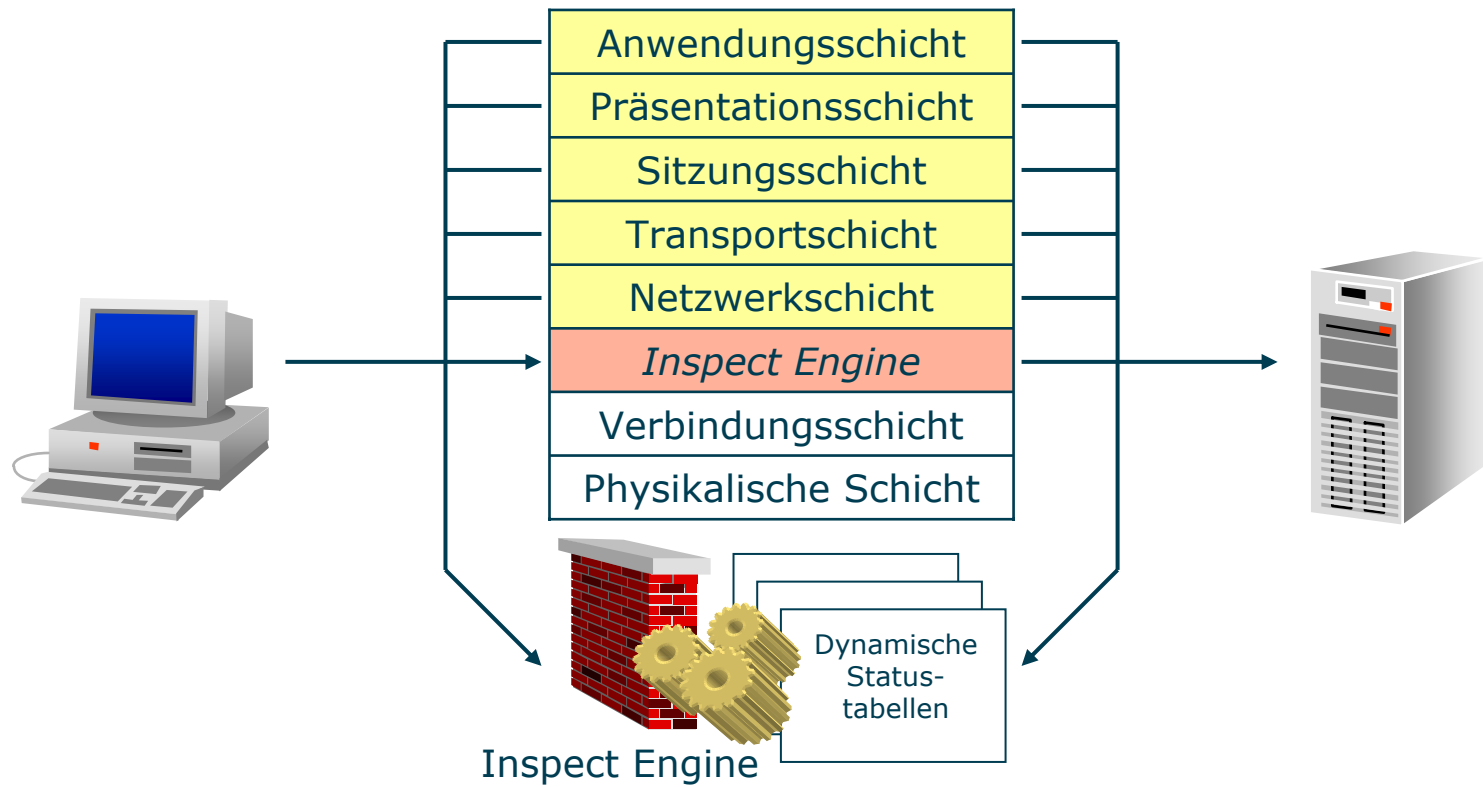
- Application Layer Gateway
- Vorteile:
 - Sehr gute Sicherheit
 - Prüfung auf der obersten Schicht, damit auch Datenprüfung möglich
- Nachteile:
 - Jeder Dienst benötigt eine „Prüfapplikation“
 - Die Leistung ist eingeschränkt
 - U.U.keine Unterstützung von UDP, RPC und anderen Protokollfamilien
 - Meist keine Transparenz
 - Informationen in den unteren Schichten werden nicht berücksichtigt
 - Zwei Verbindungen für eine Funktion
 - Das Betriebssystem ist bei Bugs anfällig

Aufbau und Philosophie von Firewalls

- Stateful Inspection
 - Die Stateful Inspection Firewalls sind Firewalls der dritten Generation.
 - Die Informationen der oberen 5 Schichten können geprüft werden.
 - Die Statusinformationen von vorhergehenden Kommunikation können geprüft werden (z.B. FTP).
 - Die Statusinformationen anderer Applikationen können geprüft und weiterverwendet werden (z.B. Benutzerauthentifizierung).
 - Die Informationen aller geprüften Schichten werden berücksichtigt.

Aufbau und Philosophie von Firewalls NTC

- Stateful Inspection



Aufbau und Philosophie von Firewalls NTC

- Stateful Inspection
- Vorteile:
 - Gute Sicherheit
 - Überprüfung der oberen 5 Schichten möglich
 - Hohe Leistung
 - Skalierbar
 - Erweiterbar
 - Transparent
- Nachteile:
 - ?

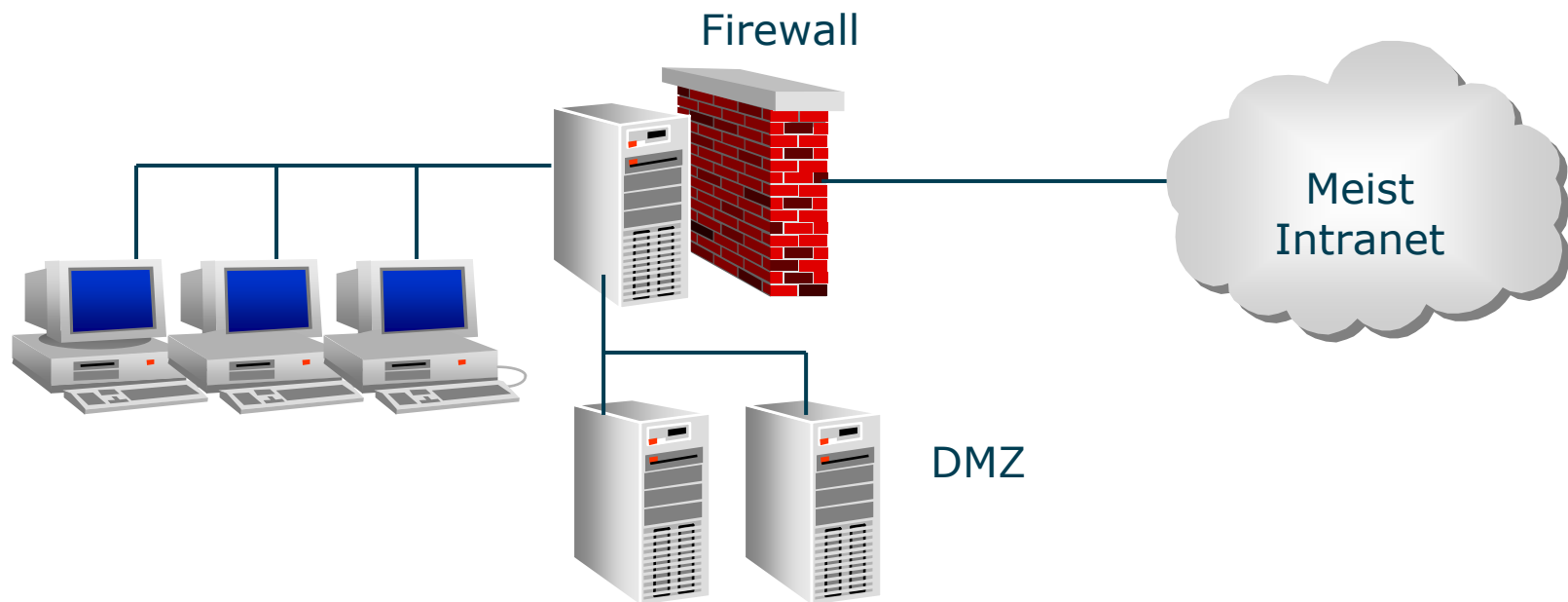
Aufbau und Philosophie von Firewalls

- Weitere Begrifflichkeiten
 - Screening Router
 - Dies ist ein Paketfilter, der Pakete aufgrund der Richtung (Inbound / Outbound) prüft.
 - Circuit Level Gateway
 - Dies ist ein Paketfilter, der zusätzlich Network Address Translation (NAT) durchführt.
 - Proxy Server
 - Darunter wird ein Server verstanden, der für interne Clients Dienste nach außen übernimmt und eventuell Firewall-Funktionalität besitzt.

- DMZ (Demilitarisierte Zone)
 - Firewalls trennen ein gesichertes Netz von einem unsicheren Netz.
 - Soll vom unsicheren Netz auf Server in einem sicheren Netz zugegriffen werden, so empfiehlt sich das Einrichten einer DMZ.
 - Die DMZ ist ein spezielles Teilnetz, in dem alle öffentlich zugänglichen Server platziert werden.
 - Der Zugriff vom unsicheren Netz auf das sichere als auch umgekehrt sollte immer über die DMZ erfolgen.

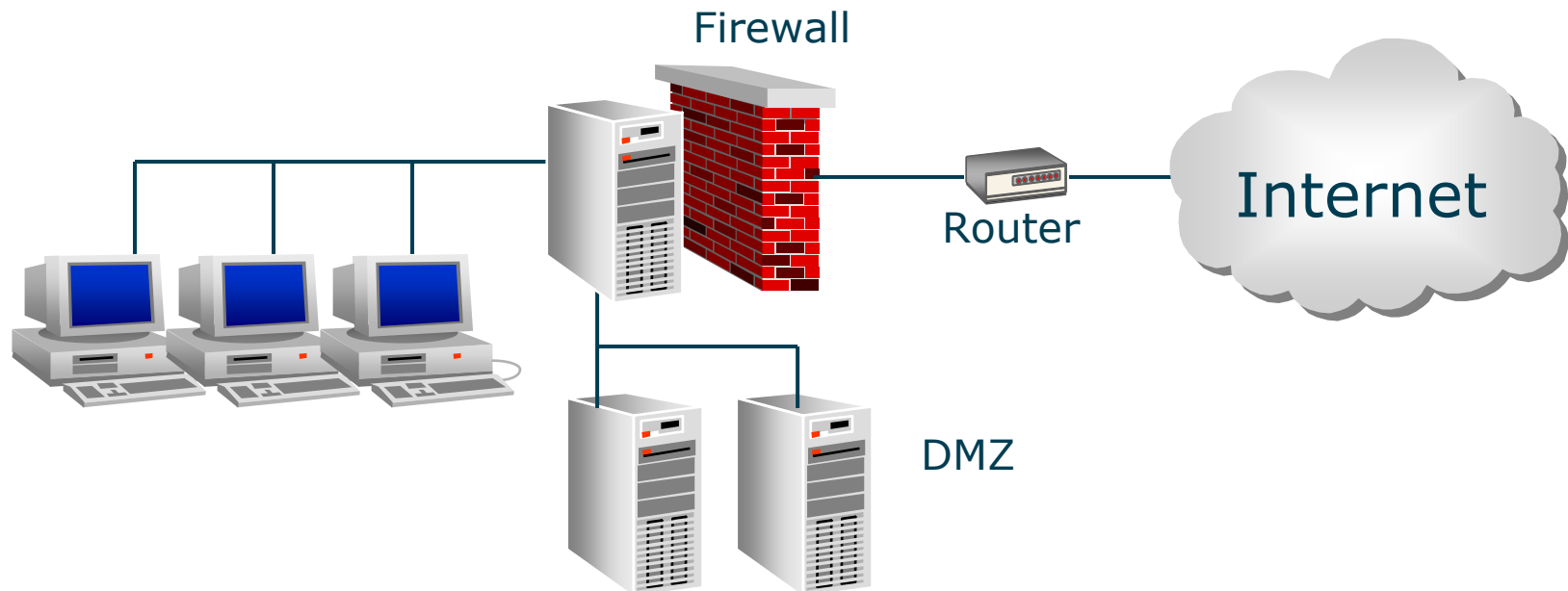
Grundlegende Firewallkonzeptionen

- Bastion Host
 - Beim Bastion Host-Aufbau ist die Firewall direkt an das unsichere Netz gekoppelt, sie ist die einzige Bastion vor dem sicheren Netz.



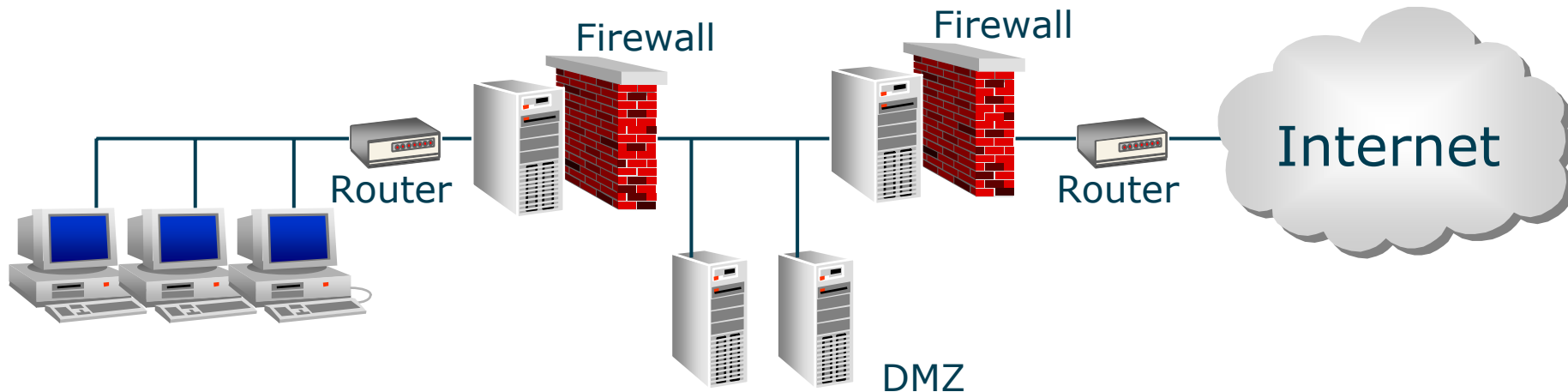
Grundlegende Firewallkonzeptionen

- Screened Bastion Host
 - Beim Bastion Host-Aufbau ist die Firewall über einen Router mit dem unsicheren Netz verbunden. Die Firewall ist dadurch „abgeschirmt“.



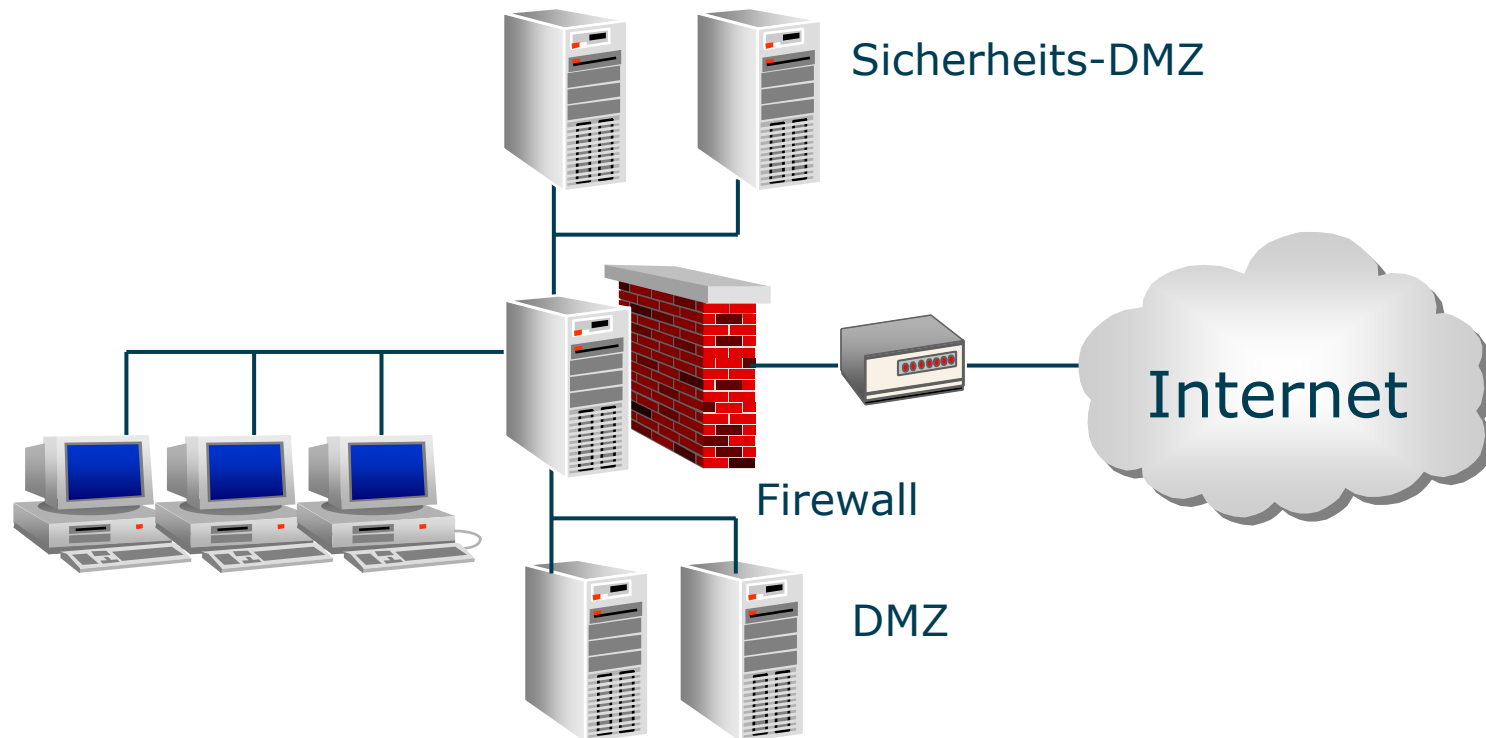
Grundlegende Firewallkonzeptionen

- Screened Subnet
 - Beim Screened Subnet-Aufbau ist die eine Firewall über einen Router mit dem unsicheren Netz verbunden.
 - Die zweite Firewall wird über einen Router mit dem sicheren Netz verbunden.
 - Das Teilnetz zwischen den Firewalls bildet die DMZ.



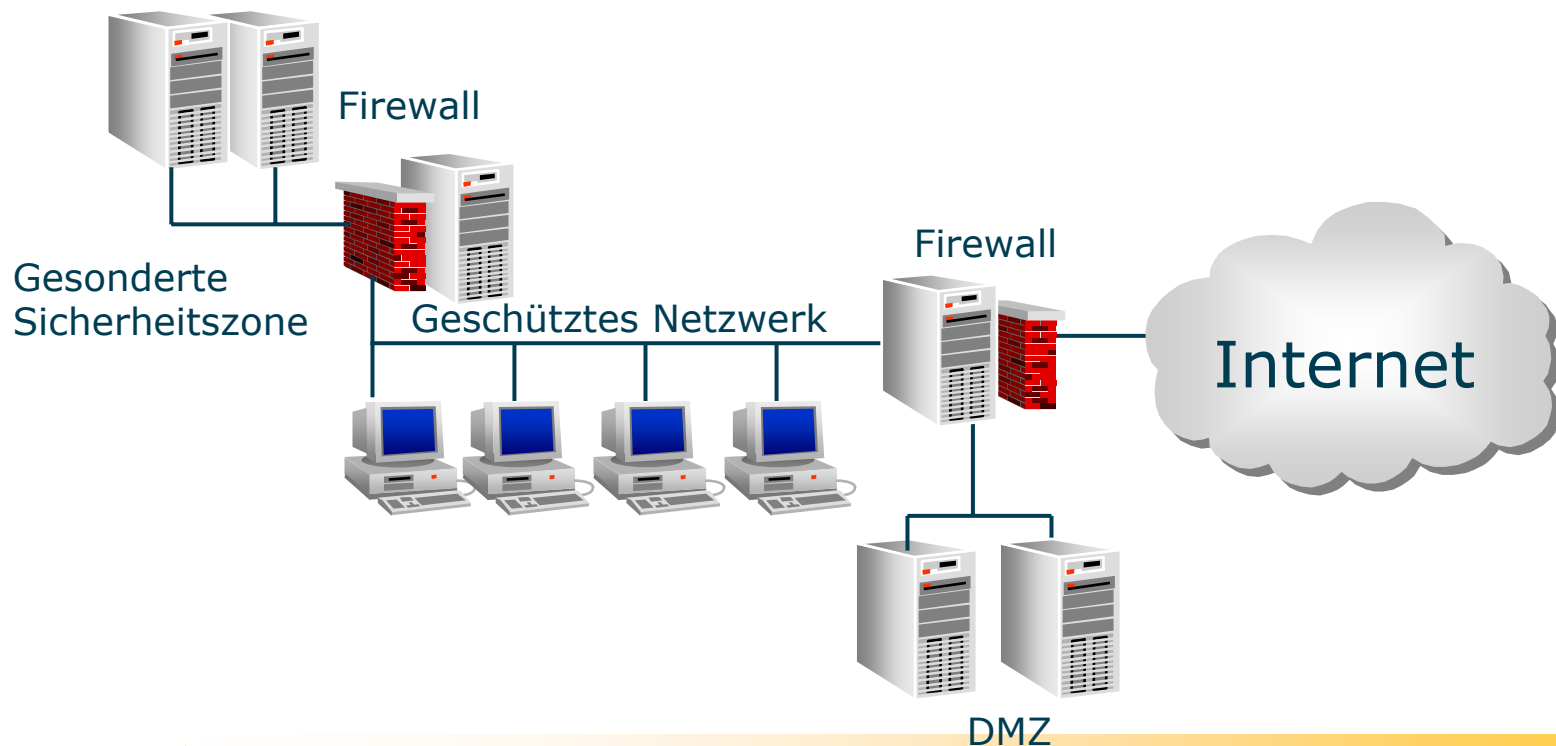
Grundlegende Firewallkonzeptionen

- Mehrere DMZ
 - Beim Einsatz von weiterer Sicherheits-Software wie zentrale Anti Viren Scanner, URL-Filter oder Authentication Server empfiehlt es sich, diese in einer separaten DMZ zu platzieren.



Grundlegende Firewallkonzeptionen

- Mehrere Firewalls in Reihe
 - Wird für bestimmte Abteilungen oder Server ein erhöhter Sicherheitsbedarf festgestellt, so können diese durch eine weitere Firewall „in Reihe“ geschützt werden.



Leistungsmerkmale und Grenzen

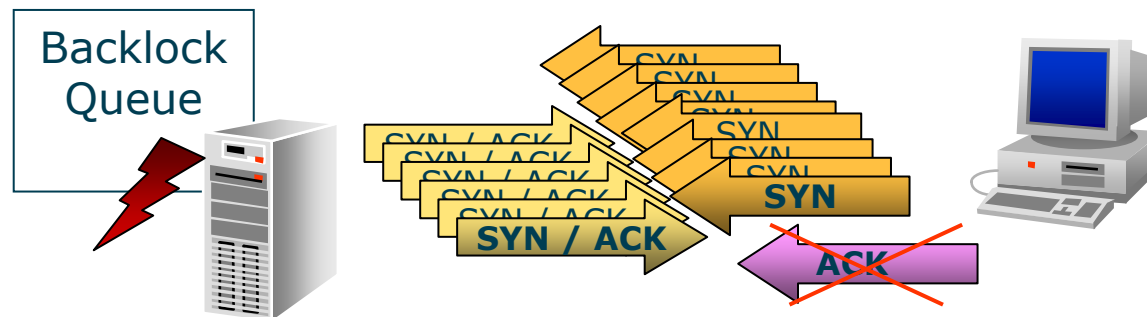
- Leistungsmerkmale
 - Die heutigen Firewalls bieten eine Reihe von Leistungsmerkmalen wie:
 - Virtuelle UDP-Verbindung
 - SYN-Defender
 - Anti Spoofing
 - Authentifizierung
 - Netzwerk Address Translation
 - Integrierte Sicherheitsdienste
 - Synchronisation
 - Load Balancing
 - Virtual Private Networks (VPN)

Leistungsmerkmale und Grenzen

- Virtuelle UDP-Verbindung
 - Beim UDP-Protokoll handelt es sich um ein verbindungsloses Protokoll.
 - Das UDP-Protokoll schickt die Pakete an das Ziel, ohne dass diese bestätigt werden.
 - Ist in einer Applikation aber eine Bestätigung des UDP-Paketes vorgesehen, so muss die Firewall die Rückantwort passieren lassen.
 - Das Antwortpaket wird von der Firewall nur dann akzeptiert, wenn es innerhalb einer bestimmten Zeit die Firewall erreicht und als Antwort auf ein ausgehendes Paket erkannt wird.

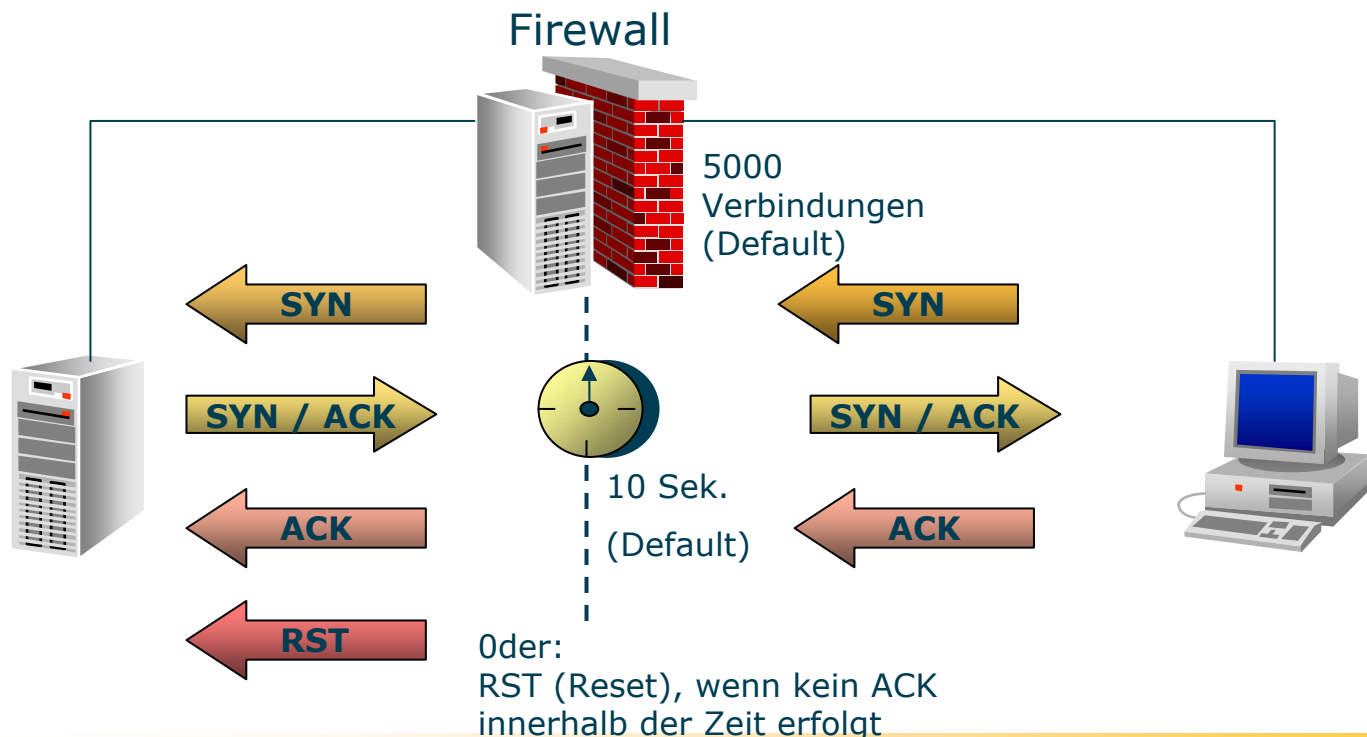
Leistungsmerkmale und Grenzen

- SYN-Defender
 - Das TCP-Protokoll arbeitet verbindungsorientiert.
 - Die Verbindungsaufnahme zwischen Client und Server geschieht durch einen „Three-Way-Hand-shake“ (SYN - SYN/ACK - ACK).
 - Der Server wird die Verbindungsaufnahme (SYN) im Cache, der sogenannten Backlog Queue, so lange zwischenspeichern, bis diese abgeschlossen ist (ACK) und das Anwenderprogramm die Verbindung übernommen hat.
 - Sendet nun ein Angreifer nur SYNs aber keine ACKs, so kommt es zu einem Überlauf der Backlog Queue und damit zum Stillstand des Servers.



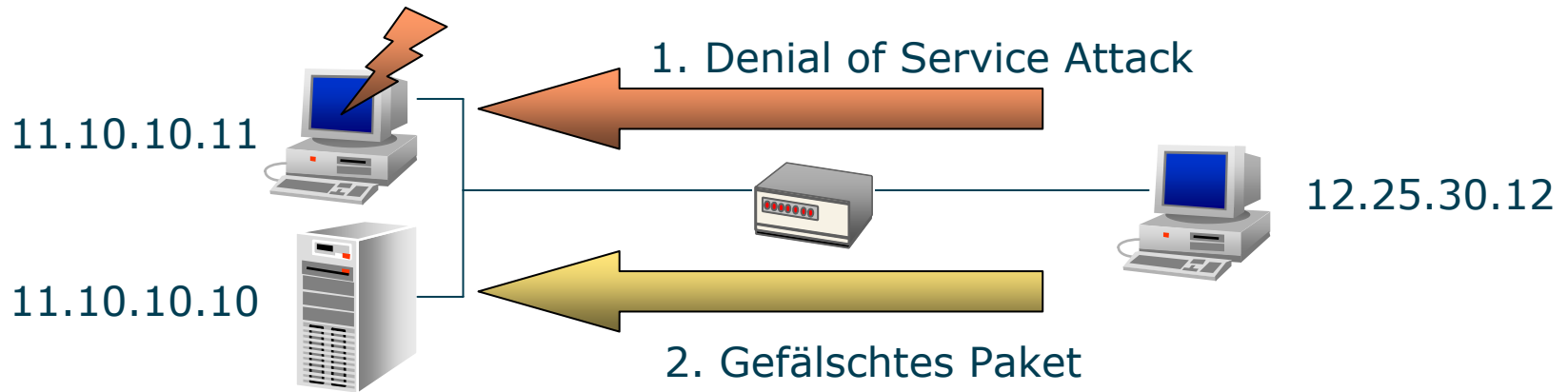
Leistungsmerkmale und Grenzen

- SYN-Defender
 - Eine Firewall wird die SYN-Attack erkennen und diese über eine eigene, große Backlog Queue mit geringer Verfallszeit der Verbindungsabfragen abfangen.



Leistungsmerkmale und Grenzen

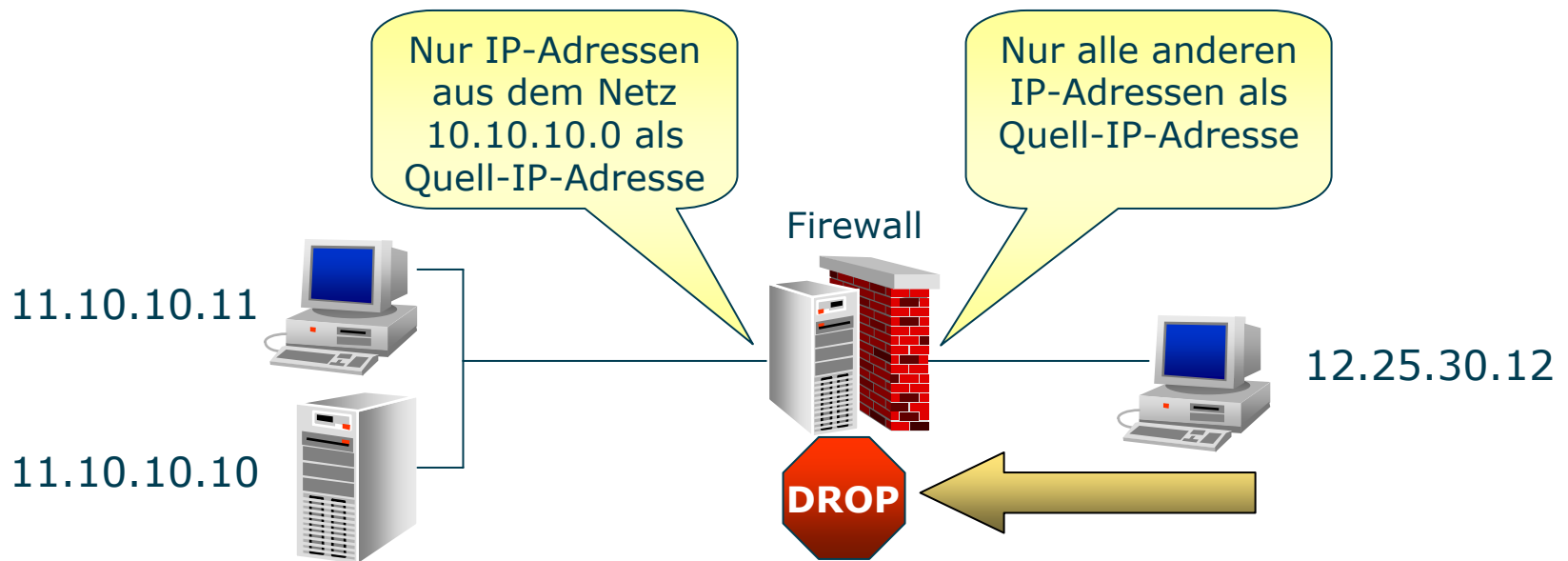
- Anti Spoofing
 - Bei einem Spoofing-Angriff versucht der Angreifer aus einem externen Netz mit einer gefälschten, internen IP-Adresse die Rechte eines Clients im internen Netz zu erlangen.



Source-IP	Dest.-IP	Source-Port	Dest.-Port	Daten
11.10.10.11	11.10.10.10	1050	80	

Leistungsmerkmale und Grenzen

- Anti Spoofing
 - Die Firewall erkennt, dass eine interne IP-Adresse als Quell-Adresse auf dem falschen Netzwerksegment erscheint und lässt das Paket fallen.



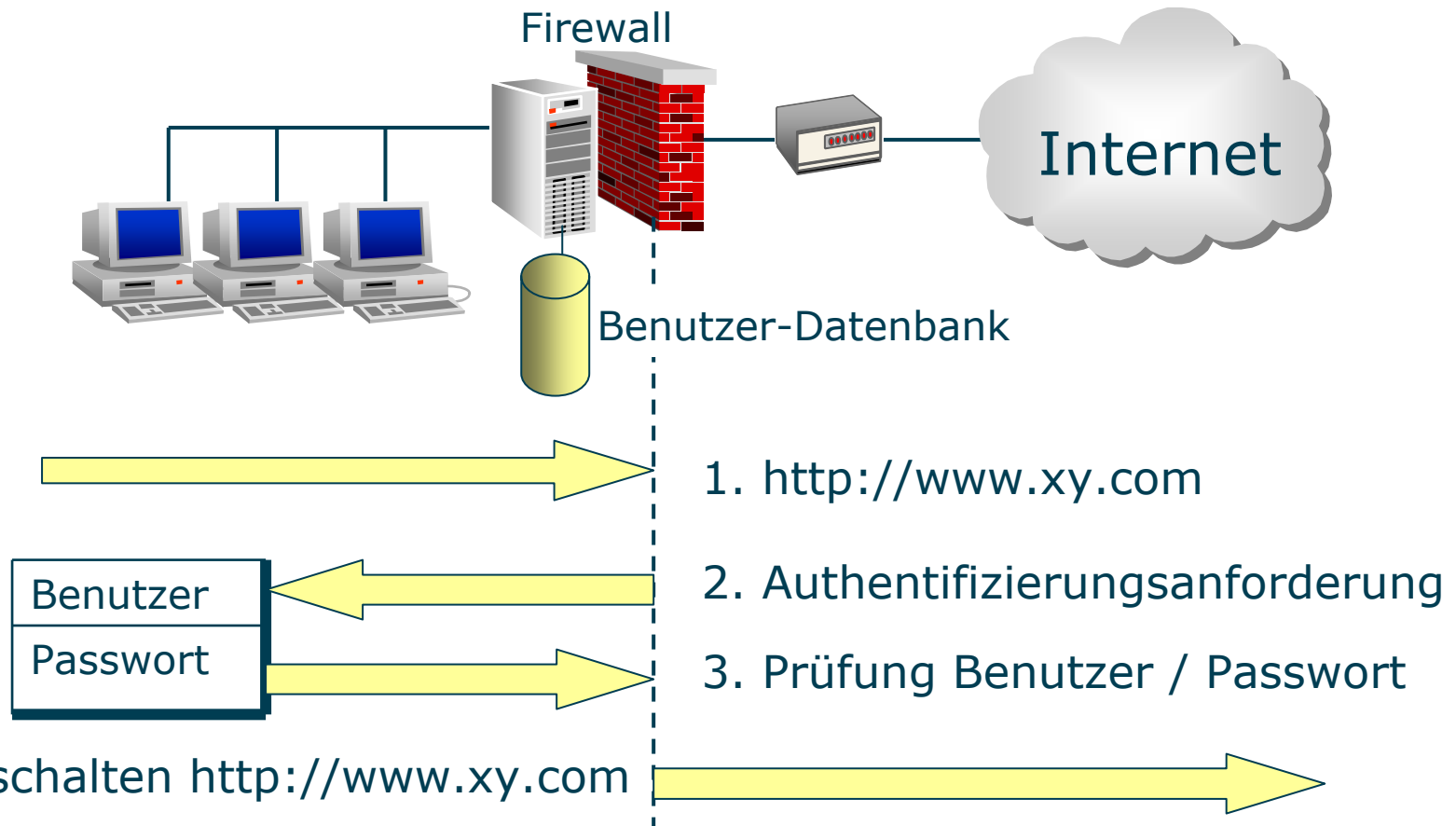
Source-IP	Dest.-IP	Source-Port	Dest.-Port	Daten
11.10.10.11	11.10.10.10	1050	80	

Leistungsmerkmale und Grenzen

- Authentifizierung
 - Einige Firewalls bieten interne Authentifizierungsschemata.
 - Will ein Benutzer die Firewall passieren, so muss er sich zunächst mit Benutzerkennung und Passwort ausweisen, bevor er für einen oder mehrere Dienste freigeschaltet wird.
 - Dazu verwendet die Firewall eine interne Benutzerdatenbank oder greift auf vorhandene Datenbanken (Betriebssystem) zu.
 - Mögliche Schemata sind:
 - Firewall Passwort
 - S/Key Einmalpasswort
 - Betriebssystempasswort

Leistungsmerkmale und Grenzen

- Authentifizierung



Leistungsmerkmale und Grenzen

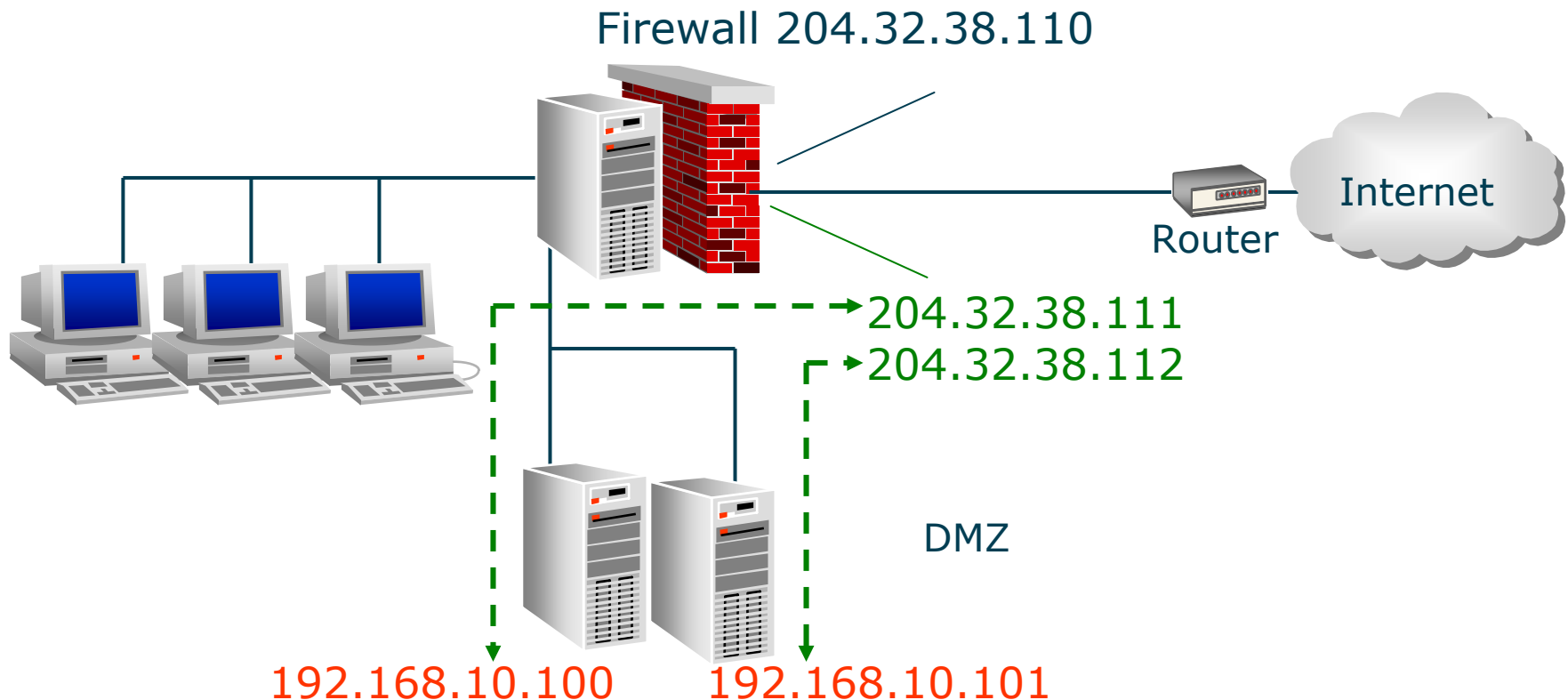
- Network Address Translation (NAT)
 - Aufgrund der Knappheit von IP-Adressen können Rechner im internen, zu schützenden Netz mit reservierten IP-Adressen versehen werden.
 - Diese Adressen kommen auf dem Internet nicht vor.
 - Die Adressen können beim Verlassen des geschützten Netzes in öffentliche Adressen übersetzt werden.
 - Man nennt diesen Vorgang NAT (Network Address Translation).
 - Zur Verfügung stehende reservierte IP-Adressen laut RFC 1597 und 1918 sind:
 - Eine Class A Adresse: 10.0.0.0 - 10.255.255.255
 - 16 Class B Adressen: 172.16.0.0 - 172.31.255.255
 - 256 Class C Adressen: 192.168.0.0 - 192.168.255.255

Leistungsmerkmale und Grenzen

- Network Address Translation (NAT)
 - Für die Network Address Translation stellen Firewalls 2 Modi zur Verfügung:
 - Statische NAT
 - Eine interne, private IP-Adresse wird extern auf eine öffentliche, gültige IP-Adresse übersetzt und umgekehrt.
 - Dieser Modus wird für öffentlich zugängliche Server verwendet.
 - Dynamische NAT
 - Ein oder mehrere Netzwerkadressen werden extern auf eine öffentliche, gültige IP-Adresse übersetzt.

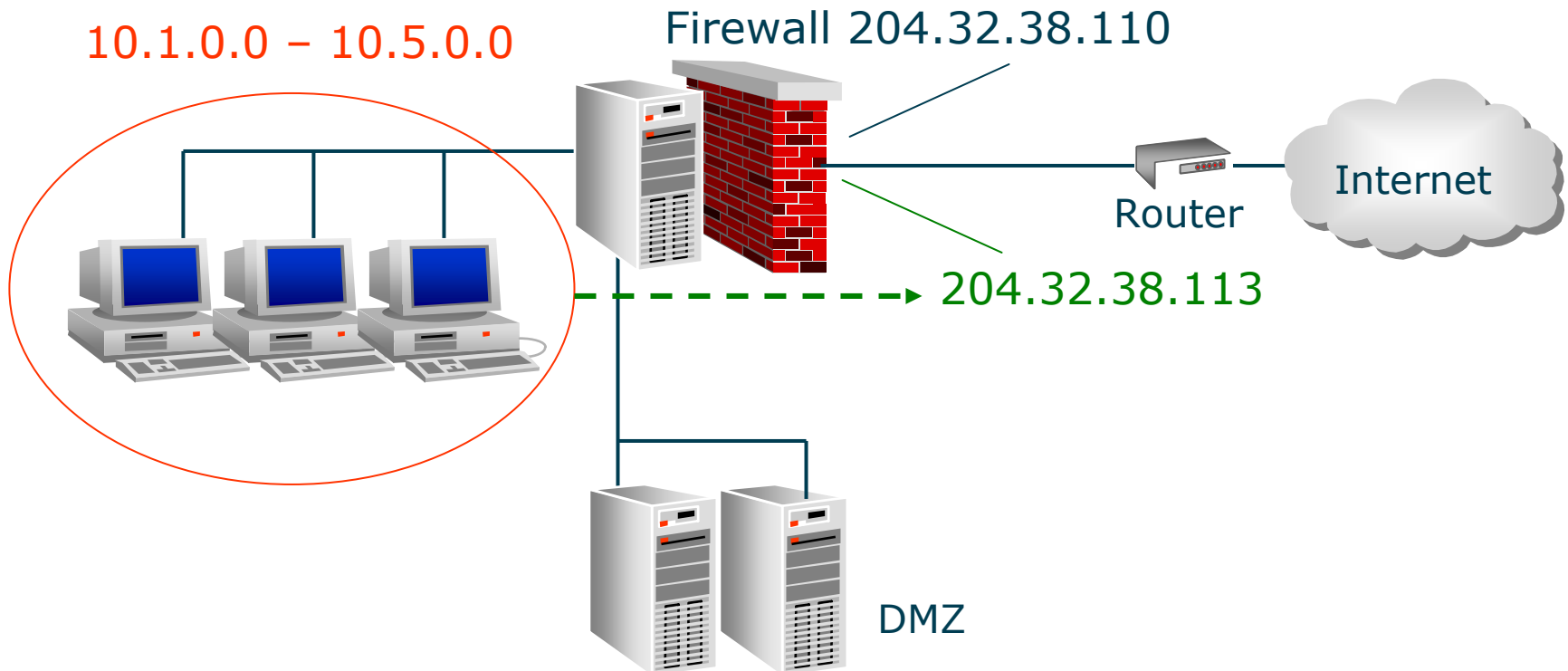
Leistungsmerkmale und Grenzen

- Network Address Translation (NAT)
 - Statische NAT



Leistungsmerkmale und Grenzen

- Network Address Translation (NAT)
 - Dynamische NAT

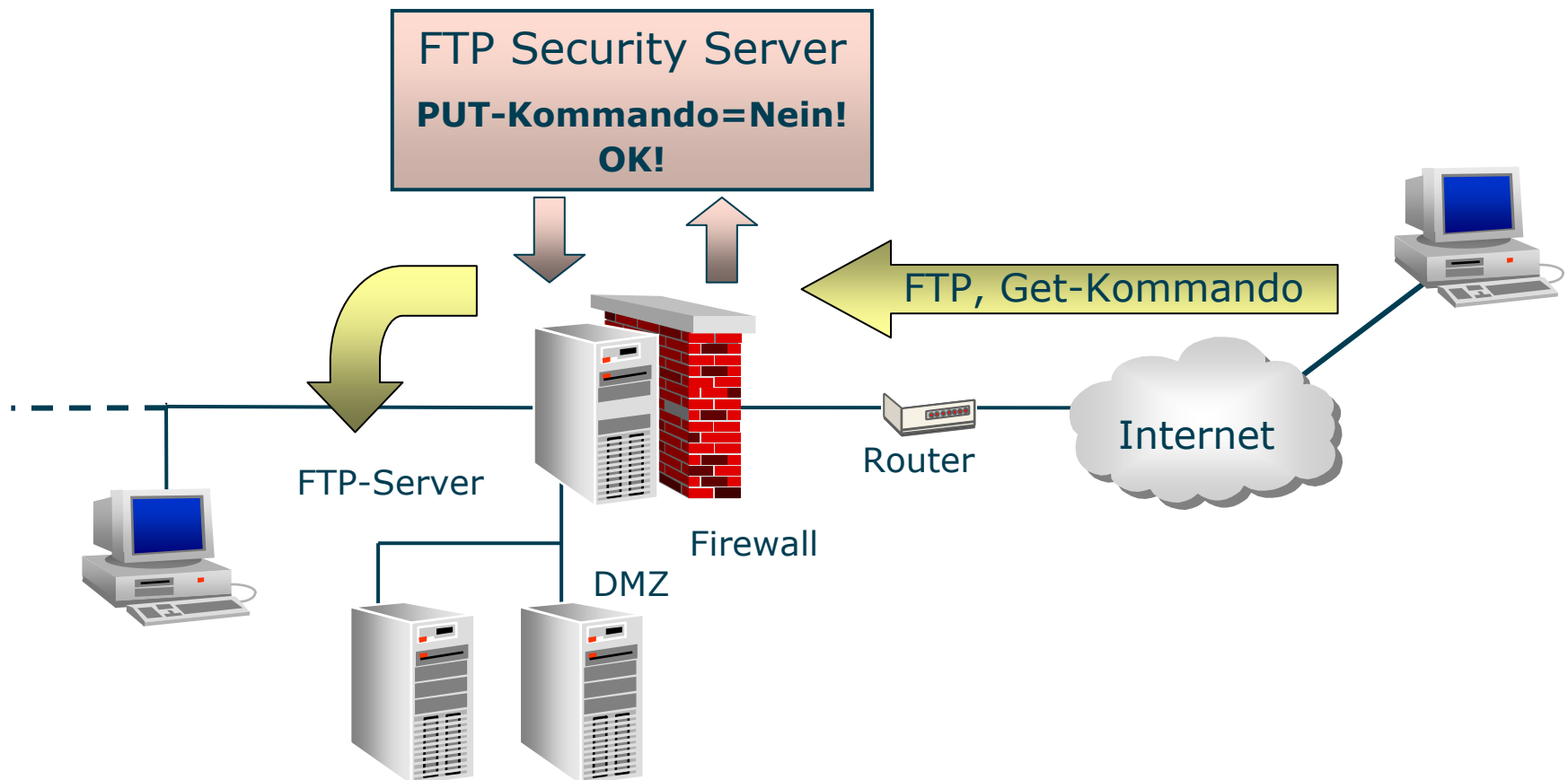


Leistungsmerkmale und Grenzen

- Integrierte Sicherheitsdienste
 - Auch „Nicht-Proxy Level Gateway Firewalls“ bieten u.U. integrierte Sicherheitsdienste für bestimmte Protokolle, um Inhalte von Verbindung prüfen oder an 3rd Party Server wie Anti Viren Scanner weiterleiten zu können.
 - Die Check Point FireWall-1 bietet sogenannte Security Server für:
 - HTTP
 - SMTP
 - FTP
 - Die Security Server arbeiten auf Schicht 7 des OSI-Modells und können so bestimmte Inhalte, wie z.B. Kommandos, URLs und Dateinamen filtern.

Leistungsmerkmale und Grenzen

- Integrierte Sicherheitsdienste
 - Z.B. FTP Security Server bei Check Point FireWall-1

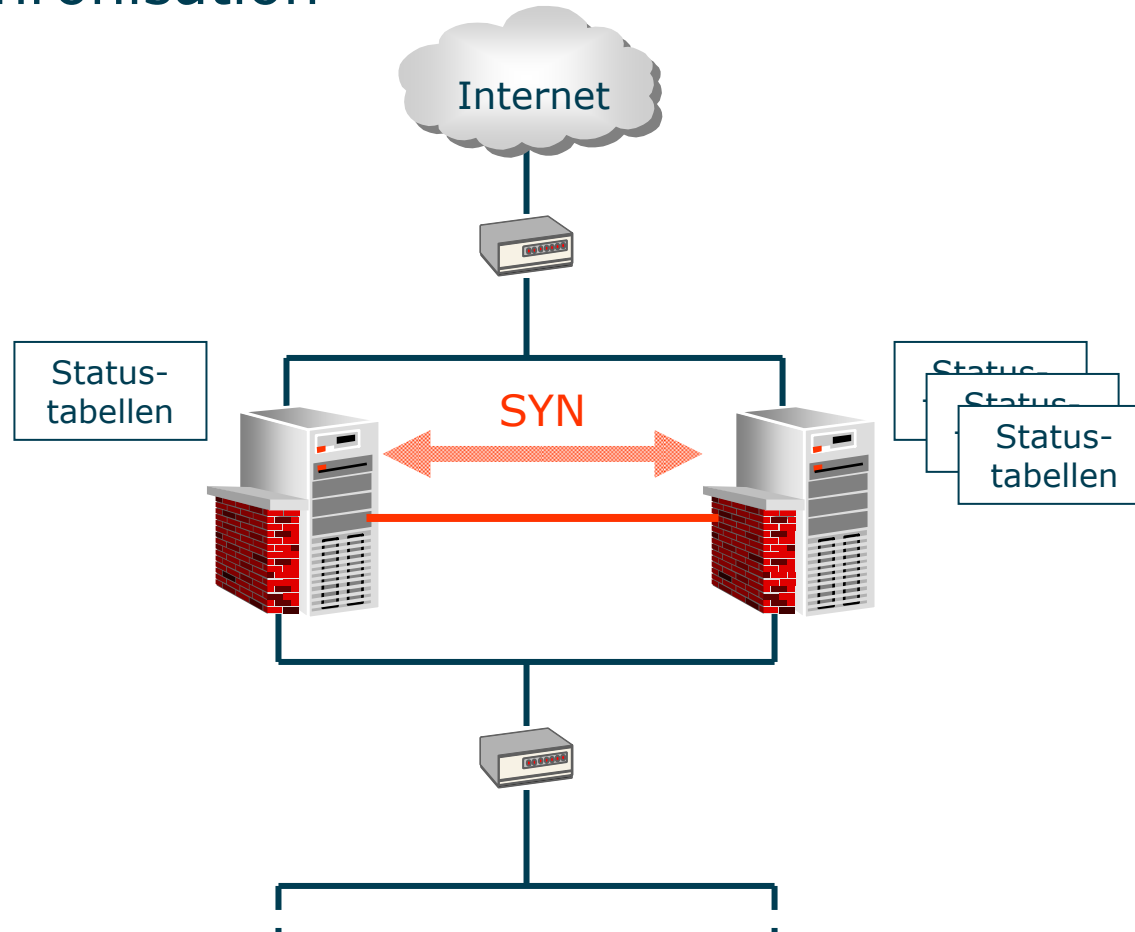


Leistungsmerkmale und Grenzen

- Synchronisation
 - Bei Hochverfügbarkeitslösungen ist die Synchronisation der Statustabellen der Firewalls eine Voraussetzung.
 - Fällt eine Firewall aus, so muss die zweite in der Lage sein, die geprüften Verbindungen zu übernehmen.
 - Dazu werden die Statustabellen in bestimmten Zeitabständen getauscht (50 ms).
 - Für die Synchronisation wird meist eine eigenständige Netzwerkverbindung verwendet.

Leistungsmerkmale und Grenzen

- Synchronisation

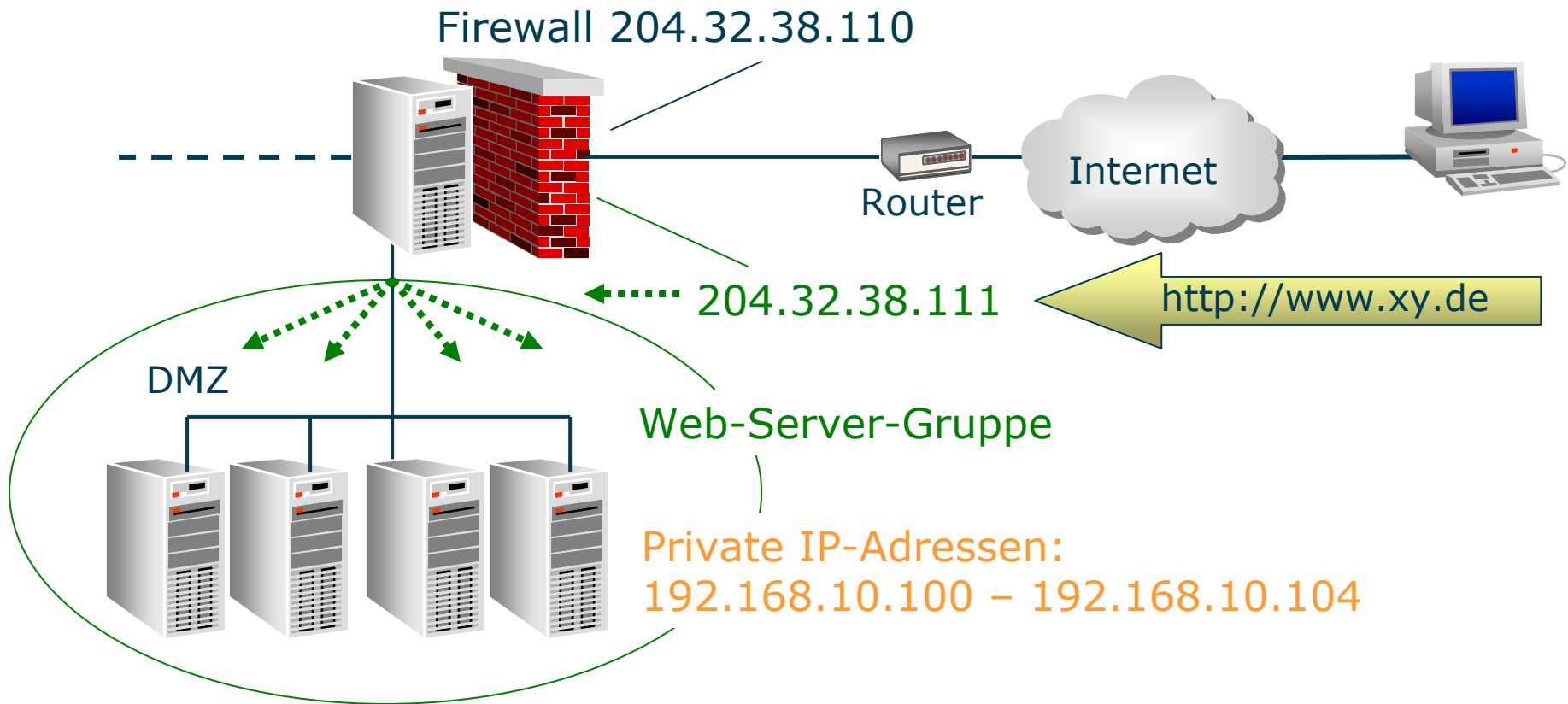


Leistungsmerkmale und Grenzen

- Load Balancing
 - Oftmals reicht ein FTP- / Web-Server für die Vielzahl der Zugriffe aus dem Internet nicht aus.
 - Einige Firewalls bieten deshalb die Möglichkeit, mehrere FTP- / Web-Server in eine logische Gruppe zusammenzufassen, die mit einer gültigen IP-Adresse angesprochen wird.
 - In die interne DMZ wird diese gültige IP-Adresse in die entsprechend ungültige IP-Adresse des ausgewählten Web-Servers übersetzt (NAT).
 - Die Firewall verteilt dann die Last unter den Web-Servern nach einem bestimmten Kriterium wie:
 - Auslastung des Web-Servers
 - Schnellste Antwort auf ein Ping
 - Der Reihe nach
 - Zufällig
 - Domänenname des Clients

Leistungsmerkmale und Grenzen

- Load Balancing

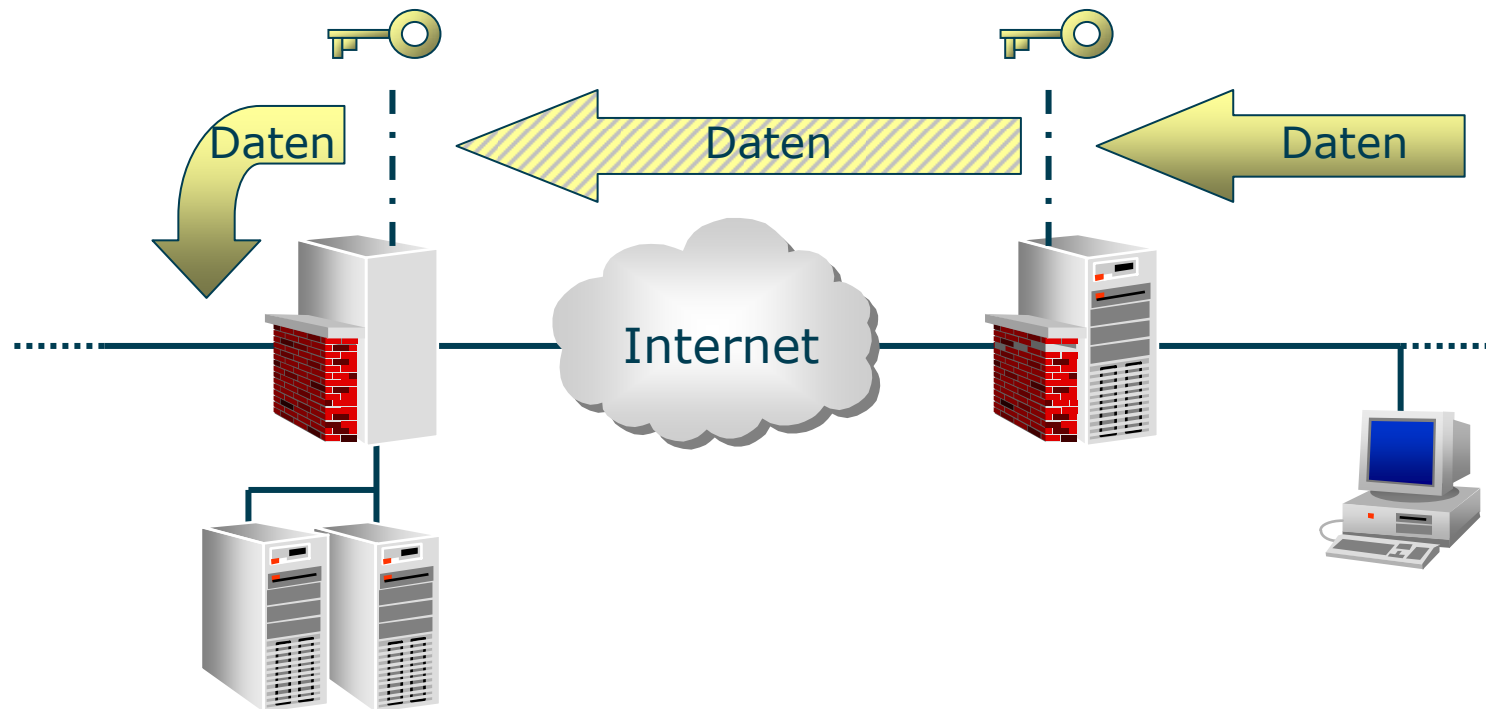


Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - Um Daten sicher über unsichere Netze übertragen zu können, müssen diese verschlüsselt werden.
 - Firewalls bieten dazu zwei Möglichkeiten, ein VPN aufzubauen:
 - Site to Site VPN
 - Zwei Firewalls, z.B. in einer Haupt- und Nebenstelle, verschlüsseln den Datenverkehr.
 - Client to Site VPN
 - Clients, z.B. Laptops von Außendienstmitarbeitern, verschlüsseln mit dem Firewall.
 - Dazu wird auf dem Rechner ein VPN-Client benötigt.

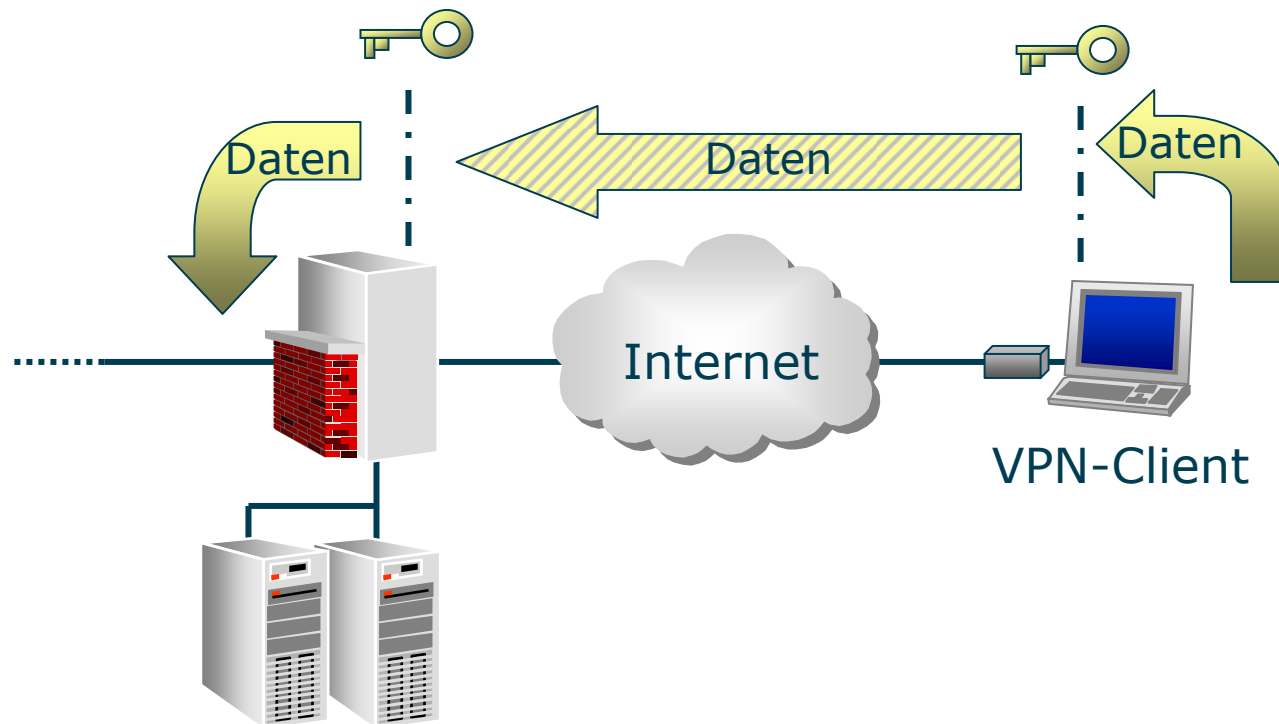
Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - Site to Site VPN



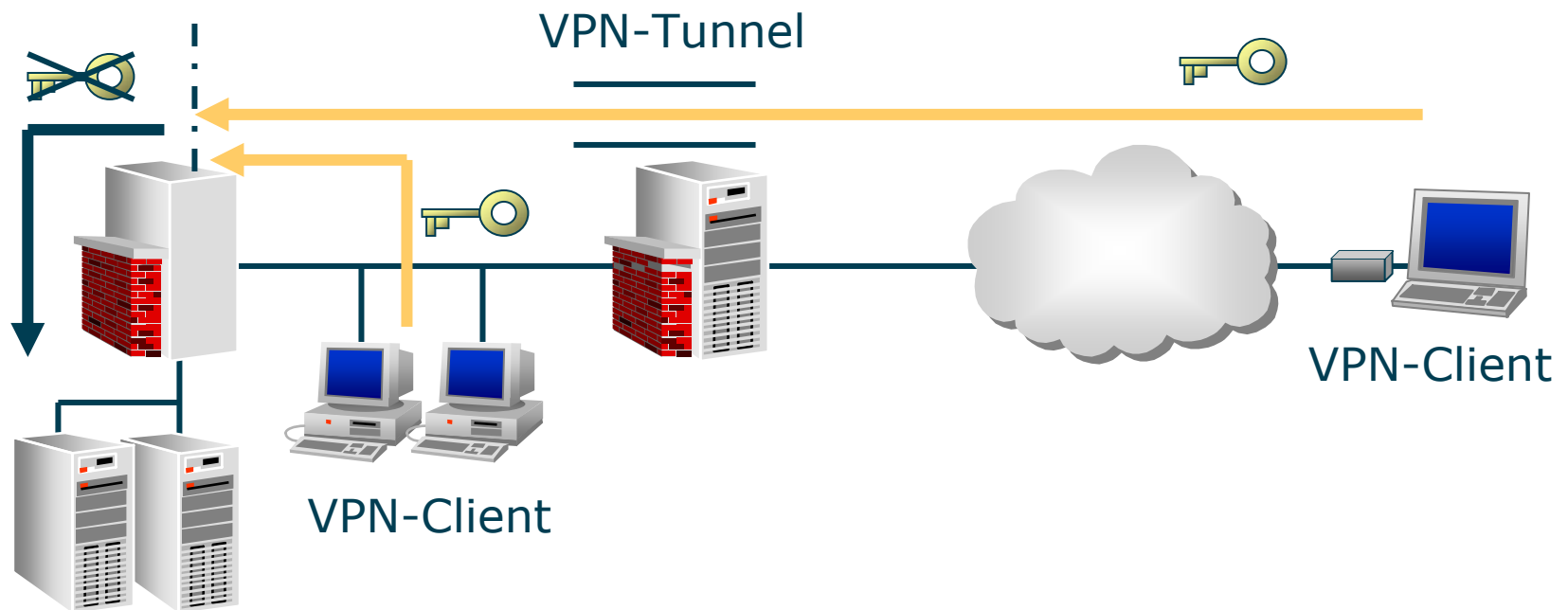
Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - Client to Site VPN



Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - Client to Site VPN
 - Die VPN-Clients können auch im internen Netz verwendet werden, um so sicheren Zugriff auf sensible Daten zu gewährleisten.



Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - Je nach Firewall-Hersteller können unterschiedliche, proprietäre Verschlüsselungsschemata eingesetzt werden.
 - Um aber eine Verschlüsselung zwischen Firewalls unterschiedlicher Hersteller zu implementieren wird heute IKE (Internet Key Exchange) eingesetzt.

Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - IKE (ISAKMP/Oakley)
 - ISAKMP (Internet Security Association and Key Management Protocol) ist der Standard der IETF
 - ISAKMP unterstützt Schlüsselübertragung und Authentisierungsdaten, unabhängig vom eingesetzten Mechanismus
 - ISAKMP unterstützt PKI (Public Key Infrastructure) und damit Zertifikate
 - Oakley ist ein Internet-Verschlüsselungsprotokoll, das zwei verifizierten Parteien den Schlüsselaustausch nach Diffie-Hellman erlaubt

Leistungsmerkmale und Grenzen

- Virtual Private Networks (VPN)
 - VPN-Clients
Bei den VPN-Clients gibt es je nach Hersteller unterschiedliche Ausführungen. Check Point z.B. bietet zwei VPN-Clients an:
 - SecuRemote
 - Dieser Client verschlüsselt die Daten, die an die definierte Firewall (Encryption Domain) geschickt werden.
 - SecureClient
 - Dieser Client besitzt zusätzlich noch eine Firewall, die den Rechner während der Verbindung zur Encryption Domain schützt.
 - Das Regelwerk für die Firewall kann von einem so genannten Policy Server im Unternehmensnetz bezogen werden.
 - Geringfügige Einstellungen können auch noch auf dem Client selbst getätigt werden.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Auch eine Firewall bietet keinen 100 %igen Schutz.
 - Eine Firewall kann nur kontrollieren, was durch sie hindurchgeht.
 - Eine Firewall kann keine „böartigen“ Benutzer im internen Netz verhindern.
 - Eine Firewall sollte immer in Kombination mit weiterer Sicherheits-Hardware und -Software verwendet werden.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Intrusion Detection
 - Um interne Angriffe oder Angriffe, die aufgrund einer Regel in das interne Netz gelangen, zu verhindern muss ein Intrusion Detection System implementiert werden.
 - Virenschutz
 - Um Virenschutz zu gewährleisten, muss Zusatzsoftware (3rd Party) und evtl. Zusatzhardware eingesetzt werden.

Leistungsmerkmale und Grenzen

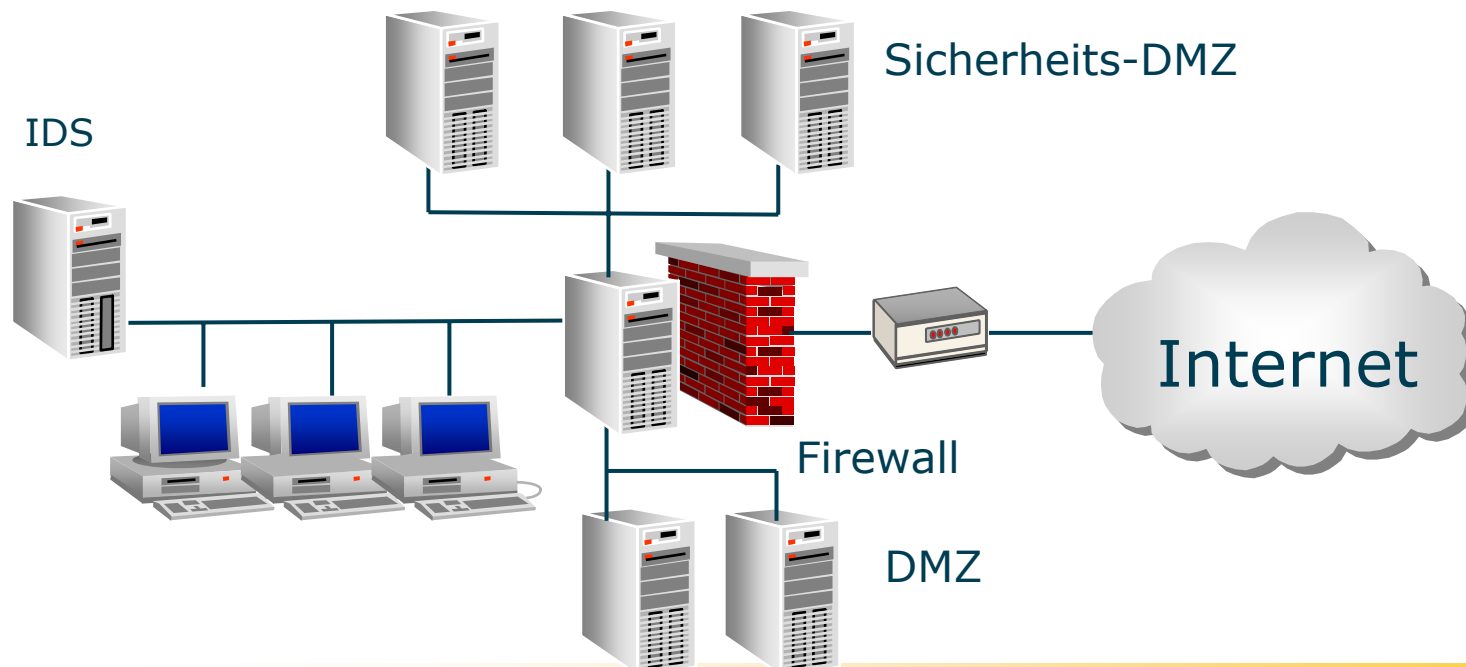
- Grenzen von Firewalls
 - URL-Filterung
 - Da die Filterung von URLs bei Firewalls meist nur begrenzt möglich ist, kann hier ebenfalls 3rd Party-Software eingesetzt werden.
 - Authentifizierung
 - Um Benutzer sicher und komfortabel zu authentifizieren werden heute meist Smartcards oder ähnliche Verfahren verwendet.
 - Dies geschieht ebenfalls über 3rd Party-Software z.B. RADIUS, TACACS, TACACS+.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls

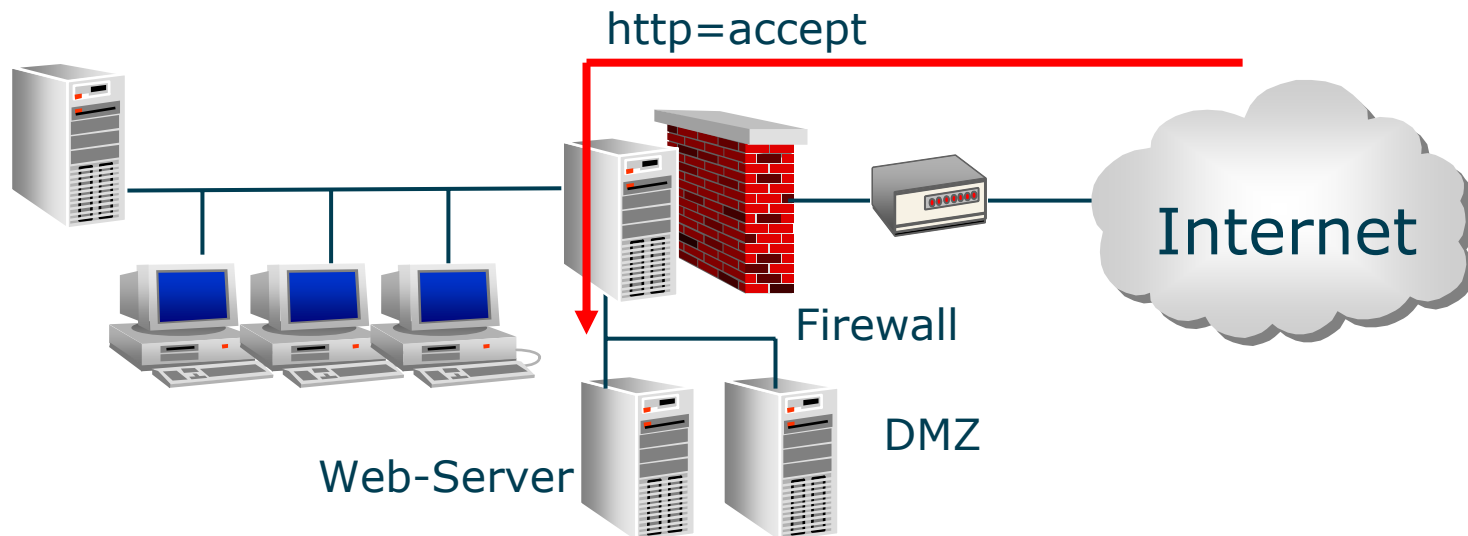
- Die Hersteller bieten zur Anbindung von 3rd-Party-Servern Schnittstellen in der Firewall an.

Anti Viren Server / UFP-Filtering Server / Authentication Server



Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Die meisten erfolgreichen Angriffe zielen heute durch die Firewall hindurch auf die Web/ Application Server.
 - Dabei werden sowohl Bugs, Programmierfehler als auch Misskonfigurationen auf den Servern ausgenutzt.



Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Eine Firewall wird laut ihres Regelwerks Dienste wie z.B. HTTP akzeptieren, nicht aber den Inhalt der Verbindung detailliert prüfen.
 - Innerhalb der verifizierten Verbindung kann ein Angriff durchgeführt werden. Beispiele solcher Angriffe sind:
 - Hidden Field Manipulation
 - Auf Web-Seiten werden oft sogenannte „versteckte Felder“ verwendet. Diese lassen sich bei Programmierfehlern am Browser anzeigen (Source) und verändert an den Server zurück schreiben.
 - Cookie Poisoning
 - Ein Erhaltenes Cookie wird auf dem Client verändert und verwendet so, wenn bei der nächsten Sitzung zurückgesandt, evtl. eine andere ID.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Beispiele von HTTP-Angriffen:
 - Backdoor und Debug Optionen
 - Evtl. hat eine Applikation versteckte Optionen, die erlauben, einen speziellen Parameter oder eine Sequenz zu senden um so an Daten zu gelangen
 - Buffer Overflow
 - Viele Applikationen reagieren sensibel auf zu große Datenmengen. Die „Übermengen“ führen zum Absturz der Applikation.
 - Stealth Commanding
 - Anstelle von geforderten, persönlichen Daten wird auf einer Web-Seite im Eingabefeld ein Kommando eingegeben

Leistungsmerkmale und Grenzen

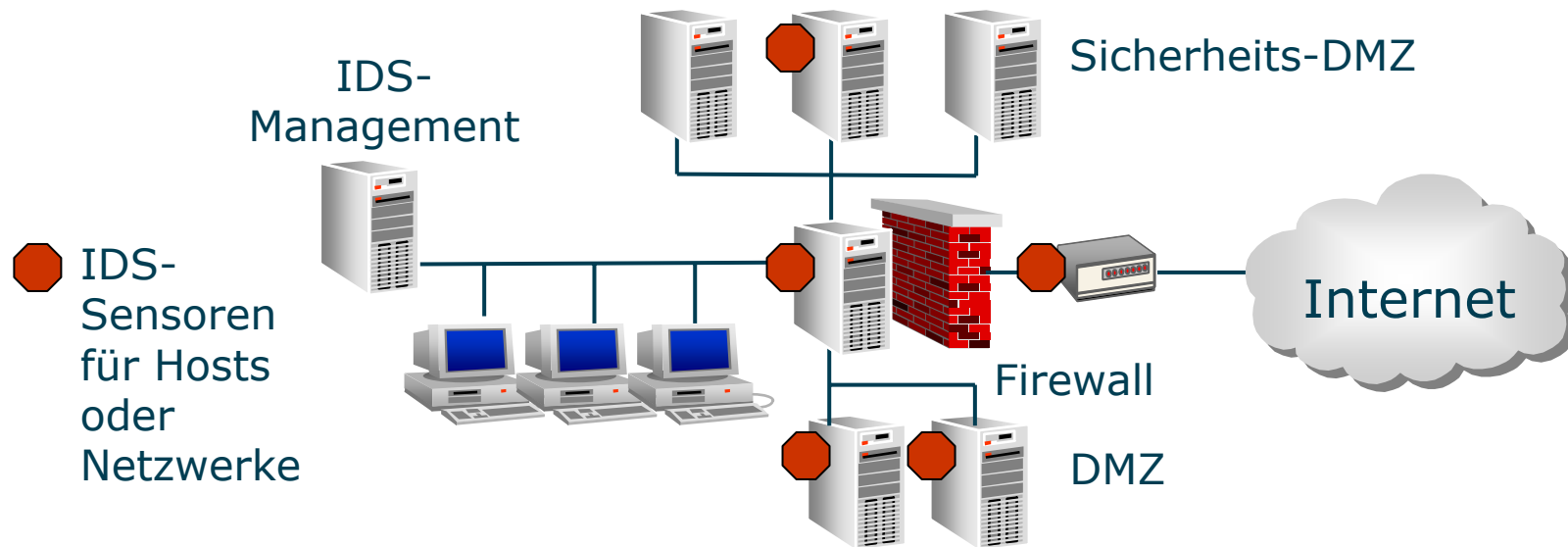
- Grenzen von Firewalls
 - Beispiele von HTTP-Angriffen:
 - Cross Site Scripting
 - Ein Hacker erstellt über ein Eingabefeld, z.B. Kommentarfeld, einen Link auf eine andere Seite.
 - Forceful Browsing
 - Durch Erraten von Datei- und Verzeichnisnamen kann ein Hacker diese im Pfad direkt verwenden, ohne dem geschäftsmäßigen Verlauf der Seite zu folgen.
 - Parameter Tampering
 - Parameter werden verwendet, um vom Client Informationen zu erhalten. Diese können evtl. im URL auf dem Client verändert werden, um so auf dem Server an Daten zu gelangen.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Wie können Angriffe auf Applikationen verhindert / entdeckt werden?
 - Die Server müssen sicher eingerichtet werden !! Sicherheits-Scans, wie z.B. QualysGuard, helfen dabei.
 - Spezielle Software, wie z.B. SANCTUM, schützt einen Web-Server.
 - Viele Intrusion Detection Systems bieten für Server mit Applikationen spezialisierte Agenten, die die Zugriffe überwachen.

Leistungsmerkmale und Grenzen

- Grenzen von Firewalls
 - Wie können Angriffe auf Applikationen verhindert / entdeckt werden?



Hochverfügbarkeitslösungen

- Da eine Firewall als „Choke Point“, also als zentraler Einstiegspunkt in das sichere Netz fungiert, sollte der Aufbau ausfallssicher gestaltet werden.
- Zudem kann bei vielen Zugriffen, z.B. auf Web-Server in der DMZ, eine Überlastung der Firewall auftreten.
- Um Ausfallsicherheit und Performance zu gewährleisten, werden drei Lösungsansätze verfolgt:
 - Stand By
 - Load Sharing
 - Full Cluster
- Diese Lösungen sind meist nur mit Zusatzsoftware für die Firewalls zu erreichen.
- Dabei werden mindestens zwei Firewalls „parallel“ geschaltet.

Hochverfügbarkeitslösungen

- Hersteller von Hochverfügbarkeitslösungen
 - Die bekanntesten Hersteller von Hochverfügbarkeitslösungen für Firewalls sind:
 - Stonesoft, Finnland
 - Stand By, Load Sharing, Full Cluster
 - Nokia, Finnland
 - Stand By, Load Sharing
 - RainFinity, USA
 - Stand By, Full Cluster

Hochverfügbarkeitslösungen

- Philosophien
 - Die Hersteller vertreten zwei unterschiedliche Philosophien:
 - Die Stonesoft- und RainFinity-Produkte setzen auf bestehenden Betriebssystemen und Firewall-Produkten auf.
 - Nokia setzt auf ein eigen entwickeltes, UNIX-basierendes Betriebssystem (IPSO), das angepasst ist und zusammen mit Check Point FireWall-1 und der PC-basierenden Hardware als Black Box-Lösung angeboten wird.
 - Die nachfolgenden Beispiele beziehen sich auf die Stonesoft-Lösung.

Hochverfügbarkeitslösungen

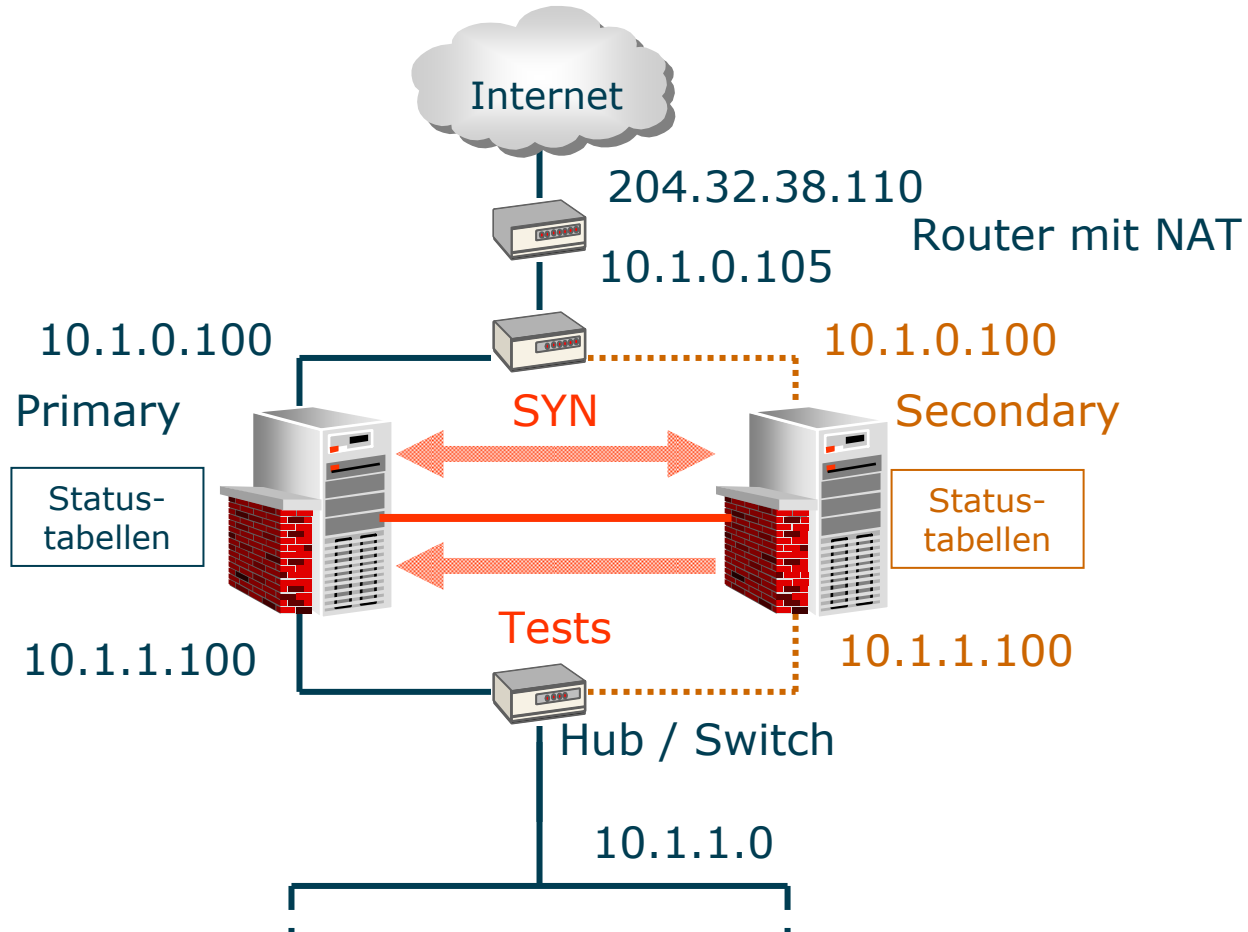
- Stand By-Lösung
 - Bei der Stand By-Lösung ist eine Firewall (Primary) aktiv, während die zweite inaktiv als „Schläfer“ (Secondary) die erste überwacht.
 - Die Primary als auch die Secondary erhalten für das äußere Netz die gleiche IP- und MAC-Adresse.
 - Die Primary als auch die Secondary erhalten für das innere Netz die gleiche IP- und MAC-Adresse.
 - Die Secondary führt über eine, eigenständige Netzwerkverbindung, Tests auf und über die Primary durch.
 - Getestet werden Betriebssystemfehler, Konfigurationsfehler, Netzwerkkartenfehler, Verbindungen zu Routern, z.T. automatisch, z.T. über ein konfigurierbares Testsystem

Hochverfügbarkeitslösungen

- Stand By-Lösung
 - Fail Over
 - Die Status-Tabellen der Primary werden mit der Secondary synchronisiert.
 - Fällt die Primary-Firewall aus, so übernimmt die Secondary die Verbindungen.
 - Die Übernahme, das sogenannte Fail Over, erfolgt transparent, ohne dass die Nutzer einer Verbindung dies bemerken.
 - Eine Steigerung der Performance wird dadurch nicht erreicht, lediglich eine Ausfallsicherheit.

Hochverfügbarkeitslösungen

- Stand By-Lösung

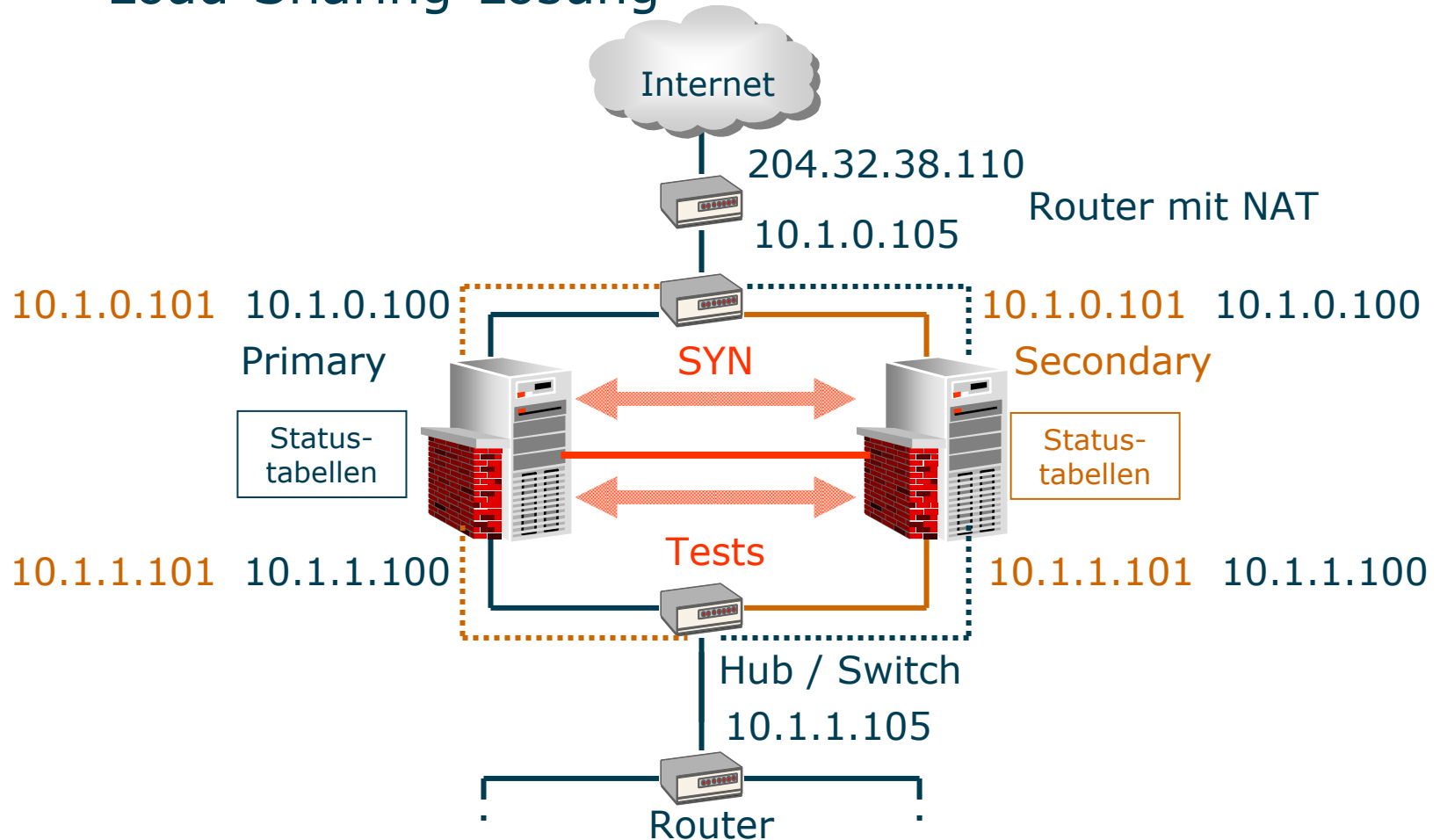


Hochverfügbarkeitslösungen

- Die Load Sharing-Lösung
 - Bei Load Sharing-Lösungen haben beide Firewalls jeweils zwei Netzwerkkarten in das innere und das äußere Netzwerk.
 - Jeweils eine Karte der jeweiligen Firewalls (Primary /Secondary) ist aktiv geschaltet.
 - Die zweite Karte ist im Normalbetrieb inaktiv.
 - Die Last wird zwischen den beiden Firewalls mittels statischen Routen verteilt.
 - Die Firewalls testen sich gegenseitig.
 - Bei Ausfall einer Firewall übernimmt die andere transparent, mittels der zweiten Netzwerkkarte und der IP- bzw. MAC-Adresse, die Verbindungen der ausgefallenen.
 - Im Normalbetrieb wird eine Steigerung der Performance erreicht, im Fehlerfall kann die aktive Firewall überlastet werden.

Hochverfügbarkeitslösungen

- Load-Sharing-Lösung



Hochverfügbarkeitslösungen

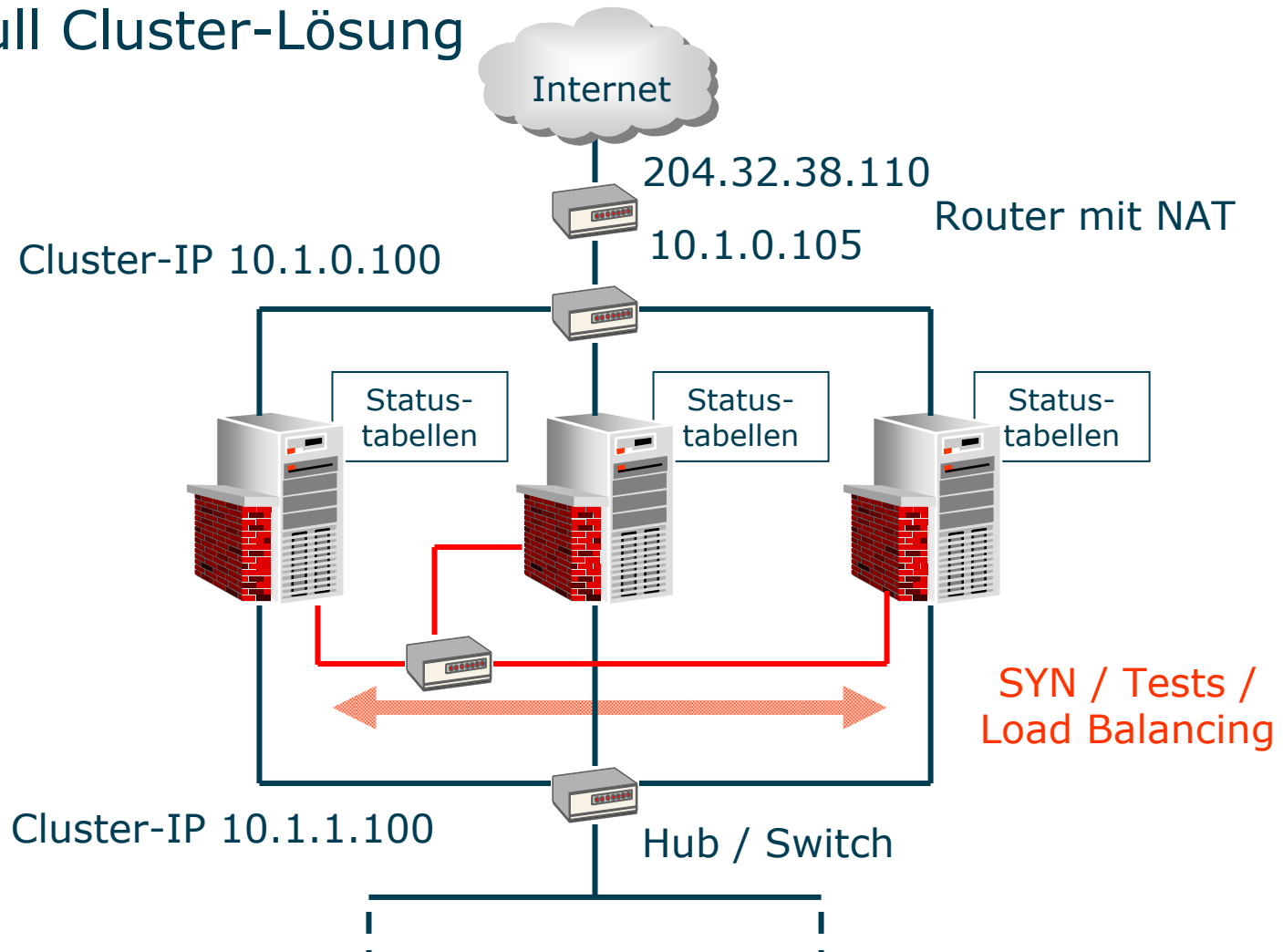
- Full Cluster-Lösung
 - Die Full Cluster-Lösung arbeitet mit Load Balancing.
 - Load Balancing ist ein Prozess, der jedem Mitglied (Node) eines Clusters exakt die gleiche Last zuweist.
 - Der kombinierte Durchsatz aller Nodes ist der Gesamtdurchsatz des Clusters.
 - Ein Cluster kann aus bis zu 16 gleichberechtigten Nodes bestehen.
 - Das gesamte Cluster erhält für das äußere als auch das innere Netzwerk eine IP-Adresse.

Hochverfügbarkeitslösungen

- Full Cluster-Lösung
 - Die Pakete werden an jeden Knoten weitergeleitet (Multi cast IP- oder MAC-Adresse).
 - Über eine eigenständige Netzwerkverbindung wird anhand eines Algorithmus der Node berechnet, der im Cluster ein ein- bzw. ausgehendes Paket weiterleiten und verwalten muss.
 - Im Normalbetrieb ist jeder Node aktiv, fällt ein Node aus, so übernehmen die verbleibenden symmetrisch dessen Last.

Hochverfügbarkeitslösungen

- Full Cluster-Lösung



Hochverfügbarkeitslösungen

- Wann wird welche Lösung eingesetzt?
 - Quelle: Stonesoft
 - Bei Durchsatzraten von weniger als 50 MBit/s
 - Stand By oder Load Sharing
 - NT bis 30 MBit/s
 - UNIX bis 50 MBit/s
 - Bei Durchsatzraten zwischen 50 MBit/s und 100 MBit/s
 - Load Sharing
 - Bei Durchsatzraten von mehr als 100 MBit/s
 - Full Cluster

Wir freuen uns über Ihr Feedback



Network Training and Consulting GmbH
Weidenauer Straße 15
57078 Siegen
siegen@networktraining.de

Network Training and Consulting Südwest GmbH
Gutenbergstraße 13
70771 Leinfelden-Echterdingen
stuttgart@networktraining.de

Bundesweite Infoline: 0180 11 77 333
(Festnetz / Telekom 4,6 Cent / Minute)