Netzwerksicherheit

Zuverlässigkeit und Skalierbarkeit

Stephen Wolthusen

Fraunhofer IGD Institut Graphische Datenverarbeitung

Konflikte

- Zur Einschränkung von Möglichkeiten zur Kompromittierung müssen präzise definierte und kontrollierte Übergangspunkte zwischen Bereichen unterschiedlicher Sicherheit definiert werden
  - Wird als „choke point“ bezeichnet
- Dieselbe Konstruktion wird aus Sicht der Zuverlässigkeit anders bezeichnet: „single point of failure“
- Ähnliche Probleme sind auch bei Skalierbarkeit gegeben
  - Einzelne Komponenten haben begrenzte Leistungsfähigkeit, Kosten steigen unverhältnismäßig
  - Mehrere Komponenten müssen parallel betrieben werden

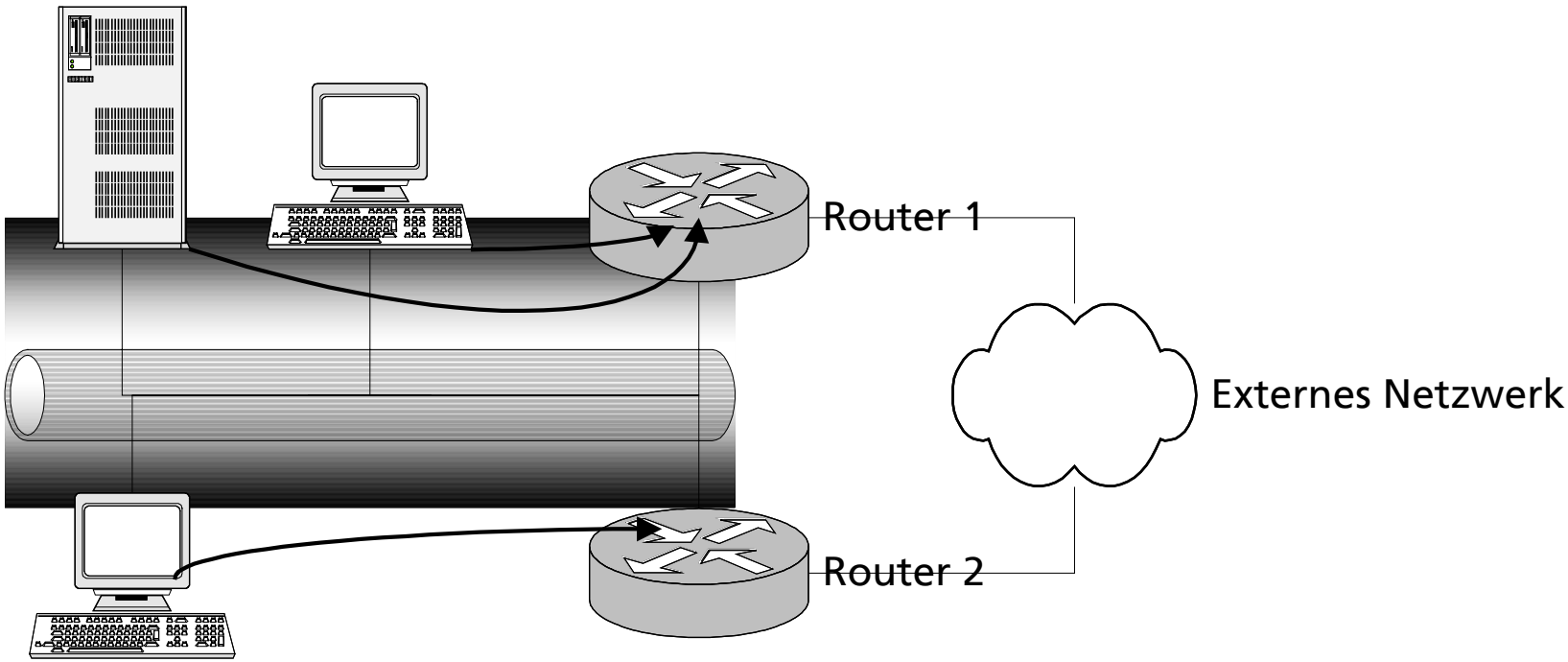
Redundanz von Netzwerk-Komponenten

- Sicherheitsverlust bei Redundanz
  - Aktivitätsmuster sind über mehrere Knoten verteilt
    - erfordert Konsolidierung von Revisionsdaten
    - Eindeutige Sequenzierung meist nicht möglich
    - Vergleichbarkeit erfordert äquivalente Konfiguration
  - Sicherheit darf nicht nur auf Kontrolle von Informationsflüssen beschränkt betrachtet werden: Verfügbarkeit
- Verfügbarkeit rechtfertigt in der Regel Reduktionen in anderen Sicherheitsparametern

Virtual Router Redundancy Protocol (VRRP)

- Die VRRP-IETF-Arbeitsgruppe wurde im Juni 1997 gegründet
- Ziel: Definition eines Protokolls, mit dem mehrere Router zu einem virtuellen Router zusammengefaßt werden können. Router wird mit virtueller Adresse (IPv4, IPv6) angesprochen
  - Rekonfiguration von Endgeräten erfordert bei statischer Konfiguration manuelle Änderung bei Router-Ausfall
  - DHCP besitzt keine Authentisierungsmechanismen, IRDP erlaubt Angreifer sich als neuer Default Router auszugeben
  - IRDP läßt zwischen Updates mehrere Minuten verstreichen
    - Trotz redundantem Router Ausfall bis Konvergenz

Redundante Router ohne Umleitung



ARP-Caching

- ARP-Einträge werden von den meisten Implementierungen in Caches gehalten (Windows 2000/XP: 2 Minuten, Solaris 8/9: 5 min im ARP-Cache, 20 min Abbildung IP/MAC)
  - Einfache Übernahme der IP-Adresse genügt daher nicht
  - ARP verfügt ebenfalls über keine Authentisierung
    - Verlängerung der ARP-Lebensdauer oder statische ARP-Einträge zur Verhinderung von Spoofing
  - Statische ARP-Adressen erfordern Mechanismus zur Übernahme von IP- und ARP-Adressen
    - wird von VRRP bereitgestellt

VRRP-Konzepte

- „Master“, „Backup“-Knoten
  - Gruppe wird durch Virtual Router ID identifiziert
  - Master wird aus Menge verfügbarer Knoten gewählt
  - Prioritäten können Wahl beeinflussen
- Kommunikation der VRRP-Knoten untereinander mit Multicast-Datagrammen auf `224.0.0.18` (link local) mit TTL 255 und eigenem IP-Protokoll (112)
  - Stellen sicher, daß selbst bei Fehlkonfiguration VRRP-Datagramme nicht über die Grenzen eines lokalen Netzwerkes hinaus verbreitet werden können

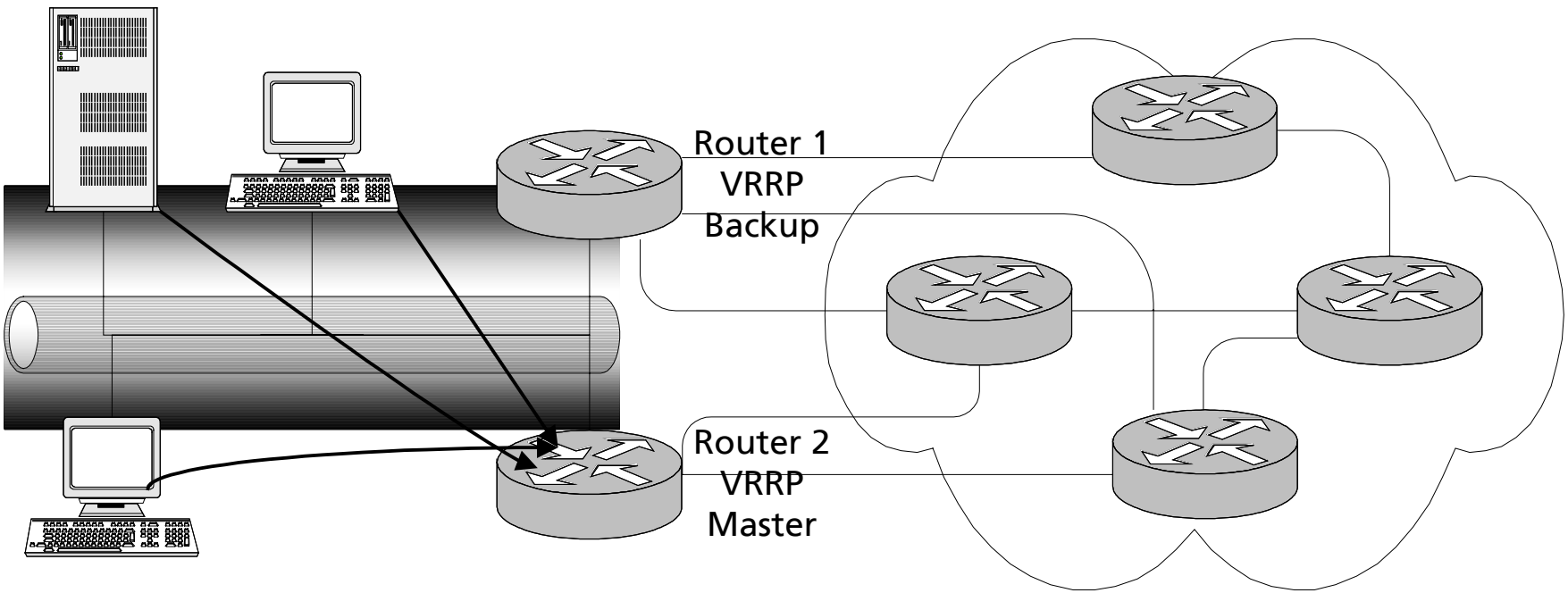
Inhalt der VRRP-Datagramme

- Version: 4 Bit; aktuell (RFC2338) ist Version 2
- Type: 4 Bit, Typ der Nachricht. Nur ADVERTISEMENT ist definiert
- VRID: 8 Bit, identifiziert Router-Gruppe. In einem LAN eindeutig
- Priority: 8 Bit, Master=255, Rest von 1-254; 0= Master gibt auf
- Count IP: 8 Bit, Anzahl IP-Adressen in Nachricht
- Auth Type: 8 Bit, Authentisierungsmechanismus (keine, Paßwort, IPSec)
- Advert Interval: 8 Bit, Meldungsintervall in Sekunden (normal 1)
- Checksum: 16 Bit, nach RFC 1071
- IP Addresses: 32 x n Bit, Adressen des virtuellen Routers
- Auth Data: 32 x n Bit, Abhängig von Auth Type

VRRP-Semantik

- Nur Master reagiert auf ARP-Anfragen
  - MAC wird aus IANA-OUI-Pool vergeben: Max. 255 VRIDs
- Neuwahl wenn Advertisement mit Priority=0 oder bei fehlendem Advertisement
  - Jeder Router hat Skew Time, abhängig von Priorität
- Authentisierung via Paßwort (Klartext): 8 Bytes
- Authentisierung via IPSec: Statische SA, SPI für HMAC MD5 nach RFC2403 ist vorgegeben
- ARP Spoofing kann eliminiert werden: statische Zuordnung

Redundante Router mit VRRP



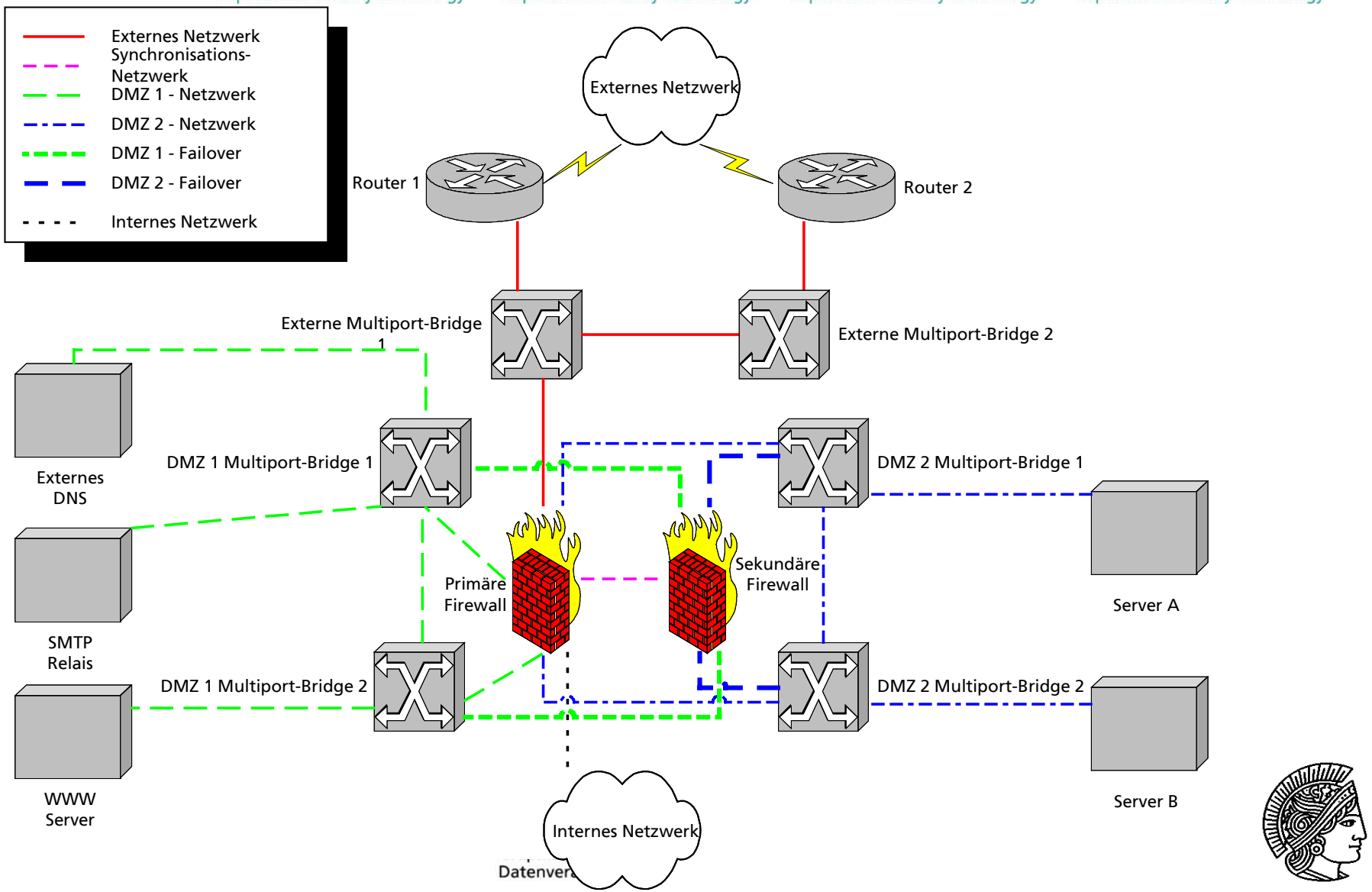
Hot Standby Router Protocol (HSRP)

- Proprietäres Protokoll von Cisco, im Dezember 1997 mit IOS 11.3 eingeführt, im März 1998 als informativer RFC 2281 eingereicht
- Funktionen analog zu VRRP
  - Multicast-Kommunikation auf Adresse `224.0.0.2`
  - MACs entstammen dem Cisco OUI (`00-00-0C-07-AC`)
  - Erlaubt ebenfalls maximal 255 Standby Groups je LAN
  - Verwendet UDP anstelle eines eigenen Protokolls
  - Authentisierung erfolgt maximal über Klartext-Paßworte
    - Default-Paßwort „`cisco`“ - wird selten geändert...

Failover / Hot Standby (1)

- Verfügbarkeit redundanter Hardware, Software die mit gleichem Netz verbunden ist und in der Lage ist, sämtlichen Datenverkehr bei Versagen eines Knoten auf anderen Knoten umzustellen
  - meist auf zwei Knoten beschränkt
  - virtuelle MAC-, IP-Adressen
- Synchronisation erfolgt meist über „Heartbeat“-Netzwerk
  - Zustandsinformationen können umfangreich sein, müssen aber vollständig übertragen werden: Gefahr bei Fehlern
  - Zustandsinformationen sind sicherheitsrelevant

Hot Standby mit Failover



Failover / Hot Standby (2)

- Versagenserkennung ist auch bei exotischen Fehlern (z.B. eigene Failover-Schnittstelle) notwendig: „Byzantine Generals Problem“
- Vorteile:
  - Einfach zu implementieren, kommerzielle und freie Lösungen existieren
  - Redundanz der Firewall-Infrastruktur ist gewährleistet
  - Weitere Kriterien (neben Aktivität) können bei Übernahme berücksichtigt werden
  - Wartungsarbeiten können ohne Unterbrechung der Dienste für Nutzer erfolgen

Failover / Hot Standby (3)

- Nachteile von Failover-Mechanismen
  - Kein Geschwindigkeitsgewinn, in pathologischen Situationen sogar Verlangsamung durch Synchronisationsmechanismen
  - Sekundäre Einheit muß identisch zu primärer Einheit sein
    - Wartungskosten
  - Übernahme langlebiger Verbindungen (z.B. FTP-Datentransfers) ist nicht bei allen Implementierungen möglich

Lastausgleich: DNS Round Robin

- Seit BIND 4.9 bzw. NT 4.0 SP 4 verfügbarer Mechanismus
- Bei Verfügbarkeit mehrerer IP-Adressen für einen symbolischen Namen wird sequentiell bei jeder neuen Anforderung ein anderer Eintrag als DNS-Antwort geliefert. Nachteile:
  - Keine echte Lastverteilung
  - DNS-Antworten werden von Clients in Caches gehalten
  - Authentisierung von Adressen ist nicht gewährleistet
  - Einträge ausgefallener Knoten bleiben in Caches auf Client und Tabellen der Server zurück, transparenter Failover nicht möglich

Probleme bei Verwendung von RIP für Lastausgleich

- Einfaches, seit Jahren bewährtes Protokoll
- Für Lastausgleich nicht geeignet. Einige Nachteile:
  - Verzögerungen, Kosten für einzelne Verbindungen werden von RIP nicht berücksichtigt: Nur Anzahl Hops
  - Konvergenz der Routen ist langsam insbesondere bei großen Netzwerken
  - RIP kann VLSM nicht verarbeiten
  - Periodische Versendung der gesamten Routing-Tabelle als Broadcast
  - Maximal 15 Hops in einem Netzwerk

Open Shortest Path First (OSPF)

- Routing-Protokoll für interne Netzwerke (IGP), von der IETF wurde 1988 Arbeitsgruppe gegründet, erste Version 1991
  - derzeit aktuell ist Version 2, 1998 in RFC 2328 definiert
- Anders als RIP (basiert auf Bellman-Ford-Algorithmus) beruht OSPF auf Gewichtung von Verbindungen. Weitere Vorteile
  - Rudimentäre Authentisierung
  - Unterstützung von VLSM
  - Aggregierung von Routen

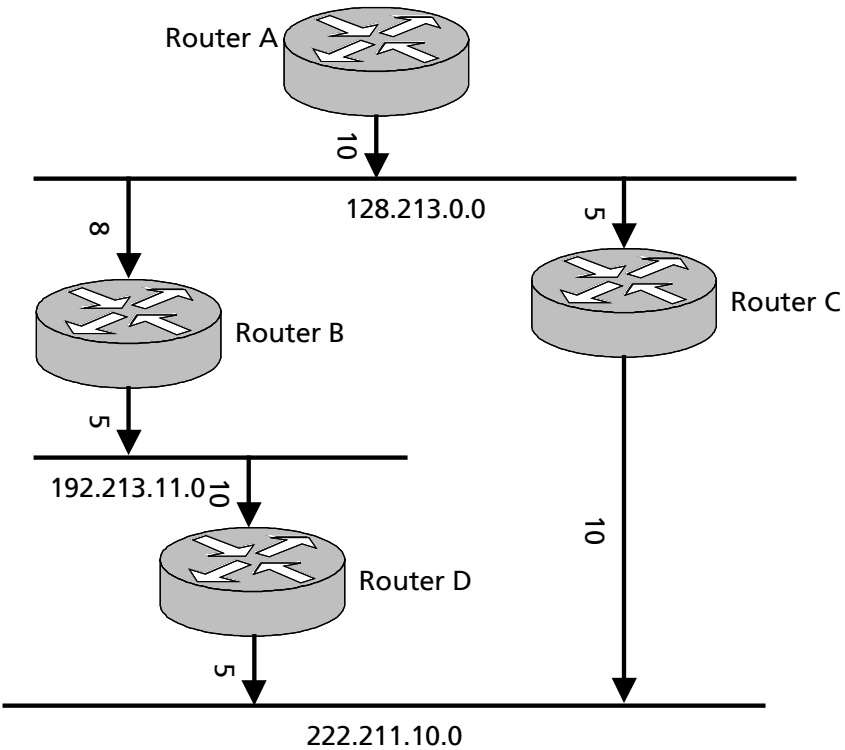
Vorzüge von OSPF

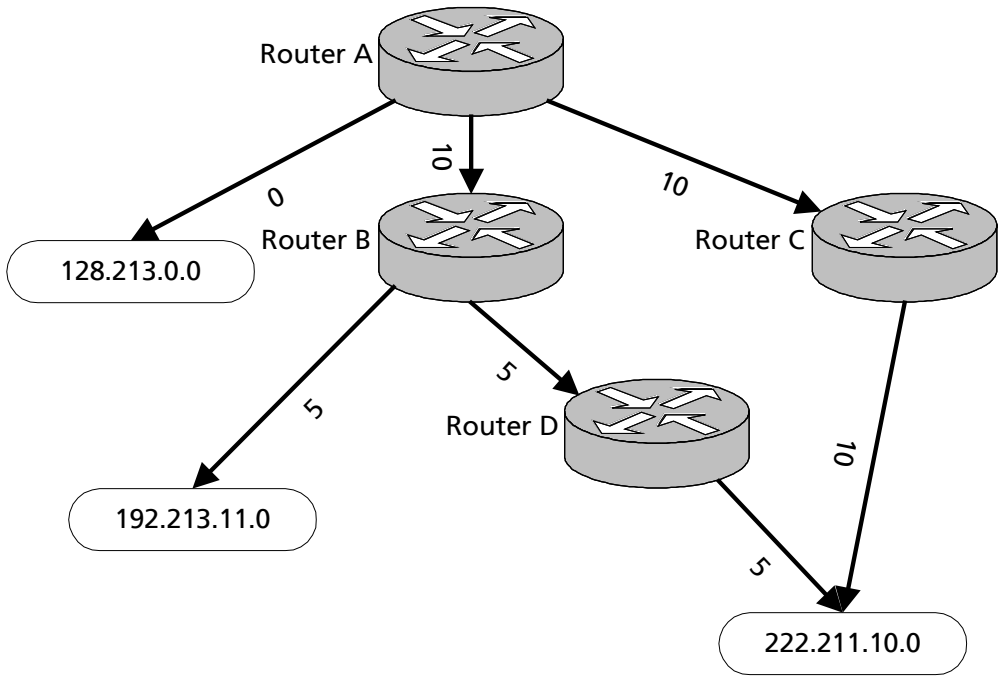
- Verbindungszustand wird via IP Multicasting übertragen
  - Pakete können mit IPSec gesichert werden
  - Zustandsübermittlung erfolgt nur bei Veränderung in relevante Zuständen
    - Ansonsten versendet OSPFs periodisch nur Nachrichten konstanter Größe
  - Konvergenz ist schnell, Zustände werden sofort aktualisiert
  - Gewichtung von Verbindungen erlaubt effizienten Lastausgleich
  - OSPF erlaubt mehrere Authentisierungsmechanismen

Link State Algorithmus in OSPF

- 1. Nach Initialisierung oder Änderung oder Zustandsänderung wird ein Link State Advertisement erzeugt (mit allen Link States)
- 2. Alle Knoten tauschen jeweilige Link States durch Flutungs-Verfahren aus. Jeder Knoten, der ein LSU erhält muß diesen in eigene Link State Database eintragen und an alle erreichbaren Knoten weiterleiten
- 3. Nachdem die Datenbank jedes Routers vollständig ist berechnet jeder Router einen Baum, der die günstigsten Wege für alle Zielknoten enthält
- Ergebnis: Tabelle mit nächstem Hop, Kosten für Verbindung

Berechnung kürzester Wege in OSPF: Dijkstra-Algorithmus

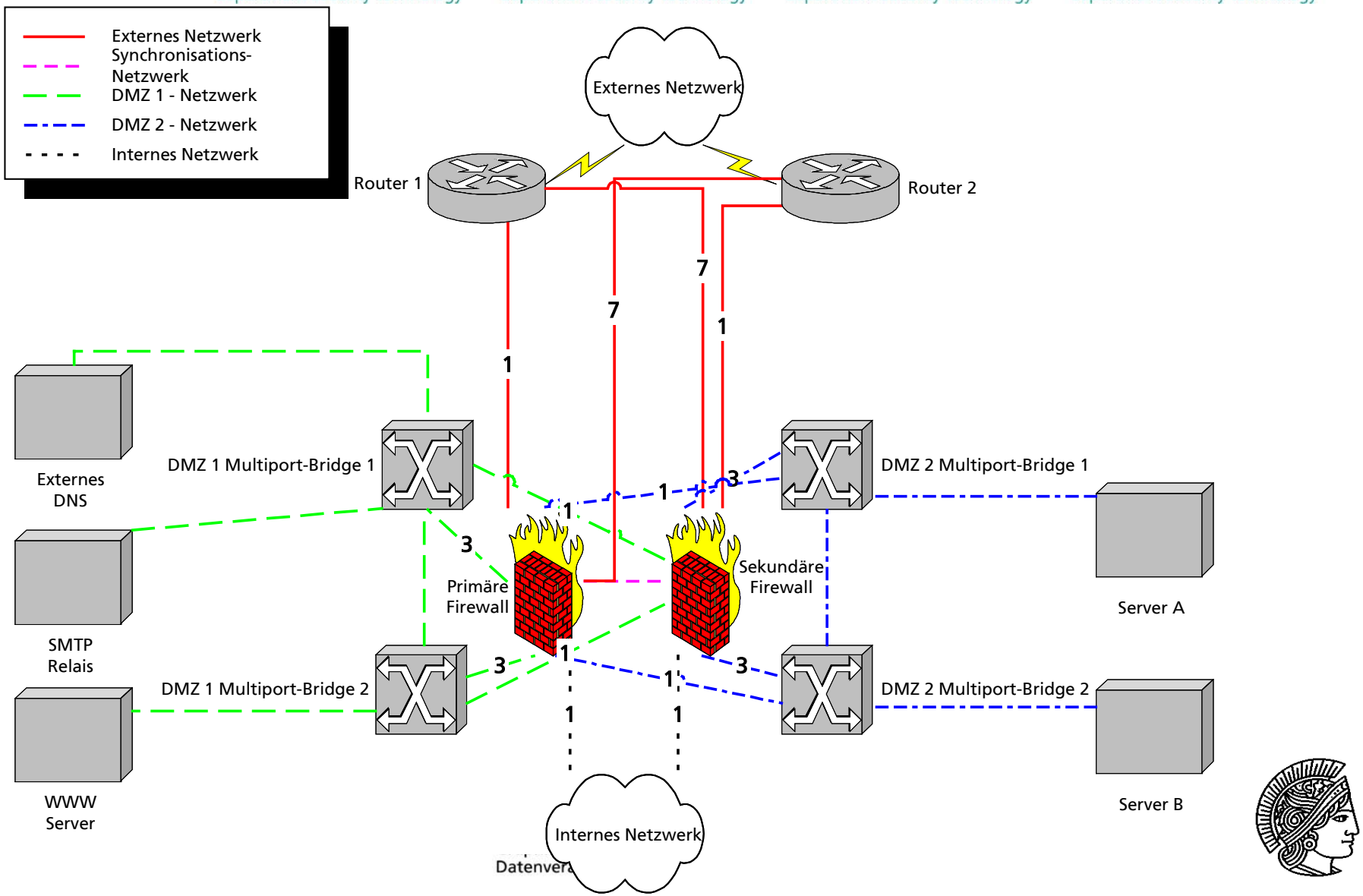




Metriken in OSPF

- Metriken („Kosten“) sind Maß für relativen Aufwand, Datagramme über eine Schnittstelle zu verwenden
  - Meist nur Bandbreite als Grundlage
- Metriken können „mißbraucht“ werden:
  - Einbeziehen von Prozessorlast, kryptographischer Coprozessoren, Speicherauslastung von Firewalls
- Kosten für Flutung sind durch Beschränkung auf Areas begrenzt
  - Router werden zu Regionen zusammengefaßt
  - Nur an Übergängen von Regionen werden Routen übergeben

Lastausgleich mit OSPF



Vorteile von OSPF für Lastausgleich

- Gegenüber Failover-Lösung ist bei gleichem Hardware-Aufwand zusätzlich Lastverteilung möglich
- Es können problemlos mehr als nur 2 Knoten verknüpft werden
- Metriken und Verhalten der Lastbalancierung können präzise gesteuert werden
- Notwendige Komponenten sind meist in Betriebssystemen von Servern und in Routern verfügbar
- Wartung und Konfiguration einzelner Knoten beeinträchtigt nicht die Bereitstellung von Diensten

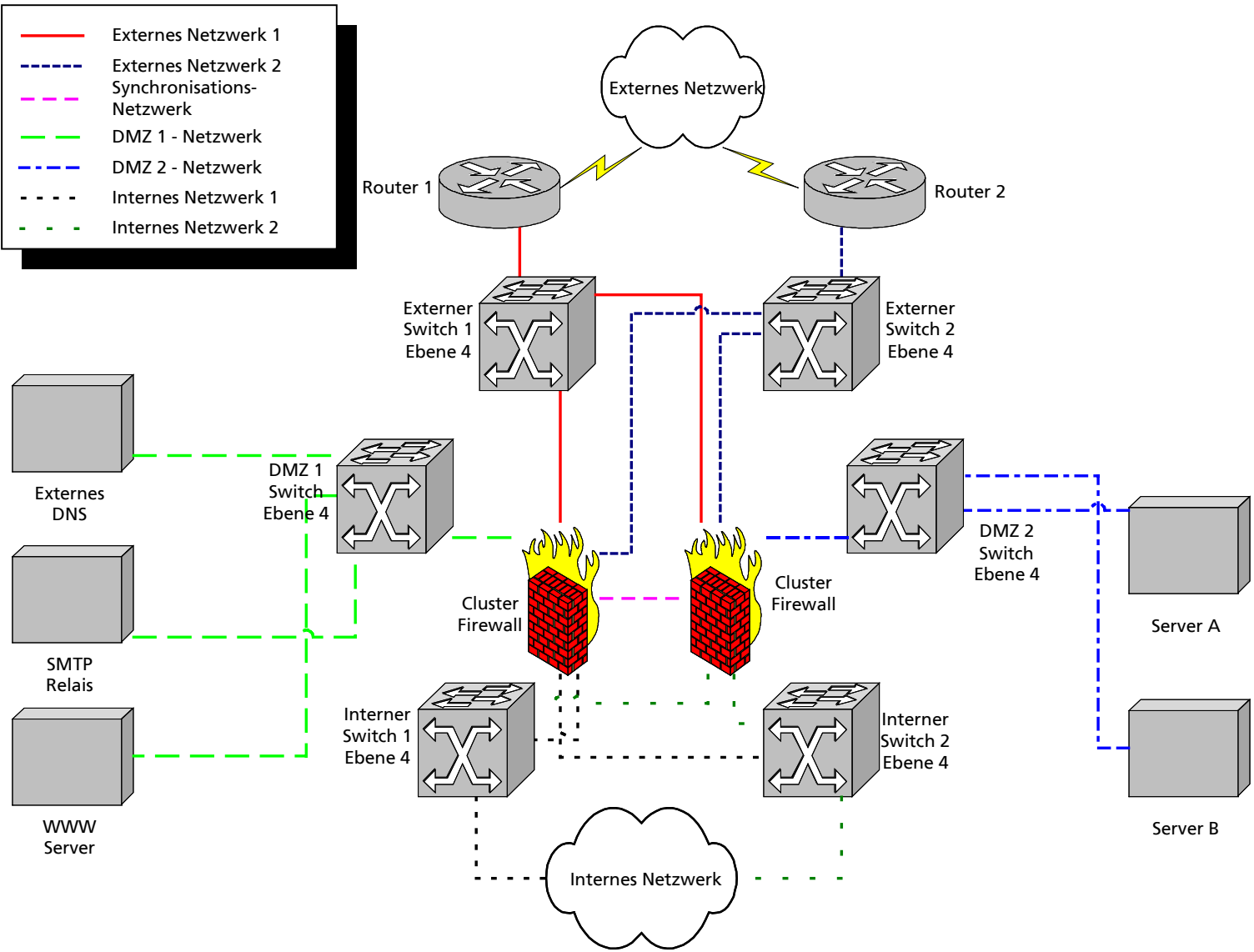
Nachteile von OSPF für Lastausgleich

- Lastausgleich erfolgt nur verzögert, spiegelt nicht exakt die Verteilung wider
- Konfiguration ist nicht ganz trivial
- Übernahme langlebiger Zustandsinformationen für Verbindungen wie IPSec-SAs sind nicht immer möglich
- Viele kommerzielle Firewalls unterstützen OSPF nicht
  - Nachrüstung meist nicht machbar
- Komplexe Protokolle wie OSPF sind immer Gefahrenquelle
- Zusätzlich wird Verfahren für ARP/IP-Failover benötigt

Hardware-basierter Lastausgleich

- Feinkörnige Lastbalancierung ist mittels Layer 4-Switches und einer Gruppe von Firewalls mit internem Lastausgleich möglich
  - Firewall wird gegenüber Endknoten isoliert
  - Eliminiert die Notwendigkeit von virtuellen IP-Adressen
  - Lastbalancierung durch Switches ist nur aufgrund von Verkehrsmustern möglich: Rest müssen Firewalls untereinander ausgleichen

Hardware-basierter Lastausgleich



Vorteile Hardware-basierter Lastausgleich

- Lastbalancierung erfolgt innerhalb des angeschlossenen Netzwerkes und zwischen Knoten des Firewall-Clusters
  - Deutliche Leistungssteigerung gegenüber Failover-Lösung
- Last wird näherungsweise gleich auf alle Knoten des Firewall-Clusters verteilt
- Skalierbarkeit ist sehr gut
  - Firewall-Cluster kann beliebig vergrößert werden, dies bleibt für Endknoten unsichtbar
- Wartung und Konfiguration einzelner Firewall (!)-Knoten beeinträchtigt nicht die Bereitstellung von Diensten

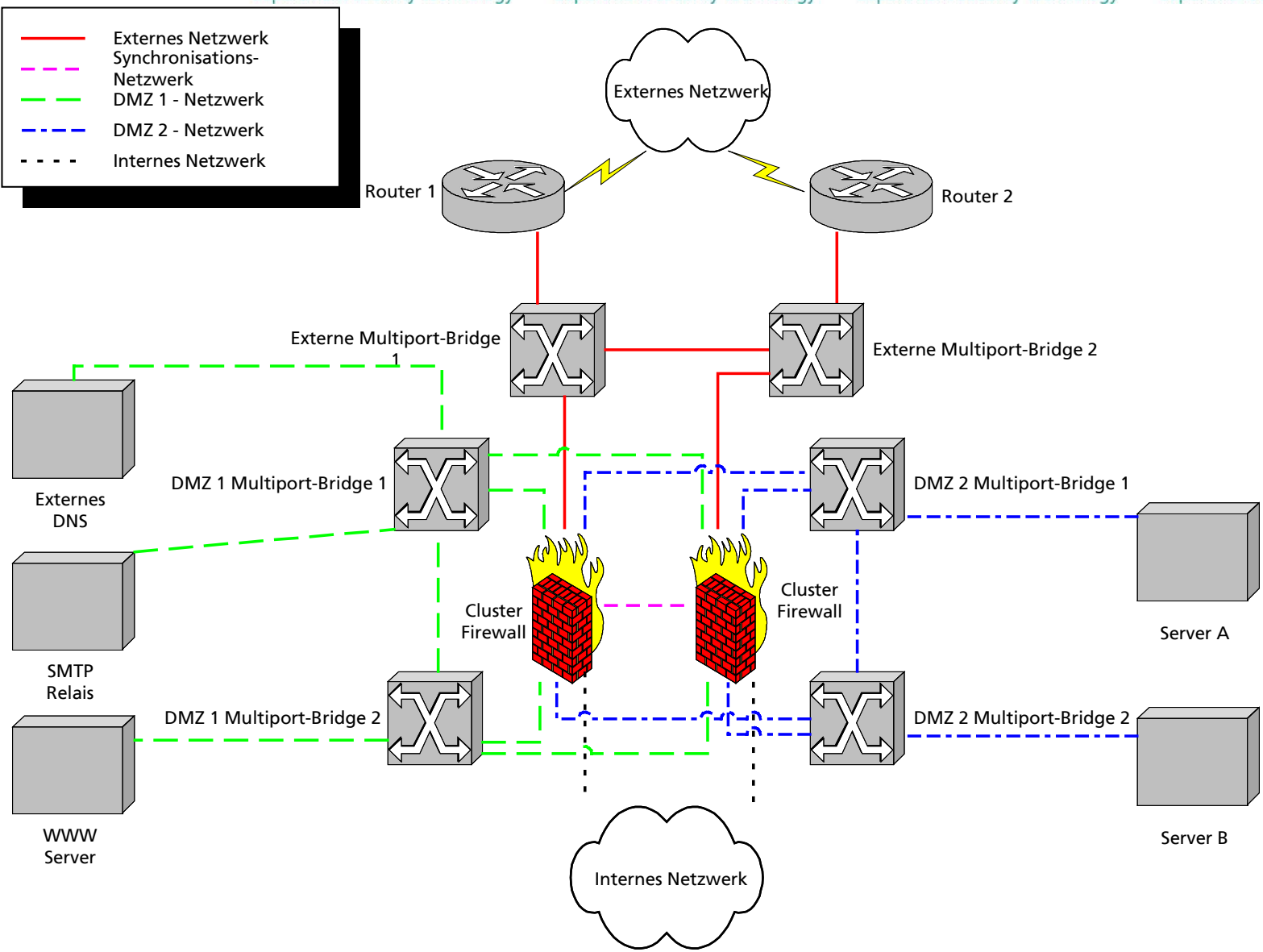
Nachteile Hardware-basierter Lastausgleich

- Kommunikationskanal zwischen Ebene 4-Switches erforderlich zwischen internen und externen, externen und DMZ-Netzen
  - Potentieller Angriffspunkt
- Wenn NAT durchgeführt wird, muß dies auf Ebene der Switches durchgeführt werden
  - Erfassung von Revisionsdaten wird erschwert
- Übernahme langlebiger Verbindungen kaum möglich
- Lastausgleich orientiert sich nur an Netzwerkauslastung
- Kosten sind durch Einsatz von Ebene 4-Switches erheblich

Clustering

- Sowohl nachträglich aufrüstbar (z.B. Rainfinity) als auch bereits in Betriebssystemen von Grund auf vorhanden (z.B. OpenVMS)
- Entscheidungsmechanismen für Lastbalancierung können auf Knoten des Clusters selbst aufsetzen
  - Ermöglicht komplexe Metriken, Migration langlebiger Verbindungen
- Implementierungsvarianten:
  - Virtuelle IP-/MAC-Adressen („Cluster Alias“)
  - Dynamische „floating“ IP-Adressen

Clustering


Externes Netzwerk
Synchronisations-Netzwerk
DMZ 1 - Netzwerk
DMZ 2 - Netzwerk
Internes Netzwerk
Externes Netzwerk
Router 1
Router 2
Externe Multiport-Bridge 1
Externe Multiport-Bridge 2
Externes DNS
DMZ 1 Multiport-Bridge 1
DMZ 2 Multiport-Bridge 1
Cluster Firewall
Cluster Firewall
Server A
SMTP Relais
DMZ 1 Multiport-Bridge 2
DMZ 2 Multiport-Bridge 2
WWW Server
Server B
Internes Netzwerk

Vorteile von Clustering für Lastbalancierung

- Hardware-Konfiguration und Fähigkeiten der einzelnen Knoten müssen nicht identisch sein
- Volle Cluster-Systeme stellen konsistene Sicht der Systemsoftware und Dateisysteme bereit:
  - Ermöglichen z.B. „rolling updates“ von Betriebssystem, Firewall-Software
- Skalierbarkeit und Qualität der Lastbalancierung ist hervorragend
- Metriken sind deutlich aussagekräftiger als bei anderen Lösungen
- Problemloser Failover möglich z.B. für Wartungsarbeiten

Nachteile von Clustering für Lastbalancierung

- Konfiguration kann je nach verwendeten Werkzeugen und Systemen komplex sein
  - Gefahr von neu eingeführten Risiken
- Bei Kombination von nachträglich aufgerüsteter Clustering-Software besteht die Gefahr, daß bei Aktualisierung der Firewall-Software das Clustering Fehler verursacht

Verteilung von Regelwerken

- Konsistente Regelwerke für Datenflüsse, Revisionsdaten, Intrusion Detection notwendig
- Unabhängige Konfiguration ist nicht praktikabel
  - Prinzip des schwächsten Gliedes
- Abstraktionsstufe für Regelwerke ist meist zu niedrig
  - Anpassung an für bestimmte Knoten geltende Netzwerksegmente sind meist notwendig, fehleranfällig
- Skalierbarkeit der Verteilungsmechanismen
  - Import von Regelwerken kann mehrere Minuten dauern während dem Verkehr für Knoten unterbrochen wird

Vertrauenswürdigkeit

- Sicherheitssysteme sind reaktiv, es existiert meist ein Zeitfenster zwischen Erkennung und Abwehrmöglichkeiten für Bedrohungen
- Frage nach Zusicherung des Funktionsumfangs und der Vertrauenswürdigkeit des Firewall-Systems
  - Vollständigkeit der Spezifikation
  - Abdeckung der funktionalen Anforderungen
  - Qualität der Implementierung
  - Analyse auf funktionale Subkomponenten

Problemkreise für Zuverlässigkeit und Vertrauenswürdigkeit

- Risikoanalyse
  - Bedrohungen müssen vollständig erfaßt sein, neue Bedrohungen, Schwachstellen durch Schutzmechanismen
- Spezifikation
  - Hinreichende funktionale Spezifikation für alle sicherheitsrelevanten Systeme und Subsysteme
- Implementierung
  - Korrektheit, Vollständigkeit, Konfiguration nach Spezifikation
- Verifikation und Validierung
  - Korrespondenz zwischen identifizierten Risiken, Gegenmaßnahmen

Zuverlässige Software ist machbar

- Kritische Systeme (Avionik, Raumfahrt, Reaktortechnik) wenden seit langem standardisierte Entwicklungsverfahren an, die ein hohes Maß an Zuverlässigkeit ermöglichen
  - IEEE 730, 829, 830, 1002, 1008, 1012...
  - Entsprechendes von IAEA, FAA, diverse MIL-STDs
- Semiformale Entwicklungstechniken erlauben Spezifikation mit mathematischen Mitteln, Korrespondenz zwischen Implementierung und Spezifikation muß jedoch von Hand demonstriert werden; Verifikation und Programmbeweise
  - Z, Object-Z, VDM, PVS, HDM, Gypsy/GVE,...

Vertrauenswürdigkeit: TCSEC

- Trusted Computer System Evaluation Criteria: Erster Standard 1985 für DoD-Computersysteme
  - vermengt Anforderungen an Funktionalität und Vertrauenswürdigkeit
  - Unterteilt Vertrauenswürdigkeit in vier Abteilungen
    - D: Evaluierung auf höherer Stufe fehlgeschlagen
    - C: Discretionary Security Protection / Discretionary Access Control
    - B: Labeled Security Protection, Structured Protection
    - A: Verified Design

TCSEC und weitere Kriterien

- TCSEC zielte auf isolierte Systeme ab, die „Network Interpretation“ brachte hier nur partiell Besserung
- Deutsche Bestrebungen: ITSK (1989)
  - Unterteilung der Sicherheitsfunktionalität in abstrakte Gruppen von Funktionen
  - Auftrennung der Kriterien in Funktionskriterien und Qualitätskriterien
  - Vordefinierte Funktionsklassen sind aus TCSEC abgeleitet
    - 10 Funktionsklassen F1...F10
    - 8 Qualitätsstufen Q0...Q8

Information Technology Security Evaluation Criteria (ITSEC)

- Nationale Kriterien sind in Europa unwirtschaftlich, da der angesprochene Markt zu klein ist
- Harmonisierungsbestrebungen: Die ITSEC wurden von Deutschland, Frankreich, dem UK und der Niederlande entwickelt. Letzte gültige Fassung: Version 1.2 (1991)
  - Aufteilung in Funktionalität, Vertrauenswürdigkeit (E0-E6) analog ITSK
  - Abwärtskompatibilität zu TCSEC in Funktionsklassen (z.B. F-C2)
  - Neu: Erweiterbare Funktionsklassen
  - Wechselseitige Anerkennung seit 1998, weitere Staaten

- ISO-Arbeitsgruppe seit 1990, parallel Harmonisierungs-bestrebungen zwischen USA (FC) und Kanada (CTCPEC) 1993
  - Entscheidung zur weltweiten Harmonisierung
  - 1996 wurde Version 1.0 der CC veröffentlicht
  - CC 2.1 wurden im August 1999 als ISO 15408 zum Standard
  - Besteht aus drei Teilen
    - Einführung, Vorstellung des Modells, Evaluierungskonzepte
    - Katalog funktionaler Anforderungen
    - Katalog der Anforderungen an Vertrauenswürdigkeit

Vertrauenswürdigkeit in CC (1)

- 7 Stufen: Evaluation Assurance Levels
- EAL1: Funktionell getestet
  - Prüfung und Bewertung von Endprodukten, unabhängige Tests anhand Spezifikation und Prüfung der Dokumentation. Soll ohne Hilfe des Herstellers ausführbar sein
- EAL2: Strukturell getestet
  - Erfordert Kooperation der Entwickler; Lieferung von Entwurfsinformationen, Testergebnissen. Soll bei Produkten die mit sauberer Ingenieurstechnik entwickelt werden kaum Mehraufwand bewirken

Vertrauenswürdigkeit in CC (2)

- EAL3: Methodisch getestet und überprüft
  - Erfordert gewissenhafte Entwickler, positive Sicherheitsmaßnahmen, jedoch keine signifikante Änderung an bestehenden Entwicklungstechniken erforderlich
- EAL4: Methodisch entwickelt, getestet und durchgesehen
  - Scharfe Entwicklungsregeln, jedoch keine tiefgreifende Spezialkenntnisse seitens Entwickler erforderlich. Die höchste Stufe auf der Nachrüstung praktikabel ist
- EAL5: Semiformal entworfen und getestet
  - Begrenzter Einsatz von Spezialtechniken, muß eigens für EAL5 entwickelt werden

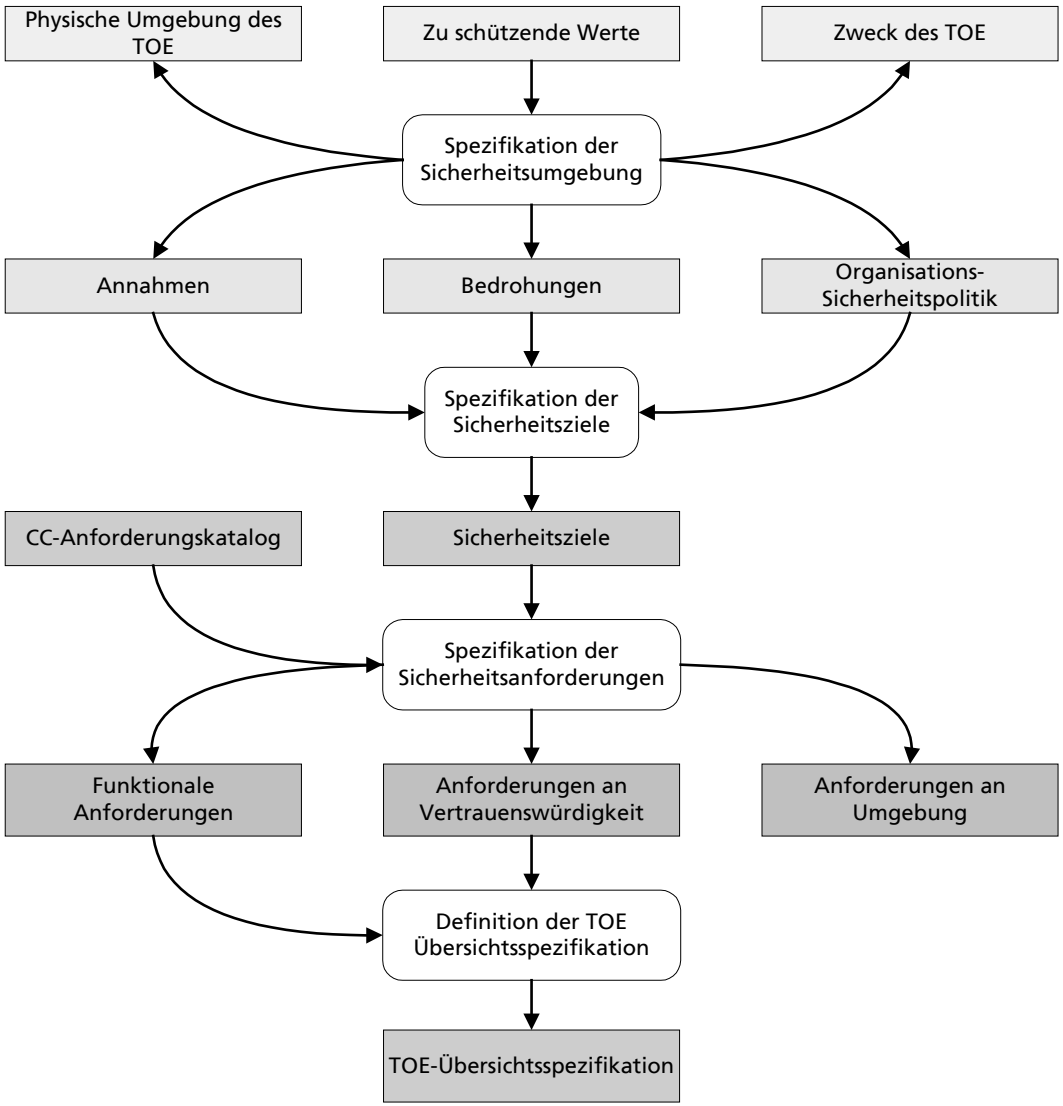
Vertrauenswürdigkeit in CC (3)

- EAL6: Semiformal verifizierter Entwurf, getestet
  - Erfordert zusätzlich streng kontrollierte Entwicklungsumgebung, für Einsatz in Situationen mit hohem Risiko, bei dem signifikante Zusatzkosten gerecht-fertigt sind
- EAL7: Formal verifizierter Entwurf, getestet
  - Einsatzgebiete mit extrem hohem Risiko. Derzeit aufgrund der geringen Skalierbarkeit formaler Techniken nur auf Systeme mit extrem geringer Funktionalität anwendbar

Protection Profiles und Security Targets

- Protection Profile
  - Menge von Sicherheitsanforderungen, entweder direkt aus CC abgeleitet oder anwendungsspezifisch (explizit)
  - Soll EAL enthalten
  - Wiederverwendbar für mehrere Implementierungen
- Security Target
  - Menge von Sicherheitsanforderungen entweder direkt oder in Bezug auf PP
  - Anforderungen an konkretem Target of Evaluation (TOE)

Herleitung von Anforderungen und Spezifikation



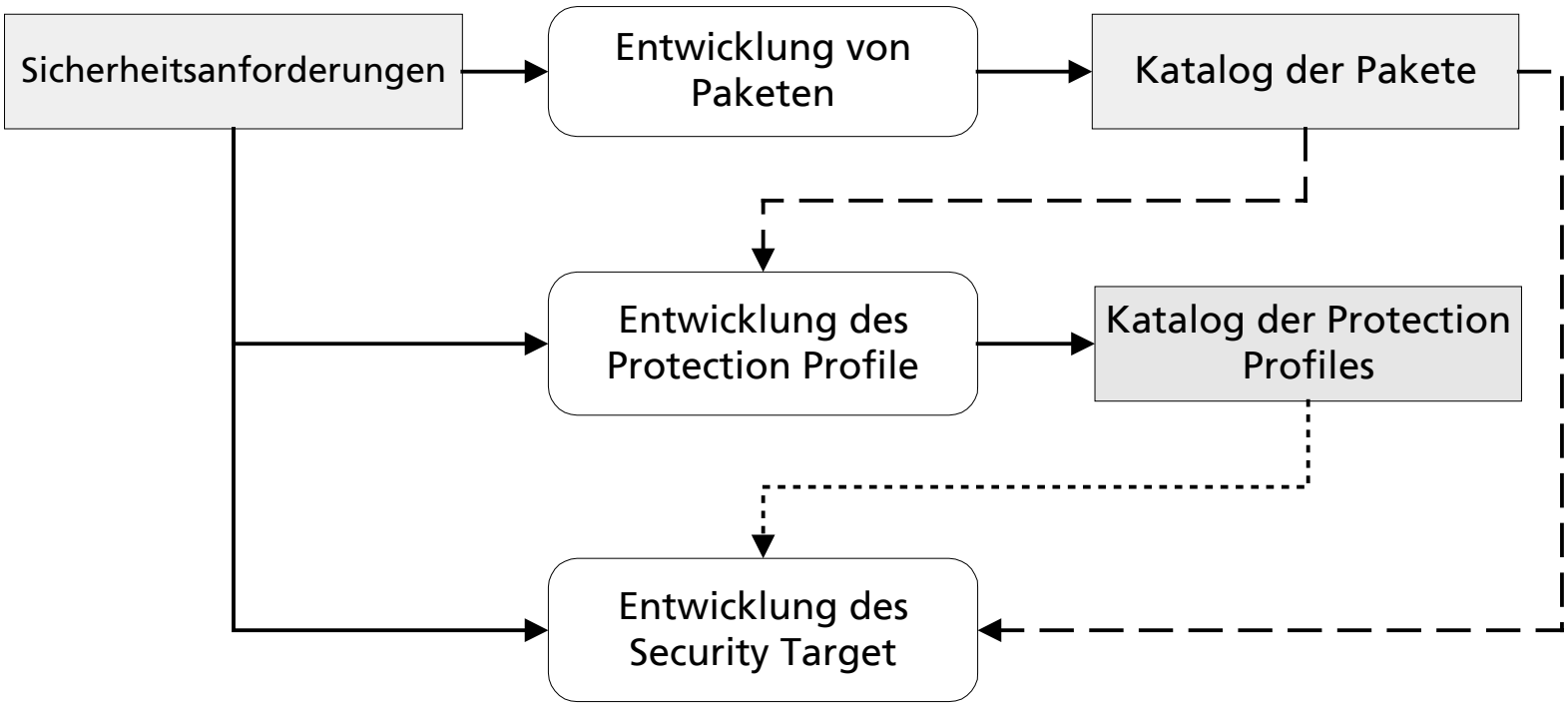
Material zur Sicherheits-umgebung (Protection Profile, Security Target)

Material zu Sicherheitszielen (Protection Profile, Security Target)

Material zu Sicherheits-anforderungen (Protection Profile, Security Target)

Material zur Sicherheits-spezifikation (Security Target)

Ableitung von PP und ST aus Sicherheitsanforderungen



Inhalt des PP

- **Sicherheitsanforderungen**
  - **PP-Einführung** — PP-Identifikation, PP-Übersicht
  - **TOE-Beschreibung**
  - **TOE-Sicherheitsumgebung** — Annahmen, Bedrohungen, Organisatorische Sicherheitspolitiken
  - **Sicherheitsziele** — Sicherheitsziele für TOE, Sicherheitsziele für Umgebung
  - **IT-Sicherheitsanforderungen**
    - **TOE-Sicherheitsanforderungen** — Funktionale Sicherheitsanforderungen an das TOE, Anforderungen an die Vertrauenswürdigkeit des TOE
    - Sicherheitsanforderungen an die IT-Umgebung
  - PP-Anwendungsbemerkungen
  - **Erklärung** — Sicherheitsanforderungen an die IT-Umgebung

Inhalt des ST

- **Sicherheitsvorgaben**
  - **ST-Einführung**
    - ST-Identifikation,
      ST-Übersicht
      Postulat der Übereinstimmung mit CC
  - **TOE-Beschreibung**
  - **TOE-Sicherheitsumgebung**
    - Annahmen,
      Bedrohungen,
      Organisatorische Sicherheitspolitik
  - **Sicherheitsziele**
    - Sicherheitsziele für TOE,
      Sicherheitsziele für Umgebung
  - **IT-Sicherheitsanforderungen**
    - **TOE-Sicherheitsumgebung**
      - Funktionale Sicherheitsanforderungen an das TOE,
        Anforderungen an die Vertrauenswürdigkeit des TOE
    - Sicherheitsanforderungen an die IT-Umgebung
  - **TOE-Übersichtsspezifikation**
    - TOE-Sicherheitsfunktionen
      Maßnahmen zur Vertrauenswürdigkeit
  - **PP-Postulate**
    - PP-Verweis
      PP-Anpassung
      PP-Ergänzungen
  - **Erklärung**
    - Erklärung Sicherheitsziele
      Erklärung Sicherheitsanforderungen
      Erklärung der TOE-Übersichtsspezifikation
      Erklärung der PP-Postulate