CloudCommand

Datum: 01.04.2024

Speaker:
Max Mustermann
Maxime Musterfrau

Cyber Security


CloudCommand
Datum: XX.XX.2024
Speaker:
DOZENTEN NAME
OSPF / NAT

AGENDA

01 Routing

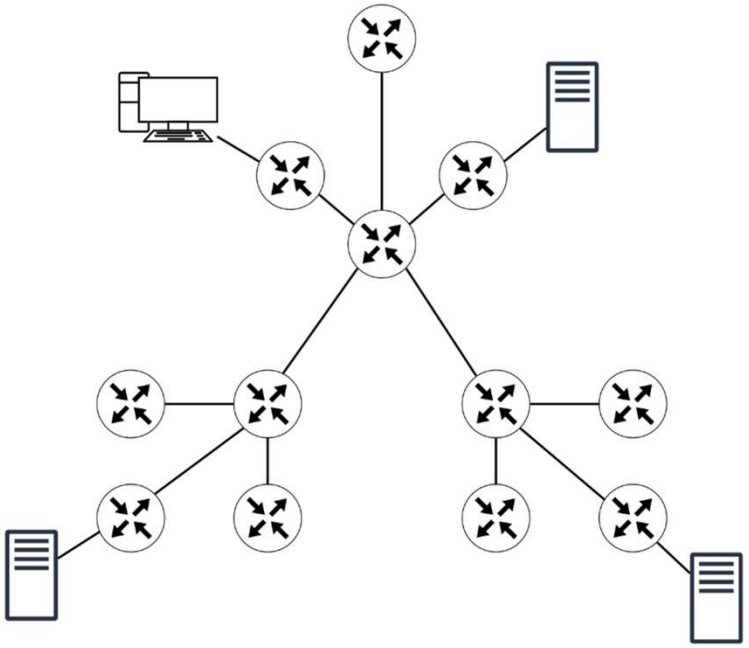
02 Remote Zugriff

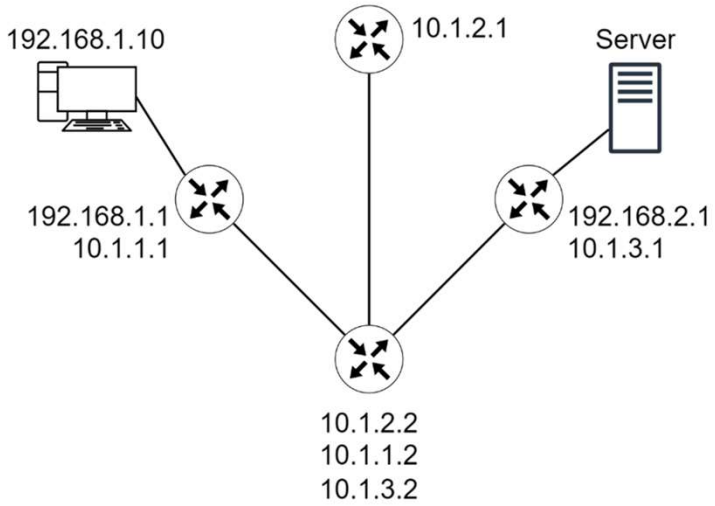
01 Routing

Router

- Router leiten Datenverkehr an Computer, andere Router und schließlich an den Zielcomputer weiter.
- Im einfachsten Fall senden Clientcomputer die gesamte Kommunikation über einen einzelnen Router, der als Standardgateway bezeichnet wird.
- Sind mehrere Router in einem Subnetz vorhanden, muss ein komplexeres Routing konfiguriert werden.

Router




192.168.1.10
10.1.2.1
Server
192.168.1.1
10.1.1.1
192.168.2.1
10.1.3.1
10.1.2.2
10.1.1.2
10.1.3.2

Statisches und Dynamisches Routen

- Eine statische Route wird manuell vom Administrator konfiguriert.
- Eine dynamische Route wird mit Hilfe spezieller Routingprotokolle ermittelt.
- Dynamisches Routing wird durch dynamische Konfiguration mit Hilfe von Routing-Tabellen umgesetzt.
    - Routing Information Protocol (RIP)
    - Open Shortest Path First (OSPF)
    - Interior Gateway Routing Protocol (IGRP)
    - Border Gateway Protocol (BGP)

Distance Vector und Link-State

Distance Vector	Link-State
Betrachtet die Netztopologie aus Sicht der Nachbarn	Erhält eine umfassende Information der gesamten Netztopologie
Addiert distanz Vektoren von Router zu Router	Berechnet den kürzesten direkten Pfad zu anderen Routern
Regelmäßige, periodische Updates; Mit langsamer Konvergenz	Ereigniss gesteuerte Updates; Schnelle Konvergenz
Leitet Kopien der Routing-Tabellen an benachbarte Router weiter	Leitet Link-State Routing Updates an andere Router weiter

RIP - Routing Information Protocol

- Ein dynamisches Protokoll, das Distanz-Vektor-Routing-Algorithmen verwendet, um zu bestimmen, welche Route die Datenpakete nehmen sollen.
- Das Protokoll berechnet den Pfad oder die Schnittstelle über die das Paket weitergeleitet werden soll, sowie die Anzahl der Hops zum Ziel.

OSPF - Open Shortest Path First

- Arbeitet mit SPF-Algorithmus (Shortest Path First) und resultierendem SPF-Baum.
- Regelmäßige Updates (Link-State-Aktualisierungen) durch Flooding.
- Feststellen der Erreichbarkeit von Nachbarn mittels Hello-Protokoll.
- Schnelle Reaktion auf Netzänderung: Der SPF-Algorithmus berechnet mit den LSA-Informationen die optimalen Pfade neu und aktualisiert die Routingtabelle (lokal).
- Die Routingtabelle enthält Pfad samt Kosten und Interfaces zu jedem bekannten Netz, um den optimalen Pfad für die Pakete zu bestimmen.

AS - Autonome Systeme

- Ein autonomes System (kurz AS) ist, laut klassischer Definition, eine Gruppe von Routern, die mehrere Netzwerke verbinden und:
  - Ein gemeinsames inneres Gateway-Protokoll (IGP) sowie gemeinsamen Metriken nutzen, um den Datenverkehr innerhalb des Systems zu steuern.
  - Unter einer einzigen technischen Verwaltung betrieben werden.
- Allerdings ist es nicht mehr unüblich, in einem AS mehrere IGP und mehrere Sätze von Metriken zu verwalten.
  - Ein autonomes System ist dann ein System, das sich anderen autonomen Systemen so präsentiert, als hätte es nur einen einzigen inneren Routing-Plan, um ein beständiges Bild davon abzugeben, welche Ziele (z. B. andere Netzwerke) durch dieses System erreicht werden können.
- Autonome Systeme sind untereinander verbunden und bilden so das Internet.

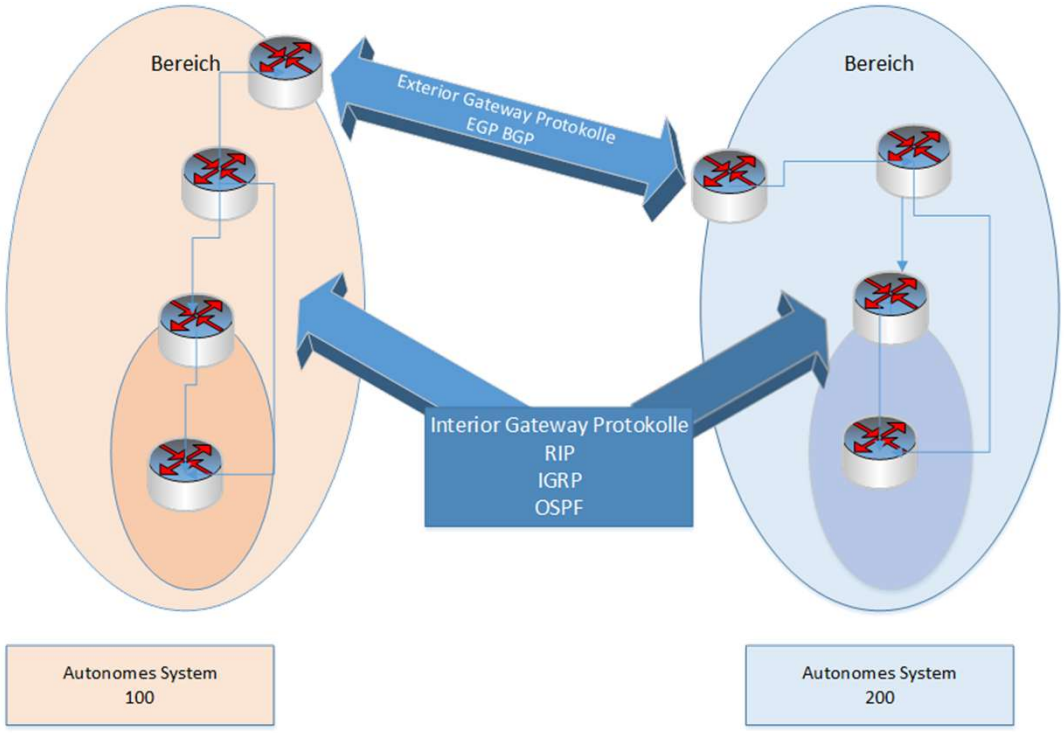
IGRP – Interior Gateway Routing Protocol

- In den 1980er Jahren von Cisco entwickelt
- proprietäres Distance-Vector-Routing Protocol
- innerhalb eines autonomen Systems
- weiterentwickelt zu EIRGP

BGP – Border Gateway Protocol

- Im Internet eingesetzte Routingprotokoll.
- Verbindet autonome Systeme (AS) miteinander.
- Auch als Exterior Gateway Protokoll bezeichnet.

Routing Protokolle



Routing Beispiel

NAT - Network Address Translation

- Beim NAT (Network Address Translation) werden die Adressen eines privaten Netzes über ein Koppelelement (Router) in öffentlich registrierte IP-Adressen „umgewandelt“.
- IP Masquerading, PAT (Port and Address Translation), bildet alle Adressen eines privaten Netzwerkes auf eine einzelne öffentliche IP-Adresse ab.

Was sollte ich auf jeden Fall behalten

- **Routing** - bezeichnet die Wegfindung von Daten einer Quelle zu einem definierten Ziel. Ein IP-Router übernimmt dabei die Aufgabe des Routings
- **AS** - ein System, das sich anderen autonomen Systemen so präsentiert, als hätte es nur einen einzigen inneren Routing-Plan, um ein beständiges Bild davon abzugeben, welche Ziele (z. B. andere Netzwerke) durch dieses System erreicht werden können.
- **Internes Routing** - mit Protokolle wie RIP, OSPF oder IGRP
- **BGP** - das verbreitetste Protokoll zum Routing zwischen AS
- **NAT (Network Address Translation)** - zur “Umwandlung” von Adressen eines privaten Netzes über ein Koppelelement (Router) in öffentlich registrierte IP-Adressen
- **PAT (Port and Address Translation)** - bildet alle Adressen eines privaten Netzwerkes auf eine einzelne öffentliche IP-Adresse ab.

02
Remote Zugriff

Internet - Extranet - Intranet

Die (Kurz-)Geschichte des Internets

- 1969 - das ARPANET, einem Projekt der Advanced Research Project Agency (ARPA) des US-DoD
- Erweiterung des ARPANET zur Vernetzung von Universitäten und Forschungseinrichtungen
- 1983 - Mit der Umstellung auf das Internet Protocol TCP/IP begann sich auch der Name ‘Internet’ durchzusetzen.
- 1990 - das Internet wird für kommerzielle Zwecke Nutzung freigegeben

Internet - Extranet - Intranet

Die (Kurz-)Geschichte des Internets

- 1991 - Tim Berners-Lee entwickelte die Grundlagen des World Wide Web, die Seitenbeschreibungssprache HTML
- 1993 - der erste grafikfähige Webbrowser namens Mosaic wird veröffentlicht
- 1995 – Windows 95 unterstützt TCP/IP und vereinfacht damit den Zugang zum Internet

Internet - Extranet - Intranet

- Das Internet besteht aus einer Vielzahl an Provider- (ISP), Firmen- und Forschungsnetzwerken, die mittels verschiedener physikalischen Verbindungen (Glasfaser, Kupfer, Sateliten, Richtfunk) die eigentliche Struktur darstellen. Diese Verbindungen werden i. d. R. an einem Internet Exchange Point (IXP) gebündelt.
- In Frankfurt befindet sich der deutsche und europäische (und zugleich der größte) IXP: DE-CIX

Internet - Extranet - Intranet

Intranet

- ein nicht öffentliches firmeninternes Rechnernetz
- Ein firmeninternes LAN wird dann zum Intranet, wenn es auf den gleichen Techniken (TCP/IP, HTTP, Email…) und Anwendungen wie das Internet basiert und den eigenen Mitarbeitern als Informations-, Kommunikations- und Anwendungsplattform zur Verfügung steht.
- Oft wird eine interne Webseite als Intranet bezeichnet, obwohl das gesamte Firmennetzwerk ein Intranet ist.

Internet – Extranet – Intranet

Extranet

- Ein Extranet ist ein besonderer Teil eines Intranets, zu dem, außer den eigenen Mitarbeitern, ein weiterer privilegierter Benutzerkreis einen gesicherten Zugang von außerhalb hat.
- Dies könnten z. B. Partnerfirmen, Zulieferer, oder einfach nur ein ausgewählter engerer Kundenkreis sein.
- nicht für die Öffentlichkeit zugänglich

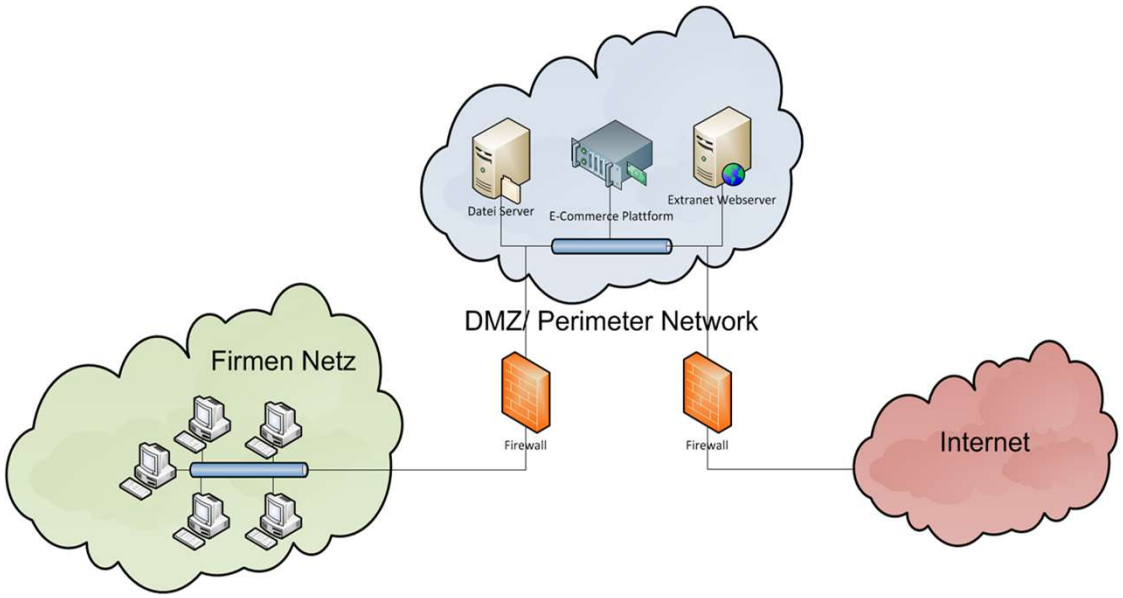
Internet - Extranet - Intranet

DMZ / Umkreisnetzwerk / Perimeter-Netzwerk

- DMZs (Demilitarized Zone/Demilitarisierte Zone) = Perimeter Networks = Umkreisnetzwerk
- zwischen dem Internet und dem internen Netz
- Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt.
- Ein Extranet ist eine Ressource in einer DMZ.

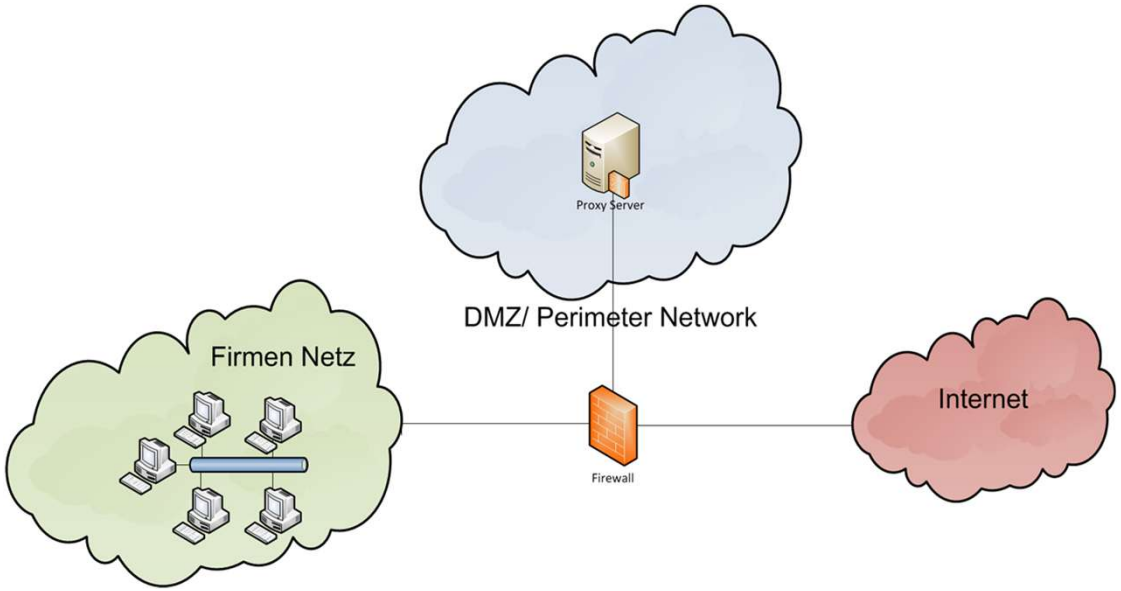
Internet - Extranet - Intranet

DMZ / Umkreisnetzwerk / Perimeter-Netzwerk



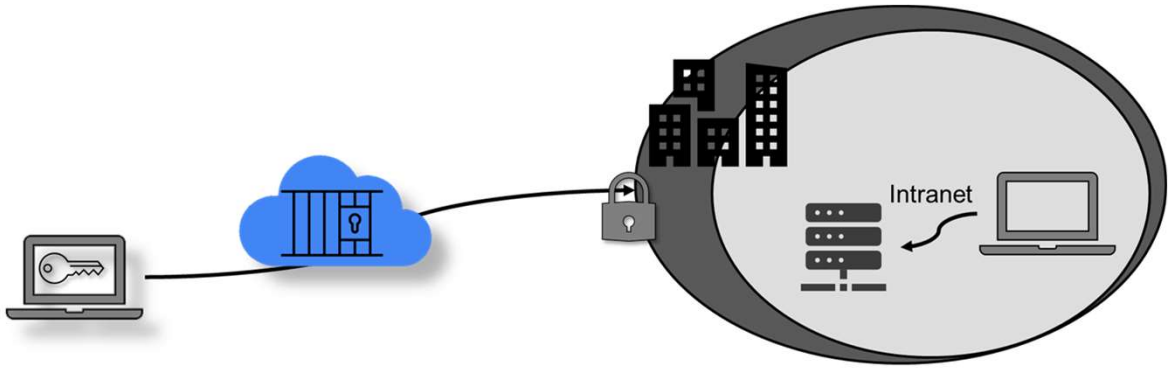
Internet - Extranet - Intranet

DMZ / Umkreisnetzwerk / Perimeter-Netzwerk



Remotezugriff Definition

- Remotezugriff beschreibt den Zugriff auf Ressourcen, die nicht lokal bzw. innerhalb des eigenes Netzwerkes/Intranet erreichbar sind
- Wir unterscheiden primär den Zugriff auf Ressourcen oder Desktops und den Zugriff auf entfernte Netzwerke, wobei ersteres auch über letzteres erfolgen kann



Virtual Private Network (VPN)

VPN (Virtual Private Networks)

- Früher (leider auch heute noch teilweise) als sog. Einwahl-Lösung (DFÜ-Verbindung)
  - Bekannt auch als Modem-Internetzugang
  - Baut auf der Telefoninfrastruktur auf und benötigen kein Internet

Virtual Private Network (VPN)

VPN (Virtual Private Networks)

- Heute als VPN Lösung
  - Tunnel-Verbindung zwischen dem Client und dem Unternehmensnetzwerk (Client-to-Server) oder zwischen Standorten von Unternehmen (Site-to-Site)
  - Verschlüsselung einer geschützten Leitung über ein ungeschütztes Netz (Internet)
  - Zunehmend auch als Browser-gestützte Lösung implementiert, ohne eigenem Client (SSL-VPN)

VPN Protokolle

- **PPTP** (Point-to-Point Tunneling Protocol)
- **SSTP** (Secure Socket Tunneling Protocol)
- **L2TP / IPSec** (Layer-2-Tunneling-Protocol / IP-Security)
- **IKEv2 / IPSec** (Internet-Key-Exchange / IP-Security)
- **OpenVPN**
- **Wireguard**
- **MPLS** (Multi-Protocol-Label-Switching)

Was sollte ich auf jeden Fall behalten?

- **Intranet** – ein nicht-öffentliches firmeninternes Netzwerk
- **DMZ** – Eine DMZ wird üblicherweise als Subnetz definiert, das zwischen dem öffentlichen Internet und privaten Netzwerken angesiedelt ist
- **VPN** – ein in sich abgeschlossenes Netzwerk, das der verschlüsselten Kommunikation über das Internet dient
- SSTP, IPSec, OpenVPN, Wireguard

DANKE!

Gibt es noch Fragen?

Kontakt:

Max Mustermann
01234 – 56 78 910
m.mustermann@email.de
Cloud Command GmbH
www.cloud-command.de

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm