CloudCommand

Datum: 01.04.2024

Speaker:
Max Mustermann
Maxime Musterfrau

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

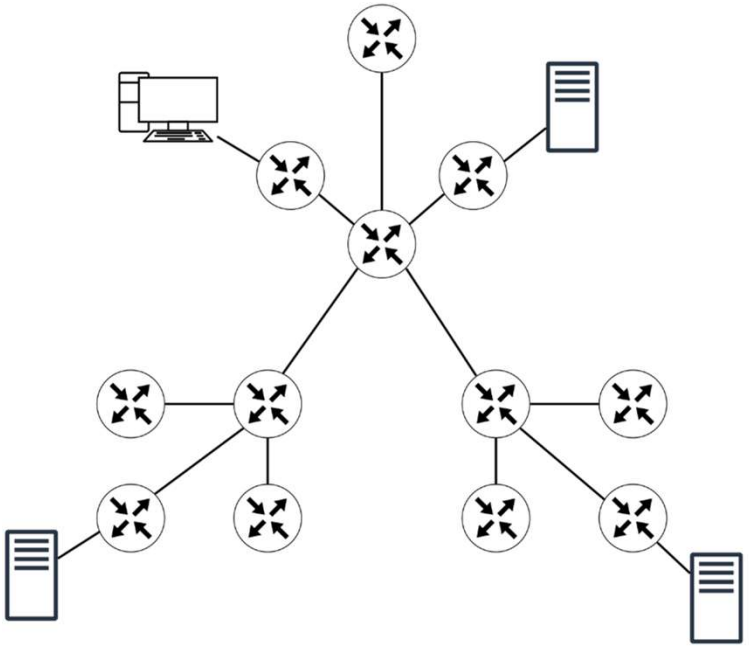
01 Routing
02 Netzwerksimulation
03 Netzwerkdokumentation

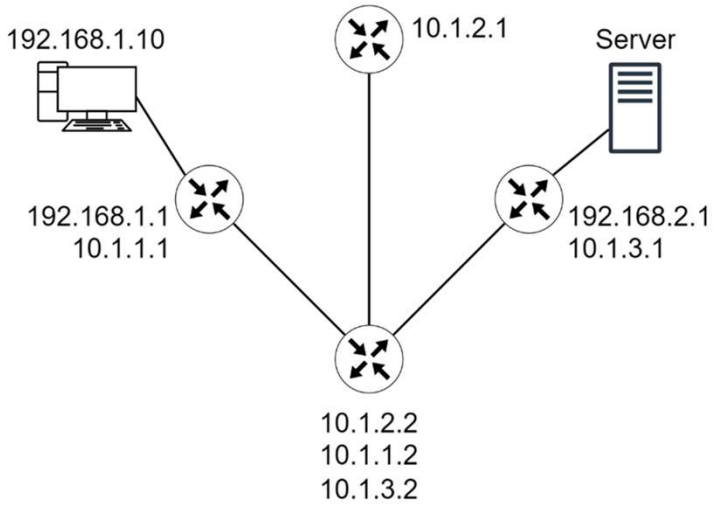
01 Routing

Router

- Router leiten Verkehr 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.
- Wenn mehrere Router in einem Subnetz vorhanden sind muss 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 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 Menge von Routern (die mehrere Netzwerke verbinden) mit einem gemeinsamen inneren Gateway-Protokoll (IGP) und gemeinsamen Metriken, die bestimmen, wie Pakete innerhalb eines AS vermittelt werden, unter einer einzigen technischen Verwaltung.
- 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.

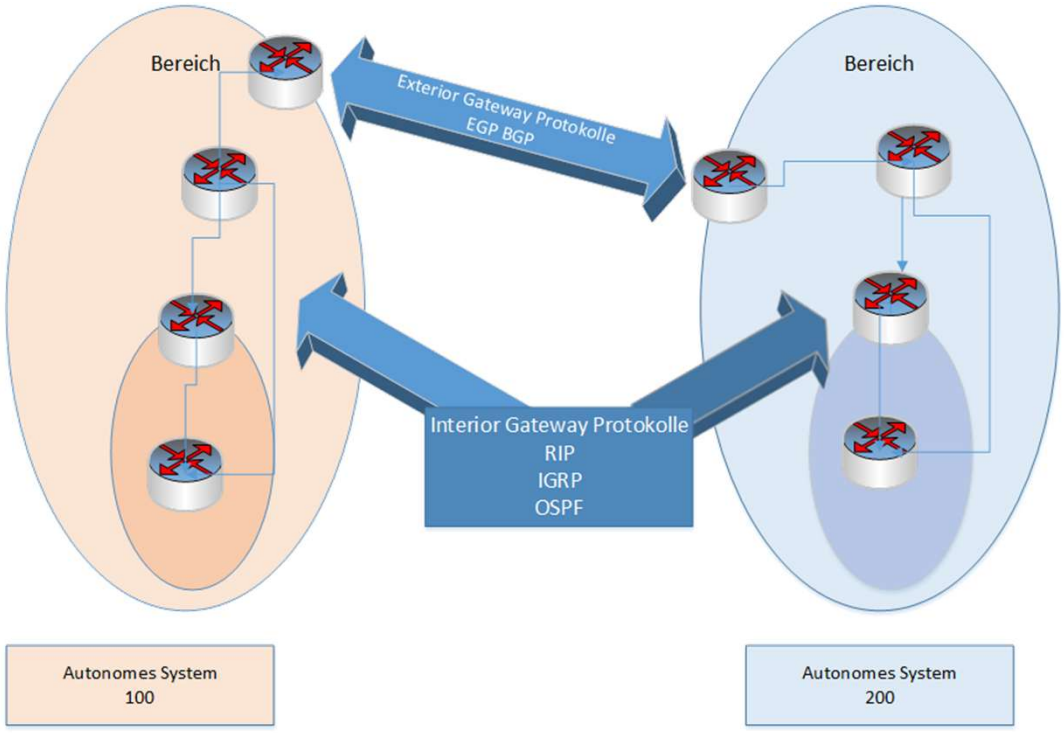
IGRP – Interior Gateway Routing Protocol

- 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

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 Netzwerk-simulation

Netzwerksimulation

- Hyper-V
  - Erstellen von internen und externen Switches
  - Testen des Netzwerkes

- Cisco Packet Tracer

03 Netzwerk-dokumentation

Netzwerkmanagement

Netzwerkmanagement bedeutet die proaktive Überwachung und Analyse der Aktivitäten, Steuerung der Prozesse und Leistungen in einem definierten Netzwerk.
Network Observability zur Optimierung der Leistung und Aufrechterhaltung der Verfügbarkeit:

- Umfassendes Monitoring für Netzwerk, Infrastruktur und Anwendungen
- Geräteüberwachung für physische und virtuelle Hosts
- Dashboards über den Zustand in Echtzeit
- Erstellung von Warnungen bei zuvor definierten Ereignissen
- Konfigurationsverwaltung für Netzwerke, Virtualisierung, Server und Anwendungen

Netzwerkmanagement

Network Performance Monitor

Herstellerunabhängige und mit den Anforderungen deines Netzwerks skalierbare Netzwerküberwachung:

- Herstellerunabhängige Netzwerküberwachung
- Network Insights für mehr Transparenz
- Intelligentere Skalierbarkeit für große Umgebungen
- Skalierbare Warnungen
- Netzwerküberwachung, die auf die Reduzierung von Netzwerkausfällen und die Leistungsverbesserung ausgelegt ist

Netzwerkmanagement

NetFlow Traffic Analyzer

- Überwachungssoftware für Netzwerkbandbreite
- Überwachung der Bandbreite
- Warnungen zum Anwendungsdatenverkehr
- Netzwerkverkehrsanalyse
- Dashboard für die Leistungsanalyse

Netzwerkmanagement

Network Configuration Manager

- Eine automatisierte Verwaltung und Sicherung der Netzwerkkonfiguration.

IP Address Manager

- IP-Adressverwaltungssoftware
- Automatisierte Nachverfolgung von IP-Adressen
- Integrierte DHCP-, DNS- und IP-Adressverwaltung
- IP-Adresswarnungen, Fehlerbehebung und Berichterstellung
- Herstellerunabhängige DHCP- und DNS-Unterstützung lokal und in der Cloud

Netzwerkmanagement

User Device Tracker

- Software zur Netzwerkgerätenachverfolgung, mit der Sie Benutzer und Geräte in Ihrem Netzwerk finden können

Network Automation Manager

- Integrierte Netzwerkautomatisierungssoftware für große oder komplexe Umgebungen

Netzwerkmanagement

Log Analyzer

- Unkomplizierte Analyse von Maschinendaten zum schnellen Identifizieren von IT-Problemen

Network Topology Manager

- Netzwerk-Management-Software zur automatischen Erstellung eines Netzwerkdiagramms

Netzwerkdokumentation

Netzwerkplan Struktur auf IP-Basis (z.B. MS-Visio, o.a. Tools)

Die umfangreichen Software Tools zum Management des IT-Netzwerks stellen an sich schon eine gute Dokumentation dar. Darüber hinaus empfiehlt es sich, eine angemessene Dokumentation des IT-Netzwerks in schriftlicher Form für folgende Komponenten zu erstellen:

- physische Infrastruktur
- Netzwerk
- Server
- Clients
- Software und Lizenzen
- Anwendungen und IT-Services
- Dokumentation des Notfall-Managements, BCM

Dokumentation

Physische Infrastruktur:

- Standorte (Arbeitsplatz, Raum, Etage, Gebäude, Gelände, Ort, ….),
- Raumpläne

Dokumentation

Netzwerk:

- IP-Adressen und deren Vergabe / Steuerung (DHCP, manuell, reserviert), VLAN-Verteilung
- Switch Konfigurationen (inkl. VLANs und Trunks)
- DNS Konfiguration und zugehörige Systeme
- Firewalls, Router und weitere Netzwerkgeräte (auch ggfs. Drucker & Co.)
- WAN-Verbindungen (FC, DSL, LTE, …)
- Verträge mit Provider inkl. SLAs und Kontaktdaten für Entstörung
- Design des Netzwerkes (Topologie, Teilsegmente (physisch und logisch), LAN/WAN-Technologie)

Dokumentation

Server:

- IP, Name, DNS, Services, Bandbreite

Clients:

- Konfiguration, IP, Benennung (kann Beispielhaft sein)

Software und Lizenzen:

- wo ist welche Lizenz eingesetzt?

Anwendungen und IT-Services:

- AD, Freigaben, Gruppen, DNS, DHCP

Was sollte ich auf jeden Fall behalten

- Netzwerkmanagement bedeutet die proaktive Überwachung und Analyse der Aktivitäten, Steuerung der Prozesse und Leistungen in einem definierten Netzwerk.
- Es gibt verschiedene Tools, welche bei der automatischen Dokumentation unterstützen können.

Was sollte ich auf jeden Fall behalten

- Dennoch sollte man eine schriftliche Dokumentation verfassen, welche zumindest die folgenden Bestandteile enthält:
  - physische Infrastruktur
  - Netzwerk
  - Server
  - Clients
  - Software und Lizenzen
  - Anwendungen und IT-Services
  - Dokumentation des Notfall-Managements, BCM

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