CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Gateway, Proxy, Router

CloudCommand GmbH chr.schumacher@gmx.tm

AGENDA

01 Gateway

02 Proxy

03 Router

01 Gateway

Was ist ein Gateway?

Ein **Gateway** ist eine Verbindung zwischen zwei Netzwerken mit unterschiedlichen Kommunikationsprotokollen. Es fungiert als **Übersetzer**, der Protokolle, Übertragungsgeschwindigkeit, Dateiformat, Adressierung und Hardware erkennt und anpasst, um eine reibungslose Kommunikation zwischen den Netzwerken sicherzustellen.

Wie funktionieren Gateways?

Gateways verbinden Netzwerke mit inkompatiblen Protokollen, z. B. ATM und IP-Netze, durch **Protokollumsetzung**. Dabei werden eingehende Daten konvertiert und an das Zielnetz weitergeleitet. Zusätzlich können sie **überflüssige Informationen** entfernen, die im Zielnetzwerk nicht benötigt werden. Beispielsweise werden Daten aus einem IPX/SPX-Netzwerk für ein TCP/IP-Netz angepasst, um eine fehlerfreie Kommunikation zu ermöglichen.

Gateways im OSI-Modell?

Das **OSI-Modell** (Open Systems Interconnection) ist ein von der ISO entwickeltes **Referenzmodell**, das die Kommunikation zwischen verschiedenen Systemen standardisiert. Es beschreibt, wie Netzwerke unabhängig von Protokollen sowie Hard- und Software-Grenzen miteinander kommunizieren können.

Das Modell besteht aus **sieben Schichten (Layer)** und unterteilt sich in:

- **Transportorientierte Schichten** (Layer 1 bis 4) – Fokus auf Datenübertragung und Protokollsteuerung.
- **Anwendungsorientierte Schichten** (Layer 5 bis 7) – Fokus auf Datenverarbeitung und Darstellung für Anwendungen.

Rolle des Gateways:
Gateways agieren innerhalb dieser Schichten als Vermittler und ermöglichen, dass Informationen zwischen unterschiedlichen Netzwerken und Protokollen übertragen und konvertiert werden. Sie helfen dabei, Daten von einer Schicht zur nächsten weiterzuleiten und anzupassen, um eine reibungslose Kommunikation zu gewährleisten.

Arten von Gateways und ihre Funktionen:

Default- oder Standard-Gateway

- Router in IP-Netzwerken, der IP-Pakete weiterleitet, für die keine spezifischen Routing-Informationen vorhanden sind.
- Keine Protokollumsetzung, sondern reines Routing.

VoIP-Gateway

- Wandelt analoge Telefonsignale und andere PSTN-Signale (z. B. GSM) in digitale VoIP-Pakete um.
- Ermöglicht die Kommunikation zwischen älteren Telefonanlagen und modernen IP-basierten Geräten.

Cloud-Storage-Gateway

- Vermittelt zwischen lokalen Systemen und Cloud-Diensten.
- Funktionen: Verschlüsselung, Komprimierung, Datensicherung und Versionskontrolle.

Arten von Gateways und ihre Funktionen:

Media-Gateway

- Konvertiert Medienprotokolle (Bild, Ton, Video) zwischen unterschiedlichen Netzwerken.
- Unterstützt multimediale Kommunikation.

E-Mail-Sicherheitsgateway

- Filtert eingehende und ausgehende E-Mails auf schädliche Inhalte.
- Schützt das Netzwerk vor Malware und anderen Bedrohungen.

Arten von Gateways und ihre Funktionen:

IoT-Gateway

- Verbindet IoT-Geräte (Sensoren, Aktoren) mit weiterverarbeitenden Netzwerken.
- Ermöglicht die Anbindung an Cloud-Dienste und übernimmt die Datenweiterleitung.

Secure Web Gateway (SWG)

- Platziert sich zwischen dem Internet und dem Unternehmensnetzwerk.
- Filtert unsichere Inhalte und schützt vor Bedrohungen wie schädlichem Code oder Datenschutzverletzungen.
- Häufig eingebettet in Sicherheitskonzepte wie Secure Access Service Edge (SASE).

Diese Gateways sind essenziell für die Interoperabilität und Sicherheit moderner Netzwerke.

Beispiele und Anwendungsgebiete von Gateways:

Unternehmensnetzwerke

- Gateways verbinden verschiedene Abteilungen und Standorte miteinander und ermöglichen den firmeninternen Datenaustausch.
- Sie unterstützen mobiles Arbeiten, indem sie die Kommunikation und den Zugriff auf Netzwerke unabhängig vom Arbeitsort ermöglichen.

Internet of Things (IoT)

- IoT-Gateways ermöglichen die Kommunikation zwischen vernetzten Geräten.
- Beispiele: Sensoren und Produktionsanlagen in einer **Smart Factory** oder Verkehrssteuerungssysteme in einer **Smart City**.

Beispiele und Anwendungsgebiete von Gateways:

Cloud Computing

- Ein Cloud-Gateway stellt die Verbindung zwischen lokalen Endgeräten und Cloud-Diensten her.
- Es ermöglicht standortunabhängigen Zugriff auf Cloud-Daten und -Anwendungen, wie etwa bei **Microsoft 365 Business**.

Verknüpfung unterschiedlicher Technologien

- Gateways sorgen für die Kompatibilität zwischen verschiedenen Technologien und Protokollen.
- Beispiel: Voicemails von Festnetztelefonen werden durch Gateways konvertiert, sodass sie auch über mobile Geräte abgerufen werden können.

Unterschied zwischen Gateway und Router:

- **Gateway**
  a. Funktion: Verbindet **Netzwerke mit unterschiedlichen Protokollen** oder Geräten mit verschiedenen Kommunikationsarten.
  b. Wird auch als **Protokollkonverter** bezeichnet, da es Protokolle umsetzt, damit Netzwerke miteinander kommunizieren können.
  c. Beispiel: Ein VoIP-Gateway wandelt analoge Telefonsignale in VoIP-Datenpakete um.
- **Router**
  a. Funktion: Vermittelt und leitet Datenpakete zwischen **Netzwerken mit dem gleichen Protokoll** (z. B. TCP/IP).
  b. Liest die **Adressinformationen** in den Datenpaketen und leitet diese gemäß **Routing-Tabellen** und **Routing-Richtlinien** weiter.
  c. Beispiel: Ein Heimrouter verbindet das lokale Netzwerk (LAN) mit dem Internet (WAN), ohne Protokolle umwandeln zu müssen.

Herausforderungen bei der Gateway-Implementierung

Protokollkompatibilität: Unterschiedliche Standards müssen übersetzt werden.

Latenz und Leistung: Konvertierung von Daten kann Verzögerungen verursachen.

Sicherheit: Schutz vor Angriffen und Datenverlust ist essenziell.

Skalierbarkeit: Gateways müssen wachsende Netzwerke unterstützen.

Fazit

Gateways sind ein zentraler Bestandteil moderner Netzwerkinfrastrukturen. Sie ermöglichen nicht nur die Kommunikation zwischen Systemen mit unterschiedlichen Protokollen, sondern tragen auch erheblich zur Sicherheit und Effizienz bei. Ihre Entwicklung geht immer stärker in Richtung Software-Definierte Netzwerke, KI-basierte Sicherheit und IoT-Integration.

02 Proxy

Was ist ein Proxy?

Ein Proxy-Server ist eine Vermittlungsinstanz zwischen einem Nutzer und einer Netzwerk-Ressource (z. B. einer Webseite).

Er wird zwischengeschaltet, um verschiedene Funktionen zu erfüllen, wie Sicherheit, Anonymität oder Performance-Optimierung.

Warum Proxy-Server nutzen?

✅ **Vorteile eines Proxy-Servers**

Anonymität & Datenschutz

Die eigene IP-Adresse wird verschleiert, sodass die Identität geschützt bleibt.

Umgehung von Ländersperren & Zensur

Ermöglicht den Zugriff auf gesperrte Inhalte, z. B. geografisch eingeschränkte Videos oder Websites.

Sicherheitsfilter & Inhaltskontrolle

Unternehmen und Organisationen können über Proxys bestimmte Inhalte sperren (z. B. schädliche oder illegale Webseiten).

Warum Proxy-Server nutzen?

Performance-Optimierung

Proxy-Server können Inhalte zwischenspeichern (Caching) und so die Ladezeiten für oft besuchte Seiten verringern.

Schutz für interne Netzwerke

Reverse-Proxys schützen Server vor direktem Zugriff durch das Internet und filtern schädliche Anfragen heraus.

Warum Proxy-Server nutzen?

❌ **Nachteile eines Proxy-Servers**

Phishing-Risiko

Hacker können gefälschte Webseiten über Proxys erstellen, um sensible Nutzerdaten wie Passwörter abzufangen.

Vertrauenswürdigkeit des Proxys

Öffentliche oder unsichere Proxys können selbst Daten speichern und Nutzeraktivitäten überwachen.

Geschwindigkeitsverlust

Ein Proxy kann die Internetverbindung verlangsamen, wenn er nicht ausreichend leistungsfähig ist oder stark frequentiert wird.

Mangelnder Datenschutz bei unsicheren Proxys

Einige Proxys protokollieren Daten und können sie an Dritte weitergeben.

Anwendungsbereiche für Proxy-Server

Beschleunigung durch Caching

Proxy-Server speichern häufig abgerufene Daten zwischen (z. B. Webseiten, Bilder oder Skripte).

Dadurch können wiederholte Anfragen schneller beantwortet werden.

Reduziert die Serverlast und verbessert die Antwortzeiten.

Anwendungsbereiche für Proxy-Server

Lastenverteilung & Bandbreitenoptimierung

Ein Proxy kann Bandbreitenzuteilung kontrollieren, um eine gleichmäßige Nutzung der Ressourcen sicherzustellen.

Er verhindert, dass einzelne Clients zu viel Bandbreite beanspruchen.

Bei mehreren Internetleitungen sorgt er für eine effiziente Lastverteilung.

Anwendungsbereiche für Proxy-Server

Sicherheitsfilter & Zugangskontrolle

Unternehmen setzen Proxys ein, um bestimmte Inhalte zu blockieren (z. B. Social Media oder unsichere Webseiten).

Schutz vor Malware und Phishing durch gefilterte Anfragen.

Anwendungsbereiche für Proxy-Server

Anonymisierung & Datenschutz

Nutzer können ihre IP-Adresse verbergen, um ihre Identität zu schützen.

Ermöglicht den Zugriff auf geografisch eingeschränkte Inhalte.

Anwendungsbereiche für Proxy-Server

Schutz interner Netzwerke (Reverse Proxy)

Schützt Server vor direkten Zugriffen aus dem Internet.

Filtert und analysiert Anfragen, bevor sie an interne Systeme weitergeleitet werden.

Application-Level Proxy vs. Circuit-Level Proxy

Merkmal	Application-Level Proxy	Circuit-Level Proxy
Schicht im OSI-Modell	Schicht 7 (Anwendungsschicht)	Schicht 3-4 (Vermittlungs- & Transportschicht)
Analyse von Datenpaketen	Ja, kann Inhalte prüfen und filtern	Nein, keine inhaltliche Analyse
Funktion	Blockieren, Modifizieren, Weiterleiten von Daten gemäß Regeln	Filtert Datenpakete basierend auf Ports und IP-Adressen
Bezeichnung	Applikationsfilter	Firewall-Filtermodul
Filterprinzip	Feingranulare Kontrolle über Inhalte	Alles-oder-Nichts-Prinzip
Einsatzbereich	Web-Filterung, E-Mail-Sicherheit	Basis-Firewall-Funktion, grundlegender Zugriffsschutz

Proxy vs. VPN

Merkmal	Proxy-Server	VPN (Virtuelles Privates Netzwerk)
Schicht im OSI-Modell	Schicht 3, 4 oder 7	Schicht 2-3
Anwendungsbereich	Leitet spezifischen Traffic (z. B. Webbrowser) um	Leitet gesamten Netzwerkverkehr um
Verschlüsselung	Meist keine oder begrenzt	Starke Verschlüsselung
Sicherheit	Grundlegender Schutz	Höhere Sicherheit und Datenschutz
Geschwindigkeit	Schneller, da keine oder geringe Verschlüsselung	Langsamer durch Verschlüsselung
IP-Verschleierung	Ja, aber oft nur für eine App oder einen Browser	Ja, für das gesamte Gerät

Fazit

Proxy-Server sind vielseitig einsetzbar – sie **beschleunigen den Zugriff**, **optimieren Bandbreiten**, **schützen Netzwerke** und **bieten Anonymität**.

Sie sind daher ein wichtiger Bestandteil der IT-Infrastruktur in Unternehmen und Netzwerken.

Application-Level Proxys sind leistungsfähig für detaillierte Inhaltsfilterung und Sicherheitsrichtlinien.

Circuit-Level Proxys bieten grundlegende Zugriffskontrolle und werden oft in Firewalls integriert.

Proxys sind schneller, aber **VPNs bieten mehr Sicherheit**, da sie den gesamten Datenverkehr verschlüsseln. Die Wahl hängt vom Anwendungszweck ab!

03 Router

Was ist ein Router?

Ein Router ist ein Hardwaregerät, das Datenverkehr zwischen einem lokalen Netzwerk und dem Internet steuert.

Er leitet Datenpakete anhand von IP-Adressen an die richtigen Geräte weiter, wodurch mehrere Geräte dieselbe Internetverbindung nutzen können.

Zusätzlich ermöglicht ein Router die Bildung lokaler Netzwerke, in denen vernetzte Geräte miteinander kommunizieren und Dateien teilen können.

Was macht ein Router?

Ein Router verwaltet die Kommunikation zwischen Netzwerken, indem er Datenpakete basierend auf Internetprotokollen zum richtigen Ziel leitet.

Dabei ermittelt er den schnellsten und effizientesten Pfad anhand eines metrischen Werts.

Router stellen sicher, dass Daten sicher und zuverlässig zwischen Netzwerkknoten übertragen werden, ähnlich wie Flugverkehrskontrolltürme den Flugverkehr organisieren.

Wie funktionieren Router?

Router arbeiten mit einem Modem zusammen, um Datenpakete zwischen Geräten und dem Internet zu übertragen.

Der Router empfängt Datenpakete von angeschlossenen Geräten und leitet sie über das Modem an den entsprechenden Server weiter.

Der Server sendet die angeforderten Daten zurück, und der Router verteilt sie an das richtige Gerät im lokalen Netzwerk.

Dabei nutzt der Router IP-Adressen, die wie physische Adressen fungieren, um sicherzustellen, dass die Datenpakete ihr Ziel erreichen.

Internetprotokolle regeln diesen gesamten Prozess.

Worin besteht der Unterschied zwischen einem Router und einem Modem?

Ein **Modem** verbindet das Netzwerk mit dem Internet, indem es Signale des Internetdienstanbieters (ISP) empfängt und in für lokale Geräte lesbare Daten umwandelt. Es stellt die Verbindung zum Wide Area Network (WAN) her.

Ein **Router** hingegen erstellt ein lokales Netzwerk (LAN) und weist den angeschlossenen Geräten lokale IP-Adressen zu. Er verwaltet die Kommunikation zwischen den Geräten und dem Internet. Ohne ein Modem hätte der Router keinen Zugang zum Internet, und ohne einen Router könnten die Geräte im Netzwerk nicht effizient miteinander oder mit dem Modem kommunizieren.

Arten von Routern

Heimrouter: Häufig vom Internetanbieter bereitgestellt, verbinden Haushalte mit dem Internet.

Unternehmensrouter: Haben erweiterte Funktionen wie VPN, VLAN-Unterstützung, Firewall und Lastverteilung.

Core-Router: In großen Netzwerken, z. B. bei Internetdienstanbietern, übernehmen sie den Verkehr auf der höchsten Netzwerkschicht.

Gibt es noch Fragen?

CloudCommand GmbH chr.schumacher@gmx.tm

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm