

Einleitung

Während auf HTTP basierte Dateiübertragung wie Nextcloud, Google Drive, OneDrive, iCloud im privaten und zunehmend auch im Geschäftsumfeld eine grössere Rolle einnehmen, spielen die Netzwerkübertragungsprotokolle SMB (CIFS), NFS, FTP, iSCSI weiterhin eine wichtige Rolle. Für IT-Fachpersonen spielt zudem das TFTP Protokoll aufgrund dessen Einfachheit eine wichtige Rolle. Nicht vergessen werden darf SSH, dass nebst dem Remote Terminal auch eine verschlüsselte Dateiübertragung (SFTP) bietet.

Ports

TCP- und UDP-Ports sind eine Software-Abstraktion, um parallele Kommunikationsverbindungen einer oder mehreren Anwendungen voneinander unterscheiden zu können. Ähnlich wie IP-Adressen zur Adressierung von Rechnern in Netzwerken dienen, adressieren Ports spezifische Anwendungen und ihre Verbindungen, die auf einem Rechner laufen.

Zuordnung zwischen Datenpaket und Anwendung: Der TCP-Port

Ein Netzwerk-Port ist eine Adresse, mit deren Hilfe sich UDP- oder TCP-Verbindungen eindeutig bestimmten Anwendungen zuordnen lassen. Zu einer Verbindung gehört auf beiden Seiten jeweils ein Port. Ports können eine fortlaufende Nummer im Bereich von 0 bis 65535 annehmen.

Zweck eines Netzwerk-Ports ist die Zuordnung von UDP- oder TCP-Paketen einer IP-Verbindung zu einer bestimmten Anwendung. Zusammen mit der IP-Adresse bildet der Netzwerk-Port die vollständige Adresse einer Anwendung auf einem Ziel- oder Absendersystem.

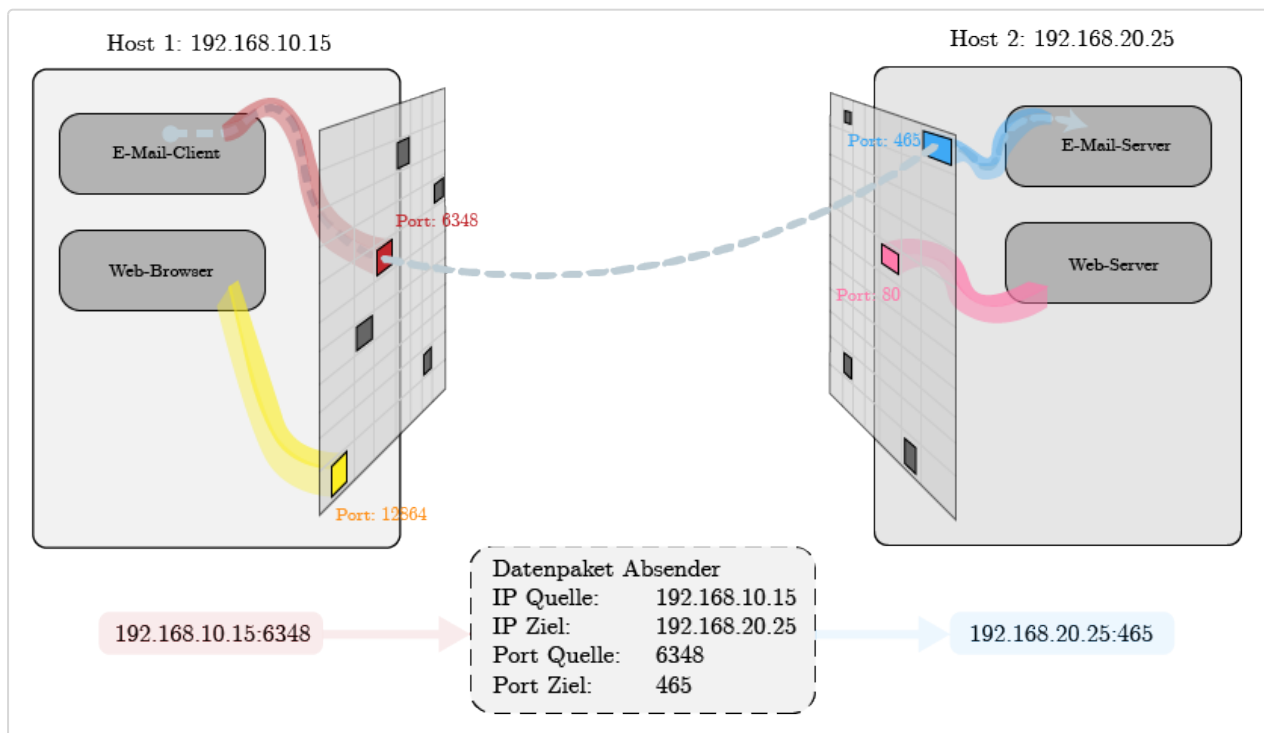
Ein Port ist somit jeweils mit einer spezifischen Applikation verbunden. Im untenstehenden Beispiel sind dies folgende:

Host 1:

- Port 6348 ist mit dem E-Mail Client
- Port 12564 ist mit dem Web-Browser verbunden

Host 2:

- Port 465 ist mit dem E-Mail-Server verbunden
- Port 80 ist mit dem Web-Server verbunden



Es kann nun daher mit der IP-Adresse und der Port-Nummer eine eindeutige Verbindung zwischen zwei Applikationen hergestellt werden. Im obigen Beispiel stellt der E-Mail Client eine Verbindung mit dem E-Mail Server her um Daten auszutauschen. Diese Verbindung funktioniert in **beide Richtungen**. Eine Verbindung hat somit in jedem Fall zwei Ports, eine auf der Client-Seite und eine auf der Server-Seite.

Dafür muss nun aber der Teilnehmer, welche die Verbindung aufbauen möchte die IP und die Port-Nummer des Kommunikations-Partners kennen. Dazu sind Portnummern fest einzelnen Anwendungen

zugeordnet. Andere Portnummern können dynamisch vergeben werden. So ein fest zugewiesener Port ist der Port 465. Dahinter ist im Normalfall ein E-Mail Server zu finden. Somit kann der Host 1, welcher eine E-Mail an den Host 2 einliefern möchte, den Port 465 als Zielport verwenden.

Funktionsweise der Ports

Anwendungsserver (Wie z. B FTP-Server, E-Mail Server, DNS-Server) fordern bei ihrem Start beim Betriebssystem einen Port an, auf dem sie Verbindungen entgegennehmen können. Für Standard-Anwendungen handelt es sich immer um die gleichen festen Portnummern. Anschließend ist der Netzwerk-Port fest mit der Anwendung verknüpft. Clients erhalten vom Betriebssystem in der Regel einen zufälligen Port dynamisch zugewiesen. Diesen können sie als Absender-Port nutzen, um eine Verbindung zu einem Zielsystem aufzubauen. Der Client muss die Ziel-IP-Adresse und den Ziel-Port des Servers kennen. Beim Verbindungsaufbau lernt der Server den Port des Clients kennen und adressiert Antwortpakete an diesen.

Standardisierung und Einteilung der Ports

Die Portnummern sind von der IANA und der ICANN (Internet Corporation for Assigned Names and Numbers) in verschiedene Bereiche eingeteilt. Den Bereich der Standard-Ports oder Well Known Ports bilden die Portnummern 0 bis 1023. Sie sind fest einem bestimmten Anwendungsprotokoll zugeteilt. Anschließend folgt mit den Portnummern 1024 bis 49151 der Bereich der so genannten Registered Ports. Diese Netzwerk-Ports dürfen für die Registrierung verschiedener Anwendungen verwendet werden. Die Reservierung erfolgt wiederum über IANA und ICANN. Die Portnummern von 49152 bis 65535 nennen sich Dynamically Allocated Ports und stehen für die dynamische Zuordnung zur Verfügung. Clients nutzen diese Ports für ihre ausgehenden Verbindungen als Absender-Ports. Beispiele für Standard-Ports sind:

- TCP 21: File Transfer Protocol (FTP)
- TCP 23: Telnet
- TCP 80: Hypertext Transfer Protocol (HTTP)
- UDP 53: Domain Name System (DNS)

- UDP 69: Trivial File Transfer Protocol (TFTP)
- UDP 161: Simple Network Management Protocol (SNMP)

Die verschiedenen Portzustände

Je nach Status einer IP-Verbindung und der jeweiligen Anwendung können Netzwerk-Ports unterschiedliche Zustände annehmen. Über den Zustand ist definiert, ob die Kommunikation mit der verknüpften Anwendung möglich ist. Es existieren die drei grundsätzlichen Zustände offen (open), geschlossen (closed) und gefiltert (filtered).

Ist ein Netzwerk-Port offen, ist die Anwendung hinter diesem Port dazu bereit, Verbindungen entgegen zu nehmen.

Ein geschlossener Netzwerk-Port bedeutet, dass es keine Anwendung gibt, die über den Netzwerk-Port erreichbar ist. Verbindungsaufbauwünsche zu diesem Port werden aktiv abgelehnt. Auch durch eine Firewall geschützte Ports können den Zustand geschlossen aufweisen. In diesem Fall ist die dahinterliegende Anwendung ebenfalls unerreichbar.

Der Zustand gefiltert (auch geblockt genannt) weist darauf hin, dass eine Firewall den Netzwerk-Port schützt. Er ist weder offen noch geschlossen, ermöglicht aber ebenfalls keinen Verbindungsaufbau.

YouTube Videos:

<https://www.youtube.com/watch?v=g2fT-g9PX9o>

<https://www.youtube.com/watch?v=aQoFR6m1yOM>

<https://www.youtube.com/watch?v=RDotMcs0Erg>

Revision #2

Created 20 December 2022 21:47:12 by Admin

Updated 12 January 2023 00:40:09 by Admin