Detailbeschrieb Daniel-Patrick ; M182

Organisation der Firma

In dieser Arbeit wird die interne IT für ein Jungunternehmen aufgebaut. Dieses besteht aus einem (1) Mitarbeiter, sowie uns als externe IT. Die gewünschte Infrastruktur wird in folgenden genauer beschrieben.

Sicherheit

Interner und externer Verkehr

Durch die Segmentierung in LAN und DMZ ist es möglich, von intern aus auf alles zugreifen zu können. Wenn nötig, ist auch ein externer Zugriff auf den Fileserver möglich, ohne einen direkten Zugriff auf das LAN geben zu müssen. Somit ist dieses Setup skalierbar auf mögliche, kommende Use-Cases.

VPN/Tunneling

Durch die Nutzung von WireGuard ermöglichen wir dem Kunden, auf sichere Art und Weise auch remote auf seine Firmen-IT zuzugreifen. WireGuard selbst garantiert einen sicheren Datenverkehr dank der Nutzung von Private-Key-Verschlüsselung sowie einem entsprechenden Handshake. Die Verbindung zwischen den beiden Peers (hier der Kunde im Home-Office und sein Arbeitsnetzwerk) wird dadurch abgesichert.

Wazuh

Wazuh wird hier genutzt, um ein zentrales Monitoring von verschiedensten Aktivitäten im Netzwerk zu ermöglichen. Es ermöglich die Erkennung von Schwachstellen, sowie die Erkennung von unerwünschten Tätigkeiten, beziehungsweise Angriffen.
Um dies zu ermöglichen wird auf jedem Host im LAN und DMZ ein Wazuh-Agent eingerichtet, welcher die jeweiligen Clients überwacht.

OPNsense

OPNsense wird hier als Firewall genutzt. Dies ermöglicht es, den Verkehr zwischen den Netzwerkzonen nach Bedarf einzurichten, und wo nötig auch einzuschränken.

Datenhaltung

Um Files, welche im Rahmen der Arbeit erstellt und genutzt werden, sicher ablegen und verwalten zu können, wird hier ein NextCloud eingerichtet. Diese Software übernimmt das «heavy lifting» in Sachen Datenspeicherung und -verwaltung und vereinfacht somit den entsprechenden Umgang damit für den Kunden.

Geräte

Client / Server	***Name***	***OS***	***Funktion***
Client	vmLP1	Ubuntu 24.04 LTS	Remote Client
Client	vmLP2	Ubuntu 24.04 LTS	Linux Client
Server	vmLS1	Ubuntu Server 24.04 LTS	SSH-Gateway
Server	vmLS2	Ubuntu Server 24.04 LTS	Wazuh-Server
Server	vmLS3	Ubuntu Server 24.04 LTS	Fileserver

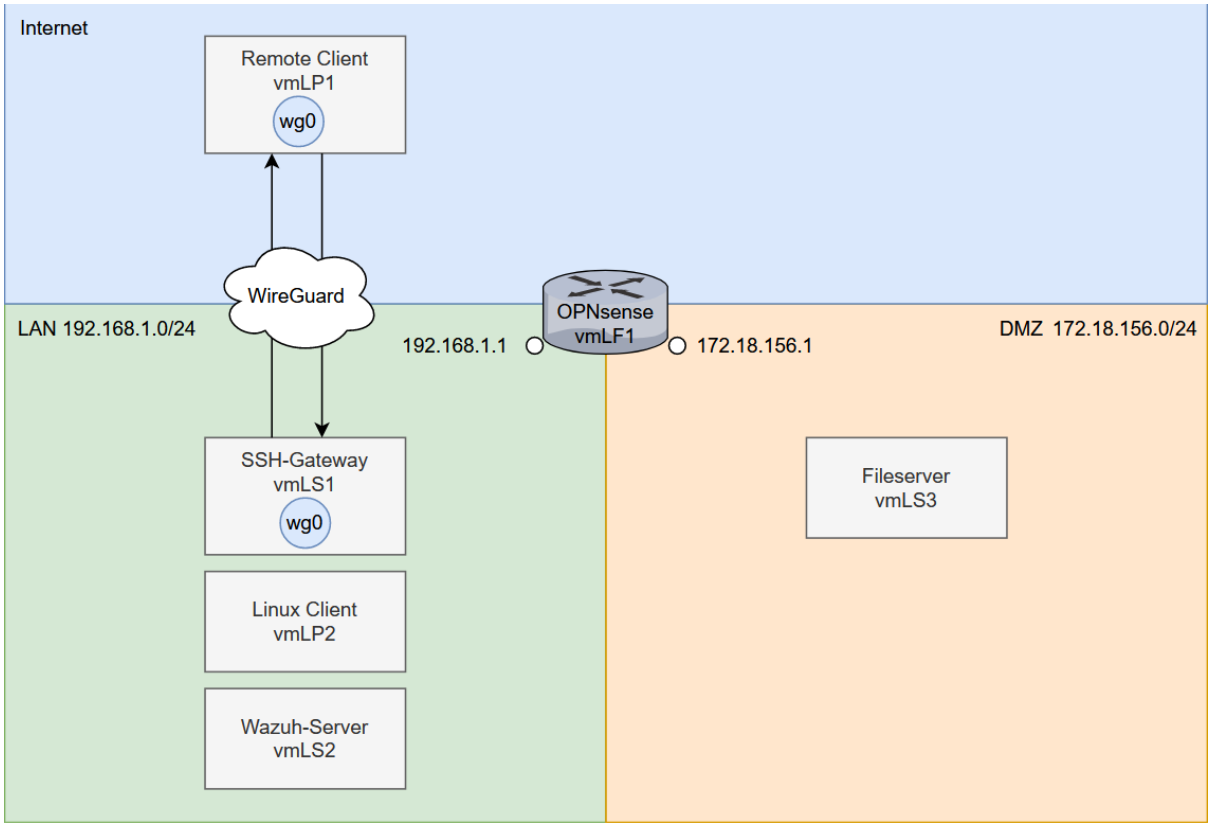
Netzwerke

Netzwerk-Name	***IP-Range***
Internet	*
LAN	192.168.1.0/24
DMZ	172.18.156.0/24

Software

Technologie	***Funktion in dieser Umgebung***
WireGuard*	Tunneling in das LAN
Wazuh	IPS/IDS/SIEM
OPNsense	Firewall/Router
Nextcloud*	Datenhaltung

Übersicht Netzwerk und Geräte



*Wir installieren dies jew. selber, hier bitte nur die VMs vorbereiten