

DMZ REISE VON KEANU UND ANTONY



ERSTELLT VON: KEANU UND ANTONY

INHALTS VERZEICHNIS

- EINLEITUNG
- NAMENSHEMA
- NETZWERKPLAN
- IP KONZEPT
- GERÄTEBESCHREIBUNG
- INSTALLATION / KONFIGURATION
- FIREWALL REGEL
- TESTING



Einleitung

In dieser Betriebsdokumentation geht es um die Demilitarisierte Zone (DMZ).

Wie funktioniert der DMZ

Ein Unternehmen kann eine Vielzahl von Daten haben, darunter Kunden-, Mitarbeiter-, Finanz-, Produkt-, Vertrags-, Marketing-, Projektmanagement-, Rechts-, IT-, Logistik- und Supportdaten. Sensible Daten wie Finanz-, Mitarbeiter- und Vertragsdaten sollten im LAN gespeichert werden, um zusätzliche Sicherheit zu gewährleisten. Weniger sensible Daten, die extern zugänglich sein müssen, wie bestimmte Kunden- oder Marketingdaten, können in der DMZ gespeichert werden.

Namenschema

Warum macht man ein Namensschema?

Wenn Sie eine Firma mit 600 Windows- und 700 Linux-Maschinen betreiben und alle Geräte ähnlich benennen, z.B. "Lin/01", kann es schnell zu Verwechslungen kommen. Daher benennen wir alle Geräte unterschiedlich und erstellen eine Tabelle, um die Bezeichnungen festzuhalten und Verwechslungen zu vermeiden.

Gerät	Benennung
Client	Name/-Nummer; z.b. Cli-1
Server	Win/Lin(Ser)-01; z.b. WinSer-01
Router	Rout/Name-Nummer; z.b. RoutTest-1

Netzwerkplan

Für was braucht man einen Netzwerk Plan:

Ein Netzwerkplan ist ein Wichtiger Bestandteil der Gestaltung, Implementierung und Verwaltung von Netzwerken.

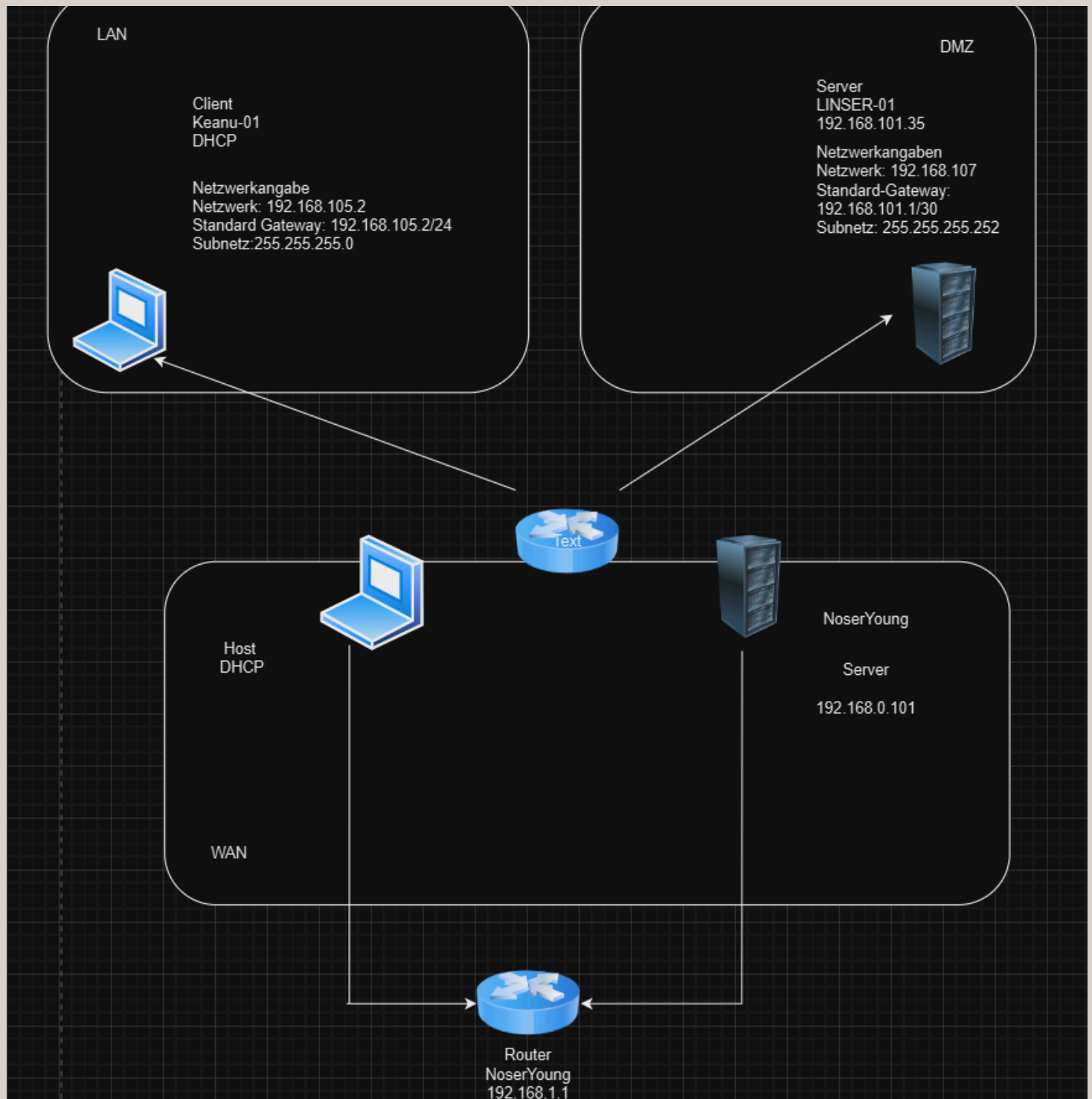
Hier sind einige Punkte Warum ein Netzwerkplan benötigt wird:

- **Struktur und Organisation:**

Es bietet einem eine klare Netzwerkarchitektur einschliesslich der Anordnung von Servern, Switches, Routern und andern Netzwerkgeräten.

- **Effizienz und Performance:**

Somit kann man eine gute Planung machen und Engpässe vermeiden.



Netzwerkplan

Von Keanu und Antony

IP Konzept

Ein IP-Konzept (Internet Protocol) ist das Prinzip wo die Grundlage für die Kommuntation im Internet und vielen anderen Netzwerken Bildet

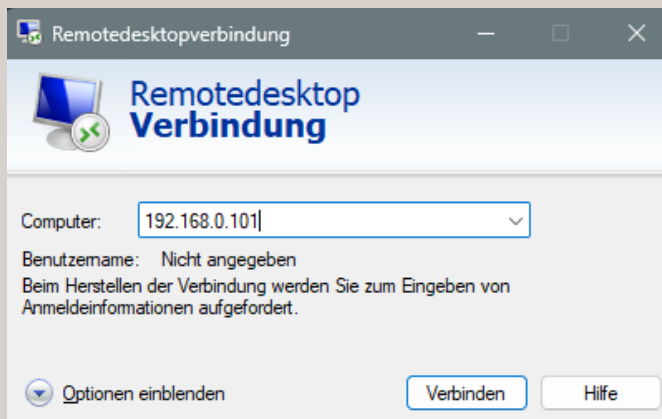
Gerätetyp	Art	Range
Router	Statisch	192.168.0.1
Kritische Infrastruktur*	Statisch	192.168.0.2 bis 192.168.0.20
Server	Statisch	192.168.0.21 bis 192.168.0.40
Clients	DHCP	192.168.0.50 bis 192.168.0.150
Management- und Reservierungsbereich	Statisch	192.168.0.41 bis 192.168.49

*Zum Beispiel: Drucker, Netzwerkspeicher (NAS)

1 Installation / Konfiguration

Remotezugriffe auf Server

IP Adresse eingeben und Anmelde Daten für Server



ISO und neuen PfSense Server

Als erstes haben wir einen neuen ETH 0 Kriiert was ein WAN ist ETH 1.

Windows Server aufgesetzt verbinden mit LAN IP,

Firewall Regel

Wir mussten die Firewall be

Testing

Testbereich	Testname	Beschreibung	Erwartetes Ergebnis	Mögliche Probleme
DMZ	Zugriff auf Webserver	Testen von den Zugriff auf den Linux-Webserver über die WAN-IP.	Der Webserver ist von außen erreichbar und zeigt die Webseite an.	- Firewall-Einstellungen blockieren den Zugriff. oder Falsche WAN-IP.
DMZ	Sicherheitsregel DMZ	Überprüfen, ob die DMZ-Firewallregeln den Zugriff auf unerlaubte Ports verhindern.	Der Zugriff auf nicht erlaubte Ports wird blockiert.	- Falsche oder fehlende Firewall-Regeln. oder eventuell Sicherheitslücken im Webserver.
LAN	DHCP-Funktionalität	Überprüfen, ob der DHCP-Dienst auf PFSense korrekte IP-Adressen im LAN-Bereich vergibt.	Geräte im LAN erhalten eine IP-Adresse aus dem /24-Bereich.	- DHCP-Dienst ist nicht aktiv. oder Falsche DHCP-Konfiguration.