ROC FRIESE POORT

VERSLAG PROJECT SECURITY

TYCHO WIJMENGA
238424

LUC HOEKSTRA
233730

Inleiding

Dit document beschrijft ons project in het kader van onze voorbereiding op de PvB (Proeve van Bekwaamheid) met betrekking tot beveiliging. Onze opdracht was om een NAT-router op basis van Linux te implementeren, samen met een Radius-server. Daarnaast moesten we een beveiligde SSH-verbinding opzetten voor het beheer van de WDS-server en een WDS implementeren voor het beheer en uitrollen van de Windows-clients. Dit verslag omvat een gedetailleerde beschrijving van de opdracht, analyse van de werkzaamheden, onderzoek naar mogelijke oplossingen, advies aan de opdrachtgever, en de uiteindelijke oplossing en testresultaten. We streven ernaar om een helder beeld te geven van ons uitgevoerde project en de behaalde resultaten.

Inhoudsopgave

Beschrijving van de opdracht

Dit document beschrijft de beveiligingsopties voor een klant. De opdracht is om een NAT-router op basis van Linux te installeren en daarbij een Radius-server te configureren. Daarnaast is het belangrijk om een beveiligde SSH-verbinding op te zetten voor het beheer van de WDS-server. Daarnaast is er ook een WDS opgezet om de Windows-clients te beheren en implementeren.

Eén van de Windows-clients moet zich aanmelden bij de Radius-server en de draadloze apparaten moeten ook via deze server worden geauthenticeerd. We hebben dus zowel hardwarecomponenten te installeren als software te configureren.

Onze opdracht is om deze opdracht zorgvuldig uit te voeren en goed te documenteren. We hebben ons gericht op het waarborgen van de beveiliging en het leveren van een betrouwbare oplossing aan de klant.

Analyse

Bij de analyse van de werkzaamheden hebben we gekeken naar de specifieke taken en stappen die nodig waren om de opdracht succesvol uit te voeren. We hebben de vereisten van de klant geanalyseerd en geïdentificeerd welke componenten en configuraties nodig waren. Daarnaast hebben we ook gekeken naar eventuele beperkingen of uitdagingen die we konden tegenkomen tijdens de implementatie. Deze analyse heeft ons geholpen om een duidelijk beeld te krijgen van wat er precies moest gebeuren en om een plan op te stellen voor de uitvoering van de opdracht.

Onderzoek

Tijdens het onderzoek hebben we verschillende mogelijkheden verkend om aan de eisen van de opdracht te voldoen. We hebben onderzocht welke technologieën en tools het meest geschikt waren voor het opzetten van een NAT-router op basis van Linux en het configureren van een Radius-server. Daarnaast hebben we gekeken naar de beste praktijken voor het opzetten van een beveiligde SSH-verbinding en het implementeren van een WDS voor het beheer van de Windows-clients. We hebben ook de verschillende opties voor authenticatie via de Radius-server onderzocht. Het onderzoek heeft ons geholpen om de meest geschikte oplossingen te selecteren en om ons advies aan de opdrachtgever te onderbouwen.

Advies aan de opdracht gever

Ik schrijf u met betrekking tot het project waarbij u een Linux NAT-router wilt implementeren, inclusief een Radiusserver en Windows Deployment Services (WDS) voor het beheer en de uitrol van Windows-clients. Gebaseerd op de verstrekte informatie, wil ik graag enkele adviezen delen om u te helpen bij een succesvolle implementatie van dit project.

Keuze van de Linux-distributie:

Het selecteren van een geschikte Linux-distributie voor uw NAT-router is essentieel. U kunt overwegen om te kiezen voor een robuuste en goed ondersteunde distributie zoals Ubuntu Server. Ubuntu is een van de bekenste distrubuties hierdoor is er veel support voor en werken de meeste programma’s er goed mee.

NAT-routerconfiguratie:

Configureer de NAT-functionaliteit op de Linux-router om netwerkverkeer tussen het interne netwerk en het externe internet mogelijk te maken. Zorg ervoor dat u een betrouwbare firewall implementeert om de beveiliging van het netwerk te waarborgen. Hiervoor geven wij het advies om IP-Tables in de Linux omgeving

Radiusserverimplementatie:

Installeer en configureer de Radiusserver op de Linux NAT-router. Er zijn verschillende Radiusserver-softwareopties beschikbaar, zoals FreeRADIUS en TekRADIUS. Onze voorkeur gaat er naar uit om FreeRadius te gebruiken dit is naar onze meening de meest simpele en stabiele oplossing.

Beveiligde SSH-verbinding voor het beheer van de WDS-server:

Stel een beveiligde SSH-verbinding in voor het beheer van de WDS-server. Dit zorgt voor een versleutelde communicatie en verhoogt de beveiliging van het beheerproces. Zorg ervoor dat u sterke SSH-sleutels gebruikt en onnodige toegangspunten tot de SSH-service beperkt om mogelijke beveiligingsrisico's te verminderen.

Opzetten van een Windows Deployment Services (WDS)-server:

Implementeer een WDS-server om het beheer en de uitrol van Windows-clients mogelijk te maken. Zorg ervoor dat de WDS-server correct is geconfigureerd en gekoppeld is aan uw Windows-installatiekopieën (images). U kunt de WDS-server gebruiken om geautomatiseerde installaties en configuraties van Windows-clients uit te voeren, waardoor het implementatieproces efficiënter wordt.

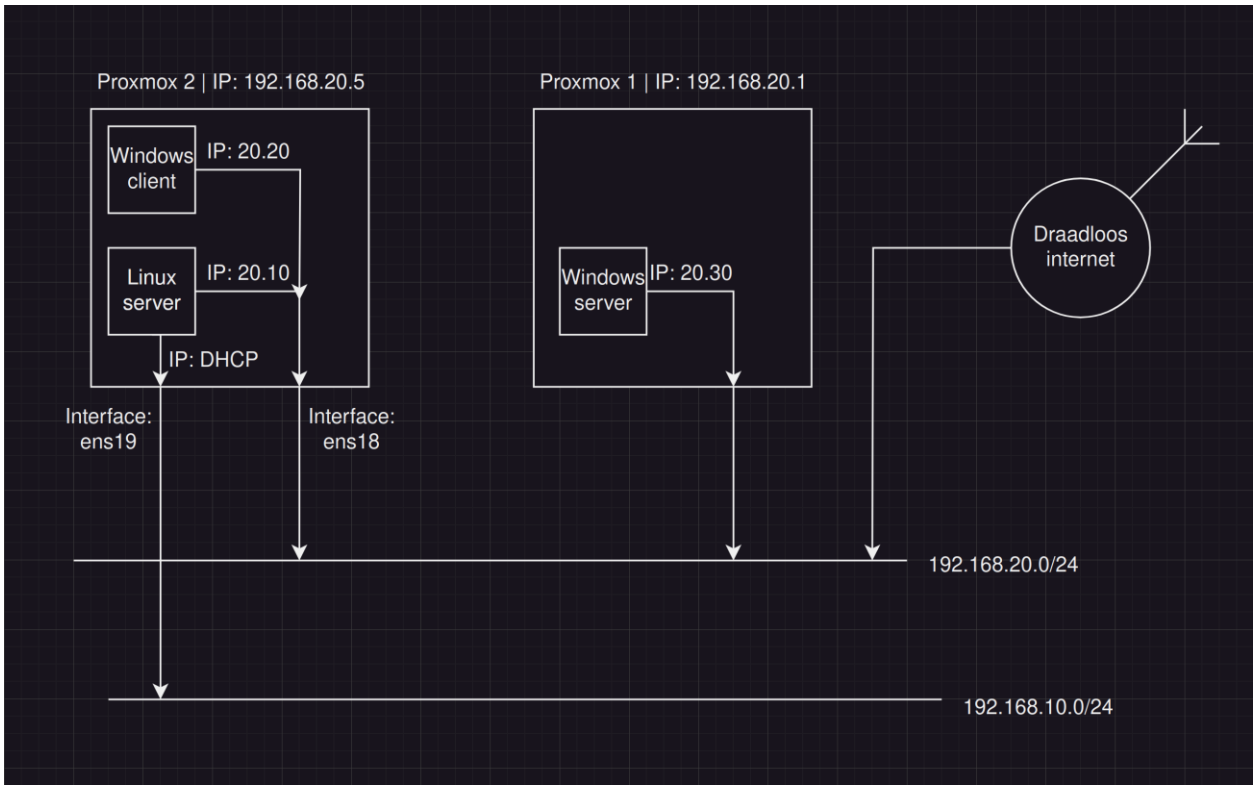
Radius-authenticatie voor Windows-clients en draadloze apparaten:

Stel de Windows-clients en draadloze apparaten zo in dat ze zich authenticeren via de Radiusserver. Dit zorgt voor een centraal beheer van gebruikersauthenticatie en verhoogt de beveiliging van het netwerk. Zorg ervoor dat de Radiusserver correct is geconfigureerd om de juiste identiteits- en beveiligingsprotocollen te ondersteunen voor zowel de Windows-clients als de draadloze apparaten.

Netwerk

Hieronder is het netwerk van de omgeving beschreven.

Netwerk tekening:



Apparaat	Interface	IP	prefix
Proxmox server 1	-	192.168.20.1	/24
VM Windows server	-	192.168.20.30	/24
Proxmox server 2	-	192.168.20.5	/24
Linux server	ens18	192.168.20.10	/24
Linux server	ens19	DHCP	/24
Windows client	-	DHCP	/24

Linux server

De linux server is hieronder uitgewerkt. De uitwerking bestaat uit drie onderdelen. Onderdeel een is algemene informatie over de server, onderdeel twee bestaat uit de uitwerking van de radius server en in onderdeel drie word de NAT router uitgewerkt.

Algemene informatie

Versie: Ubuntu-22.0.1-live-server-amd64

Yourname: natradius

Servername: natradius

username: vogel

wachtwoord: FPitDr88

OpenSSH geinstalleerd tijdens de installatie

Installatie Radius server

In dit project hebben we FreeRADIUS geïnstalleerd en geconfigureerd op een Ubuntu-server. FreeRADIUS is software waarmee we gebruikersauthenticatie en netwerktoegangscontrole kunnen beheren. Het stelt ons in staat om alleen geautoriseerde gebruikers toegang te verlenen tot ons netwerk. We hebben ook de configuratie van onze TP-Link router aangepast om deze te laten authenticeren bij de RADIUS-server.

Hieronder vind je de configuratie van de RADIUS-server, die wordt gebruikt voor het beheren van de draadloze verbinding via de TP-Link router. Met behulp van deze configuratie kunnen we ervoor zorgen dat alleen geauthenticeerde gebruikers toegang krijgen tot het draadloze netwerk.

In de configuratie van de Radius server hebben wij een gebruiker aan moeten maken. Met deze gebruiker logt de TP-Link router in op de radius server. Hieronder staat de configuratie van deze gebruiker. De gebruiker word aangemaakt in het client.conf bestand.

Client.conf:

```
client tp-link-router {

    ipaddr = 192.168.1.1

    secret = sharedsecret

    require_message_authenticator = no

    nas_type = other

    shortname = tp-link-router

}
```

Ook moet er in de configuratie een gebruiker aan worden gemaakt om in te kunnen loggen op de router via de Radius server. Dit word gedaan in het configuratie bestand users.conf.

Users.conf:

```
vogel Cleartext-Password := "FPitDr88"
```

Installatie NAT

Voor ons project hebben we een NAT-router geïnstalleerd op een Linux-systeem met behulp van IPTables. Een NAT-router stelt ons in staat om meerdere apparaten in ons netwerk te verbinden met het internet, zelfs als we maar één openbaar IP-adres hebben. IPTables is een softwaretool waarmee we het netwerkverkeer kunnen beheren en routeren.

In dit verslag beschrijven we de stappen die we hebben genomen om de NAT-router met IPTables in te stellen. We hebben IPTables-regels ingesteld, IP-forwarding geactiveerd en IP-adressen toegewezen aan onze apparaten. Met deze NAT-router kunnen meerdere apparaten veilig verbinding maken met het internet.

Laten we nu verder gaan met de gedetailleerde beschrijving van de installatie en configuratie van de NAT-router met IPTables op ons Linux-systeem.

Ip tables hebben wij met de volgende commando's ingesteld:

$ iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADECopy

Iptables opslaan

$ sudo iptables-save > /etc/iptables/rules.v4

```
root@natradius:/home/vogel# sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             203.0.113.10         tcp dpt:ssh to:192.168.20.1:22

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
MASQUERADE  all  --  anywhere             anywhere
root@natradius:/home/vogel#
```

TP-Link router

Voor dit project hebben wij een TP-Link router moeten gebruiken. Deze router moet gebruik maken van de radius server voor authenticatie.

Algemene informatie

wachtwoord: FPitDr88

IP: Zie IP plan

"Voor de beveiliging en optimalisatie van ons draadloze netwerk hebben we besloten om onze TP-Link router in te stellen als een Access Point. Hierbij hebben we ook de draadloze netwerknaam gewijzigd naar 'Afluisterbusje'.

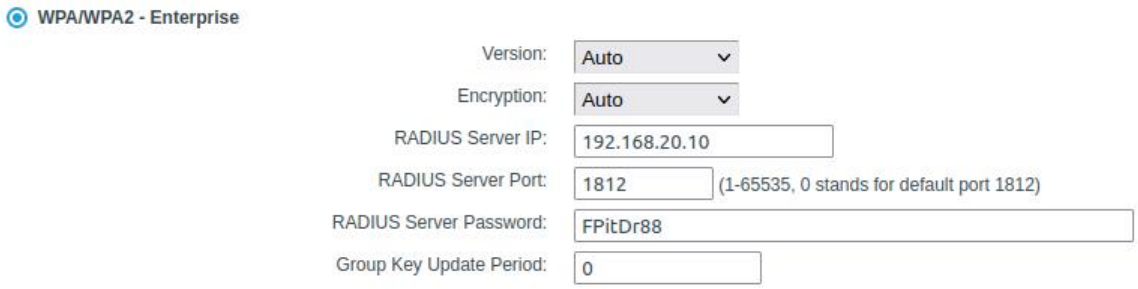
Om deze configuratie te realiseren, hebben we de volgende stappen uitgevoerd. Allereerst hebben we een ethernet-kabel aangesloten op een LAN-poort van de TP-Link router en deze verbonden met een computer. Vervolgens hebben we een webbrowser geopend en het IP-adres van de router ingevoerd in de adresbalk.

Na succesvol inloggen op de routerinterface, hebben wij als eerste de router in acces point mode gezet.

Daarna hebben we de instellingen voor 'Netwerk' of 'LAN' opgezocht. Hier hebben we de DHCP-server uitgeschakeld. Dit zorgt ervoor dat de router geen IP-adressen toewijst aan apparaten die verbinding maken met het netwerk. Dit hebben we zo gedaan aangezien de klant gebruikt maakt van een PFsense met daarop een DHCP server.

Daarna zijn we naar de instellingen voor 'Wireless' of 'WiFi' gegaan in het routermenu. Hier hebben we de draadloze netwerknaam (SSID) gewijzigd naar 'Afluisterbusje'. We hebben ook een nieuw wachtwoord ingesteld om de beveiliging te versterken.

Ook hebben wij deze router zo ingesteld dat er bij inloggen op het netwerk gebruik word gemaakt van de radius server. Bij het inloggen op het draadloze netwerk. Zie hieronder een afbeelding met de informatie.



WDS server VM

Voor ons project hebben wij een Windows Deployment Services (WDS) geïnstalleerd en geconfigureerd. Het doel van dit onderdeel is om een gestandaardiseerde en veilige methode te implementeren voor het beheer en uitrollen van Windows clients in het netwerk.

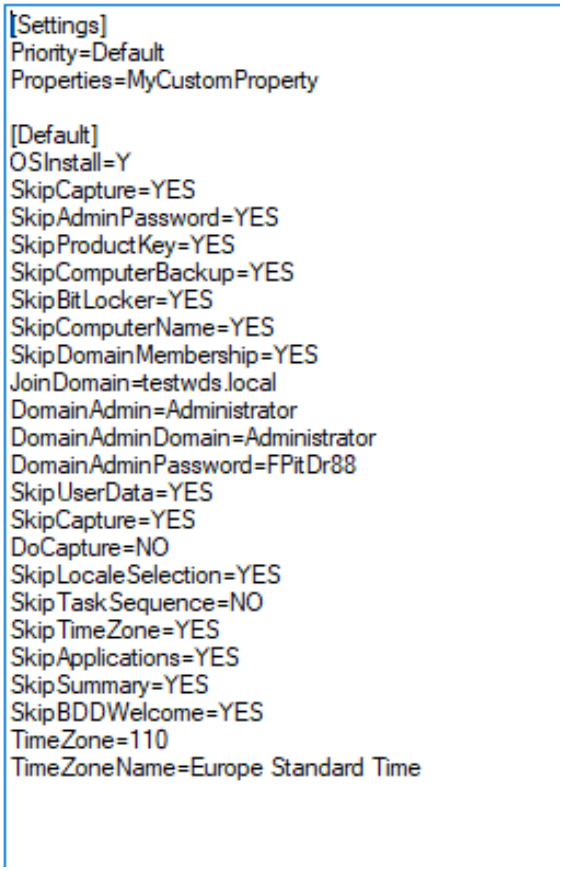
Windows server configuratie

Iso: en_windows_server_2019_180days.iso
Ram: 4 GB
Cores: 2
ID: 102
Licentie: geen

Hostname: WDS-server
Domain: WDS-server.tv
IP: Zie IP plan
Gebruiker: administartor
Wachtwoord: FPitDr88

MDT Deployment share rules:

Hieronder staat een afbeelding met daarin de deployment share rules:



```
[Settings]
Priority=Default
Properties=MyCustomProperty

[Default]
OSInstall=Y
SkipCapture=YES
SkipAdminPassword=YES
SkipProductKey=YES
SkipComputerBackup=YES
SkipBitLocker=YES
SkipComputerName=YES
SkipDomainMembership=YES
JoinDomain=testwds.local
DomainAdmin=Administrator
DomainAdminDomain=Administrator
DomainAdminPassword=FPitDr88
SkipUserData=YES
SkipCapture=YES
DoCapture=NO
SkipLocaleSelection=YES
SkipTaskSequence=NO
SkipTimeZone=YES
SkipApplications=YES
SkipSummary=YES
SkipBDDWelcome=YES
TimeZone=110
TimeZoneName=Europe Standard Time
```

Bootstrap config

Hieronder staat een afbeelding met de configuratie:

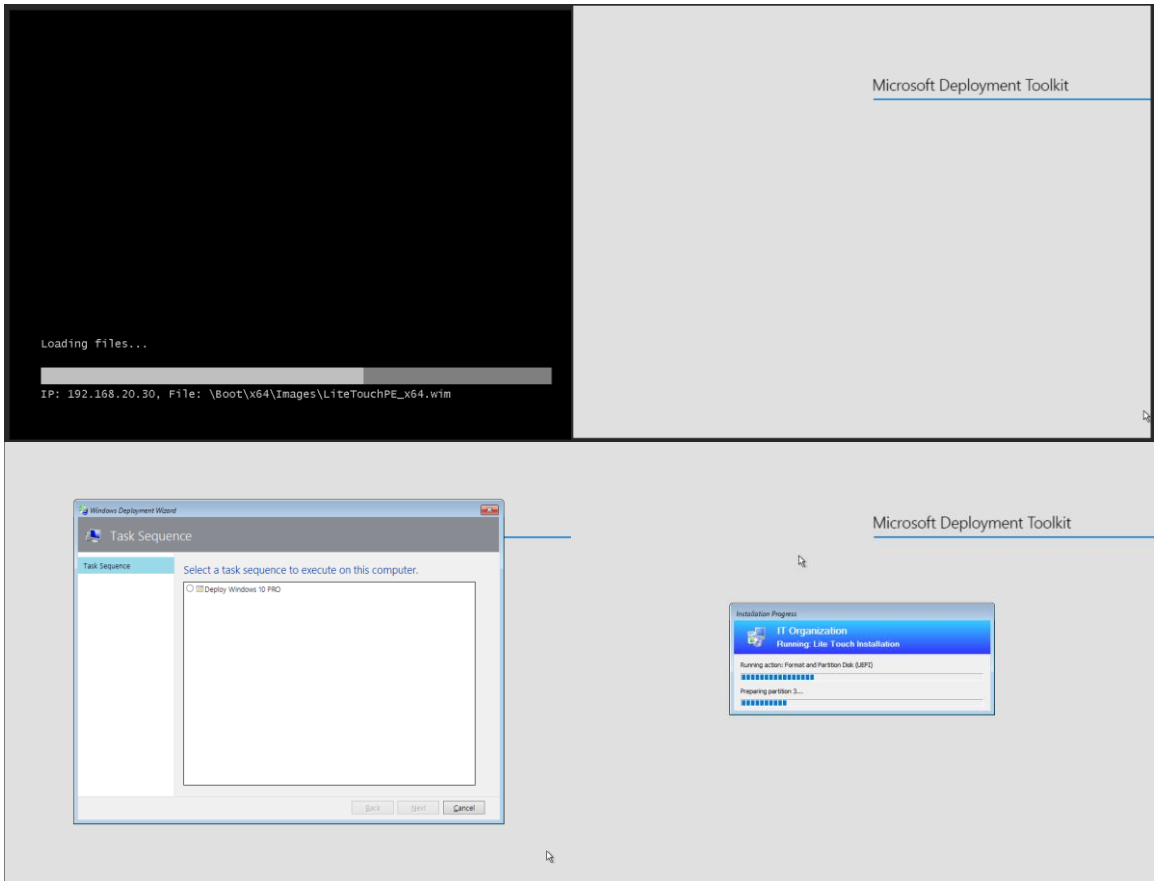
Bootstrap - Notepad

File Edit Format View Help

```
[Settings]
Priority=Default

[Default]
DeployRoot=\\WDS-SERVER\DeploymentShare$
UserID=Vogel
UserDomain=WDS-Server.tv
UserPassword=Welkom01
KeyboardLocale=en-US
SkipBDDWelcome=YES
```

Het is nu mogelijk om via het netwerk windows clients te installeeren zoals te zien is in de volgende afbeeldingen:



Beheer via SSH

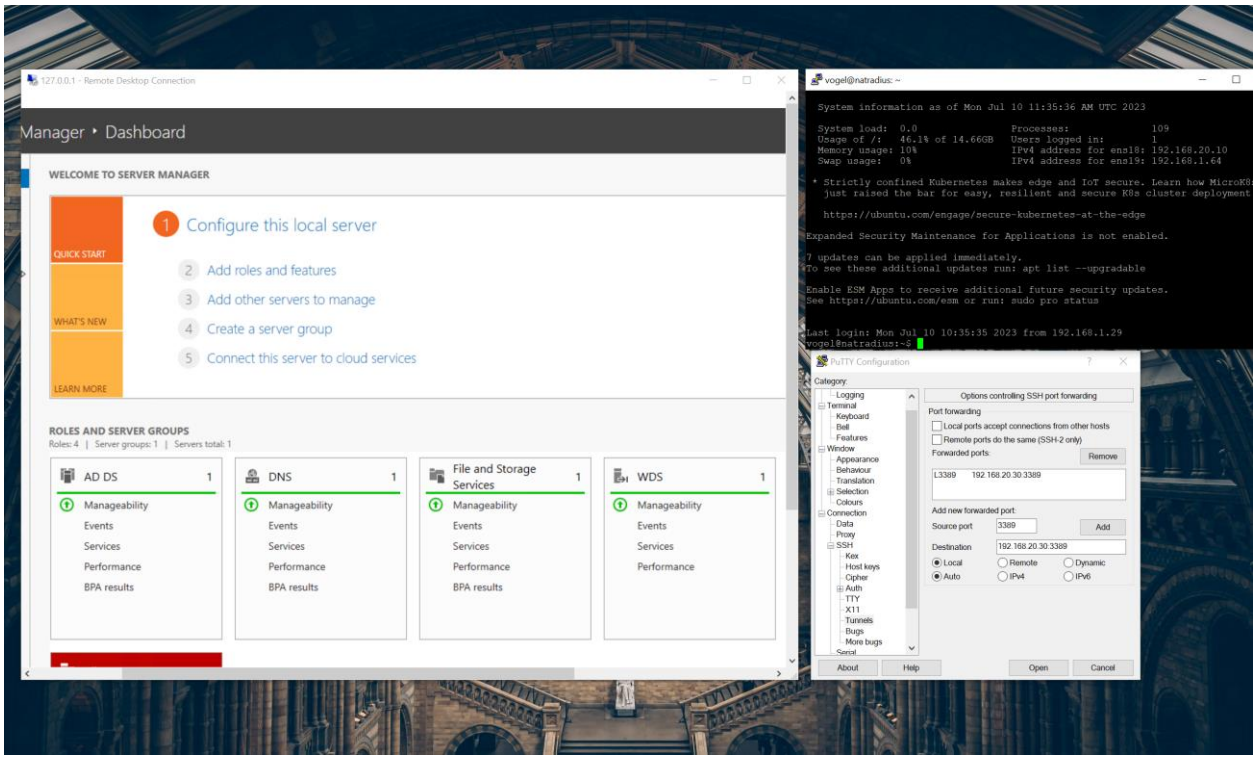
Een belangrijk aspect van het project is het mogelijk maken van extern beheer van de Windows-server via een beveiligde SSH-verbinding. Dit stelt beheerders in staat om op afstand toegang te krijgen tot de server en deze te beheren zonder dat er directe toegang tot het interne netwerk nodig is.

Om dit te realiseren, wordt er een iptables-regel toegevoegd aan de Linux NAT-router om een SSH-tunnel toe te staan. Een SSH-tunnel zorgt voor een veilige verbinding tussen een externe computer en de Windows-server, waarbij het verkeer via de SSH-verbinding wordt versleuteld.

De volgende iptables-regel wordt toegevoegd:

iptables -t nat -A PREROUTING -p tcp -d 203.0.113.10 --dport 22 -j DNAT --to 192.168.20.1:22

Nu kan de server met RDP benaderd worden door een tunnel op te bouwen met Putty.



Bronnen

Installatie NAT router:

https://linuxhint.com/configure-nat-on-ubuntu/

Radius server:

https://freeradius.org/documentation/

WDS server:

https://www.yourhowto.nl/?page_id=63

https://www.youtube.com/watch?v=0JCMzgPqtsA

https://www.yourhowto.nl/?page_id