Creating the path for mobile devices to on-premises resources

Peter van der Woude

www.wpninjas.eu
#WPNinjaS

Platinum Sponsor

PATCH MY PC

Microsoft Security

Gold Sponsor

glueckkanja gab

LIQUIT

baseVISION
SECURE & MODERN WORKPLACE

Lenovo

RECAST SOFTWARE

Snapdragon

Silver and Special Sponsors

SD:>_ SwissDev Jobs

LUZERN
DIE STADT. DER SEE. DIE BERGE.

sepago®

EPIC FUSION

SCAPPMAN

AppManagEvent.com
2022
October 7
Netherlands

dinext.

About Peter van der Woude

www.wpninjas.eu

Focus

Modern Workplace

From

Groningen, Netherlands

My Blog

https://petervanderwoude.nl

Enterprise Mobility MVP
Windows Insider MVP

Certifications

Microsoft 365 Certified: Enterprise Administrator Expert

Microsoft 365 Certified: Modern Desktop Administrator Associate

Hobbies

Family

Basketball

Gaming

Contact

pvanderwoude@hotmail.com

@pvanderwoude

/peterwoude

Agenda

Introducing Microsoft Tunnel

What is Microsoft Tunnel and how can it be used

Architecting the infrastructure of Microsoft Tunnel

What are the options for architecting the infrastructure of Microsoft Tunnel and which components are part of that infrastructure

Understanding the flow of Microsoft Tunnel

What is the flow of Microsoft Tunnel and how are the different components used in that flow

Getting started with Microsoft Tunnel

How to get started with Microsoft Tunnel (installing, configuring and distributing)

Interacting with Microsoft Tunnel

How to interact with Microsoft Tunnel

Key takeaways:

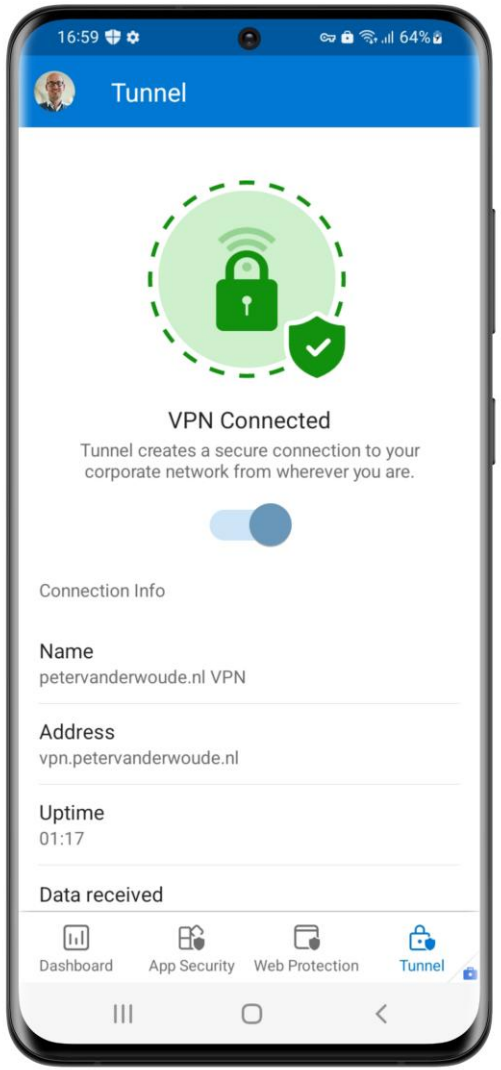
- **Learn about the path to on-premises resources for mobile devices**
- **Understand what Microsoft Tunnel is**
- **Grow some love for the sweet integration with Conditional Access**

Introducing Microsoft Tunnel

What is Microsoft Tunnel and how can it be used

Introducing Microsoft Tunnel

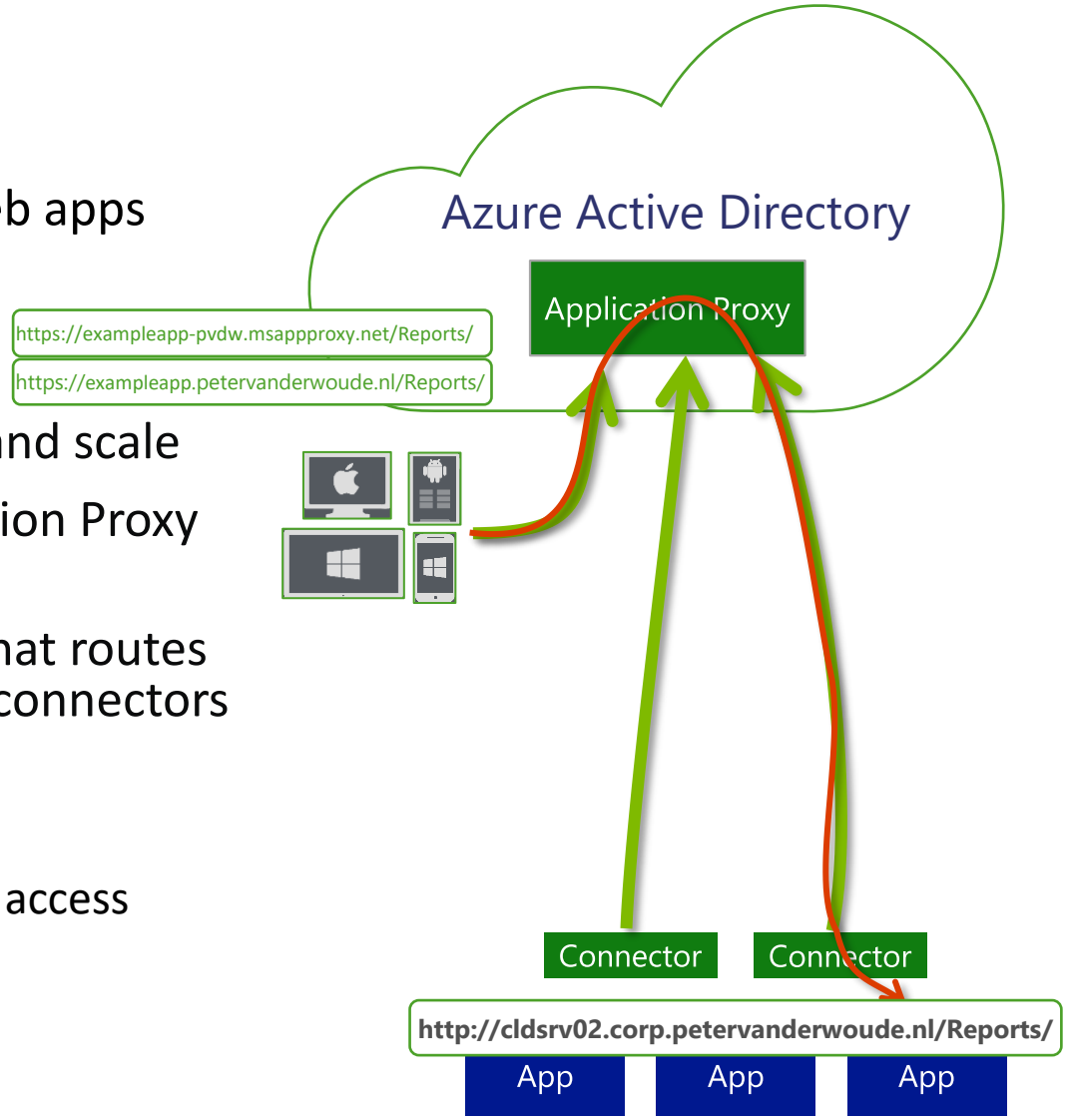
- Microsoft Tunnel Gateway is a VPN gateway solution for mobile devices
  - Supports iOS/iPadOS and Android Enterprise fully managed, corporate-owned work profile, and personally-owned work profile
- Runs on a Docker (or Podman) container on a Linux server
- Provides access to internal apps and resources
- Seamless integration with Azure AD for authentication and single sign-on experience for the VPN connection
- Access is protected with Conditional Access
- Smooth integration with Microsoft Defender for Endpoint for VPN-functionality
- Server and site configuration options available to define the setup
- Configuration can be achieved via a standard VPN profile
- Provides configuration options for per-app and device-based VPN
- Part of the existing Microsoft Intune licenses!



>> Microsoft Tunnel Deployment Guide provided by Microsoft <<

What about Azure AD Application Proxy

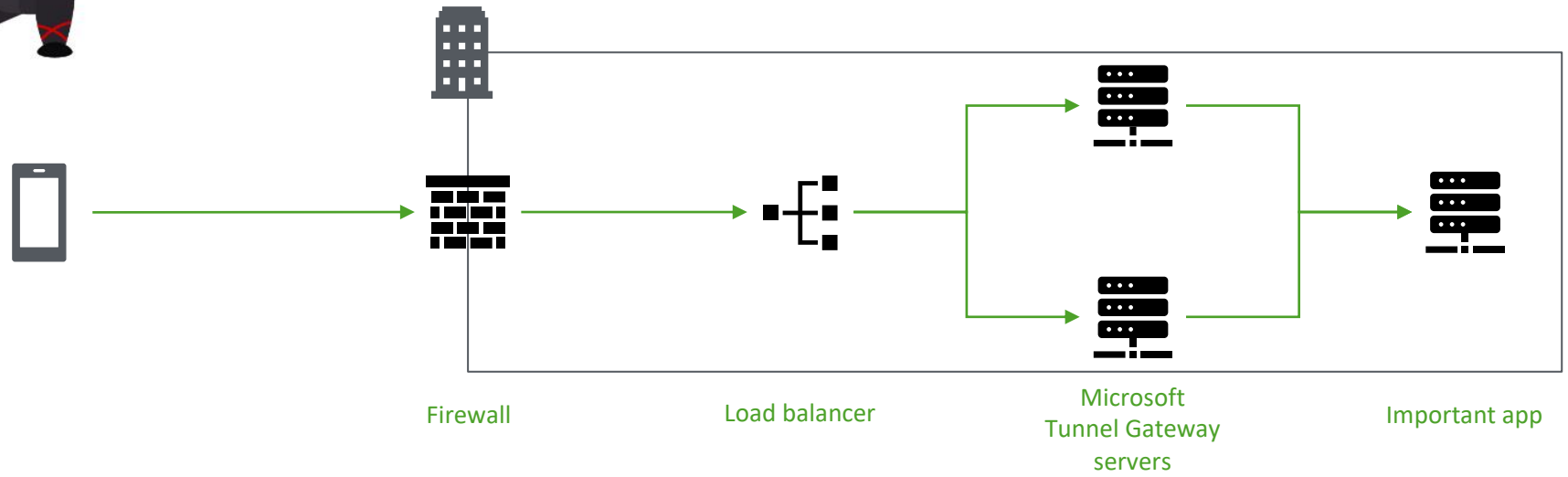
- Azure AD feature for remote access to on-premises web apps
- Application Proxy service that runs in the cloud
- Application Proxy connector that runs on-premises
- Multiple connectors can be deployed for redundancy and scale
- Application Proxy connectors auto-connect to Application Proxy service
- User connects to the Application Proxy cloud service that routes their traffic to the resources via the Application Proxy connectors
- Application Proxy can be used for:
  - Web applications that use IWA for authentication
  - Web applications that use form-based or header-based access
  - Web APIs to expose to rich applications
  - Apps hosted behind a Remote Desktop Gateway
  - Rich client apps that are integrated with MSAL
- Replaces the need for a **VPN** or reverse proxy



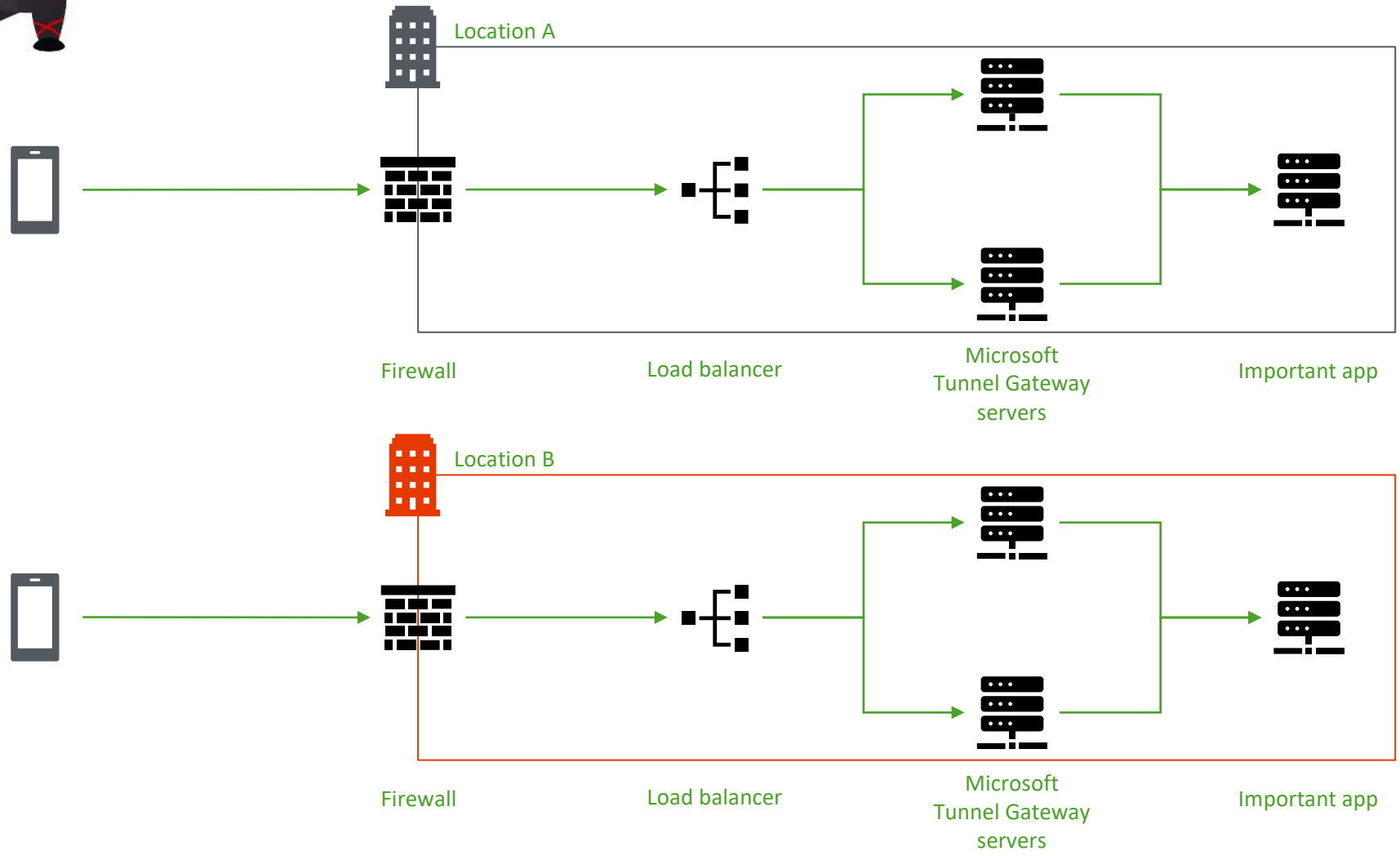
Architecting the infrastructure of Microsoft Tunnel

What are the options for architecting the infrastructure of Microsoft Tunnel and which components are part of that infrastructure

Single-site architecture



Multi-site architecture



Understanding the flow of Microsoft Tunnel

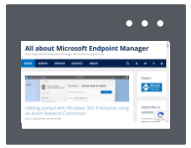
What is the flow of Microsoft Tunnel and how are the different components used in that flow

Understanding the different components

	Component	Usage
1	Microsoft Intune	The solution for managing the Tunnel Gateway and the device
2	Azure AD	The solution for authentication to the Tunnel Gateway
3	Linux server	The platform for running containers (Podman or Docker)
4	Containers	The engine for running containers of Tunnel Gateway and the management agent
5	Microsoft Tunnel	The VPN provider for access to on-premises resources
6	Management agent	The agent for applying the required configuration to the Tunnel Gateway
7	Authentication plugin	The authorization plugin for authentication with Azure AD
8	TLS certificate	The certificate for securing connections from devices to the Tunnel Gateway server
9	Firewall	The secure wall for protecting the on-premises resources
10	Public IP/FQDN	The public address for accessing the Tunnel Gateway
11	Corporate network	The location for the on-premises resources
12	Public Internet	The location for the mobile devices
13	Device	The device for connecting to the Tunnel Gateway server

Understanding the flow of Microsoft Tunnel

www.wpninjas.eu



Webpage (12)

User navigates to public resources (with split tunnel enabled)

Azure Active Directory (2)

Microsoft Intune (1)

Intune administrator configures *Server configurations* and *Sites*

Intune administrator installs Microsoft Tunnel Gateway and the authentication plugin authenticates Microsoft Tunnel Gateway with Azure AD

Intune administrator creates and deploys VPN profiles and the MDE app to devices

Device authenticates to Azure AD and Conditional Access policies are evaluated

Device (13)

User navigates to internal resources (and public resources when split tunnel disabled)

Management agents (6)

Load balancer (10)

Microsoft Tunnel Gateway (5)(8)

Authentication Plugin (7)

Containers (4)

Linux server (3)

Apps and resources

Proxy

Management agent communicates to Intune to retrieve the *Server configuration*, and to send telemetry logs to Intune

Firewall (9)

Corporate network (11)

The proxy can only use "*Break and Inspect*" on the client traffic.

Getting started with Microsoft Tunnel

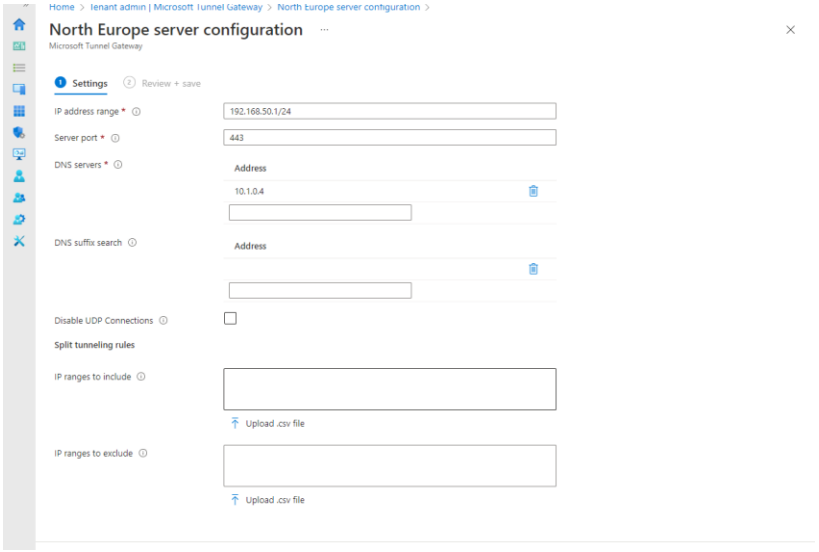
How to get started with Microsoft Tunnel (installing, configuring and distributing)

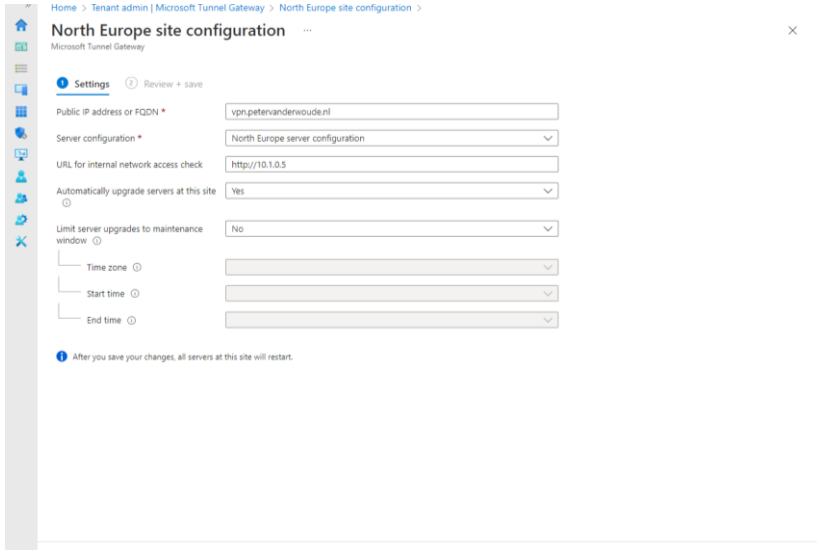
Prerequisites for Microsoft Tunnel

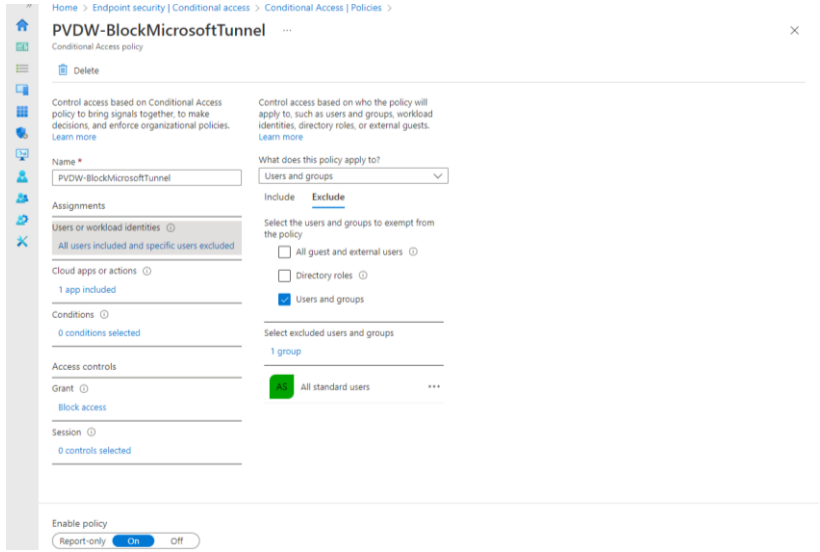
- An Azure subscription or datacenter location for hosting
- An Intune subscription (and license) for eligibility
- A Linux server that runs Docker 19.03 CE or later, or Podman 3.0
  - CentOS 7.4+ (Docker)
  - Red Hat (RHEL) 7.4+ (Docker) and Red Hat (RHEL) 8.4, 8.5 or 8.6 (Podman)
  - Ubuntu 18.04 and 20.04 (Docker)
- A TLS certificate (secure connections from device to gateway)
- Devices that run Android or iOS/iPadOS and enrolled in Intune
- Inboud TCP/UDP 443 and outbound TCP 80 and 443
- Following the documentation for guidance about sizing: Identify the prerequisites to install and use the Microsoft Tunnel VPN solution for Microsoft Intune | Microsoft Docs

Step 1: Prepare the environment

www.wpninjas.eu







Service configuration

Configure the IP range for clients, the port that the server listens to, the DNS servers for clients, the DNS suffix for clients and any split tunnel rules.

Site configuration

Configure the public IP address/FQDN of the site, the default server configuration, the network access check, the upgrade behavior and the maintenance windows for upgrades.

Conditional Access

Configure Conditional Access to make sure that the access is protected during the configuration. Use st-CA-readiness.ps1 (available via aka.ms/ms-ca-provisioning) to get started.

Step 2(a) : Install the Docker engine

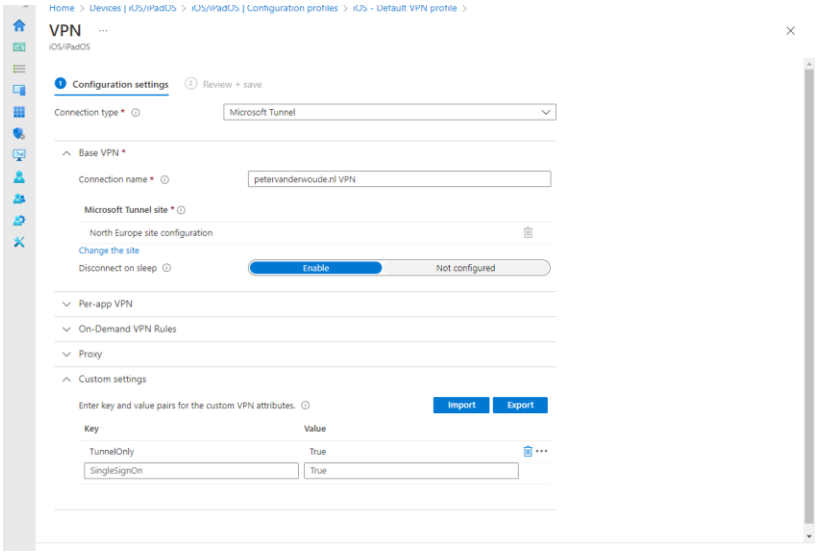

```
# Connect to the Linux VM by using SSH
ssh {yourIPorFQDN} -l {username}


# Update package index with latest version of each package and dependencies
sudo apt-get update
# Install the required packages to create a Docker repository
sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common
# Add the official Docker GPG key
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg
# Set up the Docker repository
echo "deb [arch=$(dpkg --print-architecture) signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null


# Update package index again with latest version of each package and dependencies
sudo apt-get update
# Install the latest version of Docker engine
sudo apt-get install docker-ce docker-ce-cli containerd.io
```

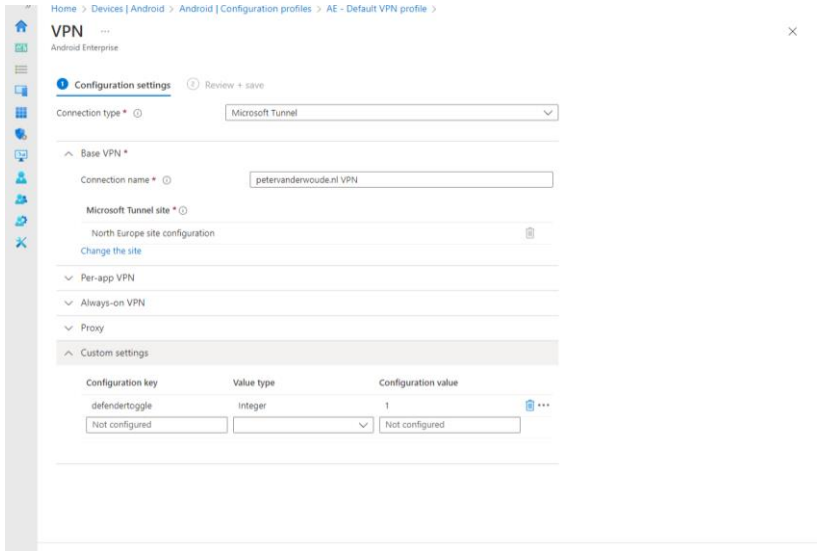
Step 2(b): Install Microsoft Tunnel Gateway


```
# Connect to the Linux VM by using SSH
ssh {yourIPorFQDN} -l {username}

# Download the Microsoft Tunnel readiness script to check the environment
# wget --output-document=mst-readiness https://aka.ms/microsofttunnelready

# Download the Microsoft Tunnel installation script
wget --output-document=mstunnel-setup https://aka.ms/microsofttunneldownload

# Provide the user with the execute permissions
sudo chmod u+x ./mstunnel-setup

# Execute the Microsoft Tunnel installation script
sudo ./mstunnel-setup

# During the execution: when prompted accept the license agreement (EULA), copy the TLS certificate and sign-in and authenticate with Intune (device login)
```

Step 3: Configure the mobile devices

www.wpninjas.eu





Configure iOS devices

Configure the Microsoft Tunnel site, the VPN behavior and the usage of the app (TunnelOnly).

Configure Android devices

Configure the Microsoft Tunnel site, the VPN behavior and the usage of the app (defendertoggle).

Device versus per-app

The differences in behavior of the configured VPN profile.

Interacting with Microsoft Tunnel

How to interact with Microsoft Tunnel

Viewing local information


```
# mst-cli - command-line tool for local interaction
# agent – property to operate on the agent component
# server – property to operate on the server component
# uninstall – property to uninstall the Microsoft Tunnel
# eula – property to show the EULA
# import_cert – property to import or update the TLS certificate
sudo mst-cli server show users

# journalctl - command-line tool to view local log files (interactive)
# mstunnel-agent – property to display agent logs
# mstunnel_monitor – property to display monitoring task logs
# ocserv - property to display server logs
# ocserv-access - property to display access logs
journalctl –t ocserv –f

# Location that contains configuration files
# /etc/mstunnel – to browse through the root directory for all configurations
cd /etc/mstunnel/
```

Reminders and summary

- Android Enterprise dedicated devices are not supported by Microsoft Tunnel
- Microsoft Defender for Endpoint app is the one-and-only client app for Microsoft Tunnel
- Any required custom configuration can be applied by using the VPN configuration profile
  - Including completely disabling the Microsoft Defender for Endpoint functionality
- Don’t forget to configure the upgrade behavior (automatic versus manual) of the servers within a site
- Don’t forget to configure an internal resource to check the internal network accessibility
- If needed customize the health status metrics to change the monitoring thresholds
- Don’t hesitate to view local logs on the Linux server (syslog format)
- Don’t forget to enable Conditional Access by creating the required service principle (via script)

Thank You