Špecializované IKT systémy Windows

Ing. Stanislav Lukac, PhD.

Organizácia predmetu

Začiatok: Prvé tri týždne mesiaca od 9:45 | 13:30

Koniec: 12:25 | 15:55

Prestávky: podla potreby

Hodnotenie: 2 testy + 2 zadania + hodnotenie aktivity

Introducing

- Ing. Stanislav LUKÁČ, PhD
- TSSK Position:
  ICT Senior Engineer
- Core Tech:
  - MS Windows Servers
  - MS Hyper-V
  - VMware vSphere
  - Cisco UCS
  - PowerShell
- Contact:
  Stanislav.lukac@t-systems.com

  +421 901 903 279

Agenda

Teória

- Úvod do predmetu
- VPN protokoly
- PKI infraštruktúra
- Vysoká dostupnosť
- Load balancing
- Sieťové úložiská dát
- PowerShell

Lab

- Inštalácia a konfigurácia VPN
- Inštalácia a konfigurácia CA
- Inštalácia a konfigurácia CLU
- Vytváranie on linner PS
- Vytváranie skriptov v PS

Téma 1

VPN

Špecializované IKT systémy Windows

Úvod do problematiky

- Protokol
- Paket
- Autentifikácia
- Autorizácia
- Šifrovanie
- ,,Enkapsulácia,, dát

PROTOKOL

Úvod do problematiky

Predstavuje postup a pravidlá komunikácie zariadení v sieti

Internetový protokol definuje spôsob výmeny dát medzi dvoma zariadeniami v sieti

Fungovanie a popis protokolu obsahuje RFC xyz

Príkladmi sú napríklad IPv4 internetový protokol alebo IPv6, UDP, FTP, HTTP, ...

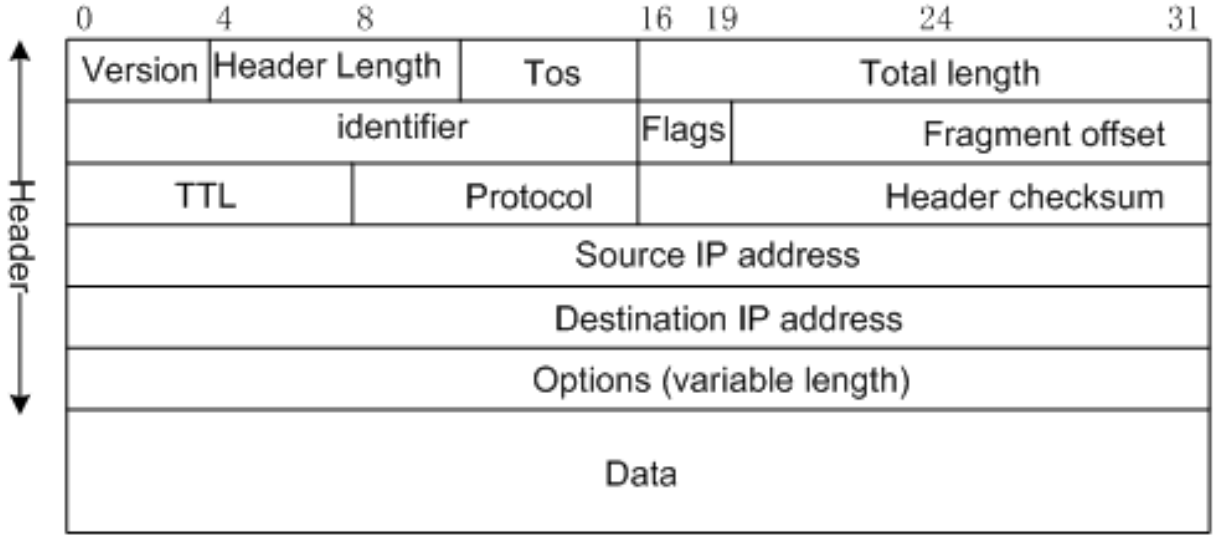
PACKET

Úvod do problematiky

Predstavuje dátovú štruktúru výmenný dát medzi dvoma alebo viacerými zariadeniami po sieti

Môže mať max 64K

Obsahuje dve časti (hlavička a dátová časť)



https://support.huawei.com/enterprise/my/doc/EDOC1000166600/dd76ea1f/ipv4-packet-format

Autentifikácia
Úvod do problematiky

Je proces overovania užívateľa alebo zariadenia voči autentifikačnej autorite s cieľom uistiť sa, že sa jedná o oprávnenú osobu alebo zariadenie

Overenie identity

https://www.entersekt.com/solutions/strong-authentication

Autorizácia

Úvod do problematiky

Je proces overovania užívateľa alebo zariadenia voči autentifikačnej autorite so zameraním sa na jeho oprávnenia pre prístup ku zdrojom

https://www.changehealthcare.com/solutions/clearance-authorization

Šifrovanie

Úvod do problematiky

Je proces zabezpečenia senzitívnych dát voči neautorizovanému prístupu tretích strán pomocou matematických operácií a algoritmov

Cieľom je ochrana dát počas ich platnosti pred neoprávnenou entitou

Šifry poznáme symetrické a asymetrické

Blokové šifry 3DES, AES, ...

Enkapsulácia dát

Úvod do problematiky

Predstavuje proces akým spôsobom sú užívateľské dáta vložené do paketu a poslané po sieti t.j. formát obsahu

- ✓Čo bude obsahom hlavičky
- ✓V akom poradí budú bloky usporiadané
- ✓Aká bude veľkosť blokov

Enkapsulácia môže prebiehať na úrovni Layer 2 vrstvy a vyššie

Encapsulating Security Payload (ESP)

ESP

Úvod do problematiky

Súčasť IPSec

Šifrovanie a autentifikácia každého paketu

Šifrovanie je použité pre data paketu (packet payload)

Autentifikácia je použitá pre hlavičku a data

Čo je VPN ?

VPN = **V**irtual **P**rivate **N**etwork

VPN = Typ počítačovej siete pre vytvorenie bezpečného pripojenia cez verejnú nechránenú sieť

VPN= emulované privátne spojenie

Načo slúži VPN ?

VPN vytvára bezpečné šifrované pripojenie počítačov s určitou mierou zabezpečenia

Pripojenie je vytvárané po verejnej sieti (Internet) tak, aby komunikácia bola bezpečná

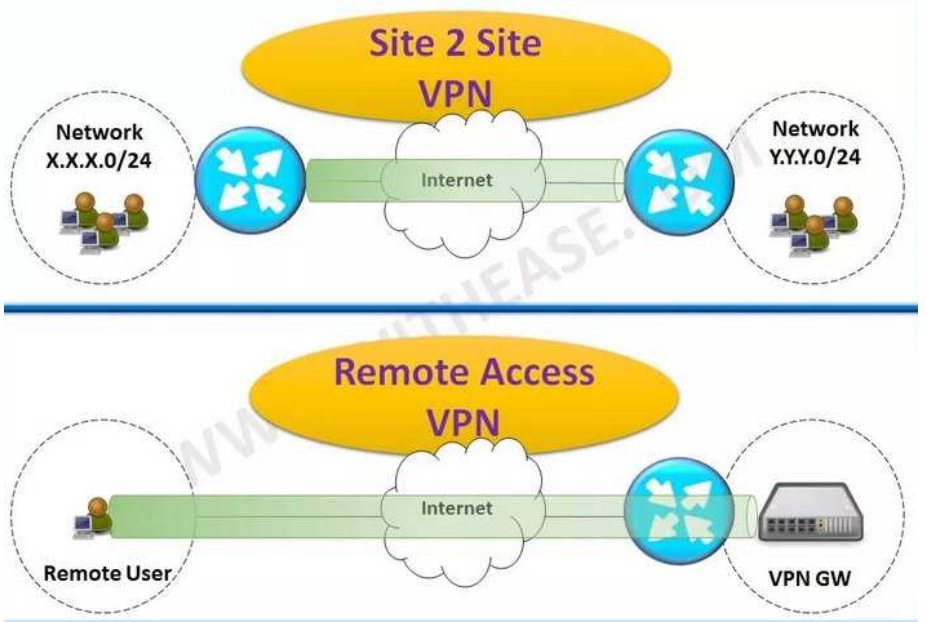
V literatúre sa často znázorňuje ako tunel

Počítače môžu byť na rozdielnych sieťach a po vytvorení VPN budú dočasne na jednej spoločnej virtuálnej sieti

Typy VPN ?

A. Remote access VPN
   - Užívateľ má prístup do firemnej siete po verejnej sieti, k jeho zdrojom (súbory, počítače, printre)

B. Site-2-Site VPN
   - Slúži na prepojenie dvoch alebo viacerých LAN bez hoľadu na ich fyzické umiestnenie



https://ipwithease.com/site-to-site-vpn-vs-remote-access-vpn/

VPN protokoly

OpenVPN

PPTP

L2TP/IPSec

SSTP

IKEv2

PPTP protokol

Point to point tunelovací protokol

Najstarší protokol

Jednoduchá konfigurácia

Kryptovanie do 128 bit

Nízka úroveň bezpečnosti

Nízke zaťaženie zariadení a rýchla odozva

Kompatibilita s Windows, Linux, MacOS, iOS, ...

SSTP protokol

Balíček bezpečnostných protokolov IPsec

Layer2 tunelovací protokol

Zložitejšia konfigurácia

Kryptovanie do 256 bit

Kryptovacie štandardy 3DES a AES

Veľmi vysoká úroveň bezpečnosti

Vyššie zaťaženie zariadení a pomalšia odozva

Kompatibilita s Windows, Linux, MacOS, iOS, ...

L2TP/IPSec protokol

Kombinácia IKEv2 a IPSEC protokolov

Uzavretý protokol vyvíjaný MS a Cisco

Najnovší protokol

Kryptovanie do 256 bit

Podpora digitálnych certifikátov

Najvyššia úroveň bezpečnosti

Vysoká rýchlosť a odozva

Kompatibilita s Windows, Linux, MacOS, iOS, ...

OpenVPN protokol

Kryptovanie do 256 bit

Podpora digitálnych CERT

Použitie OpenSSL a TLS protokolov

Najvyššia úroveň bezpečnosti

Vysoká rýchlosť a odozva

Natívna podpora akéhokoľvek OS

Obľúbenosť u poskytovateľov VPN služieb a vývojarov

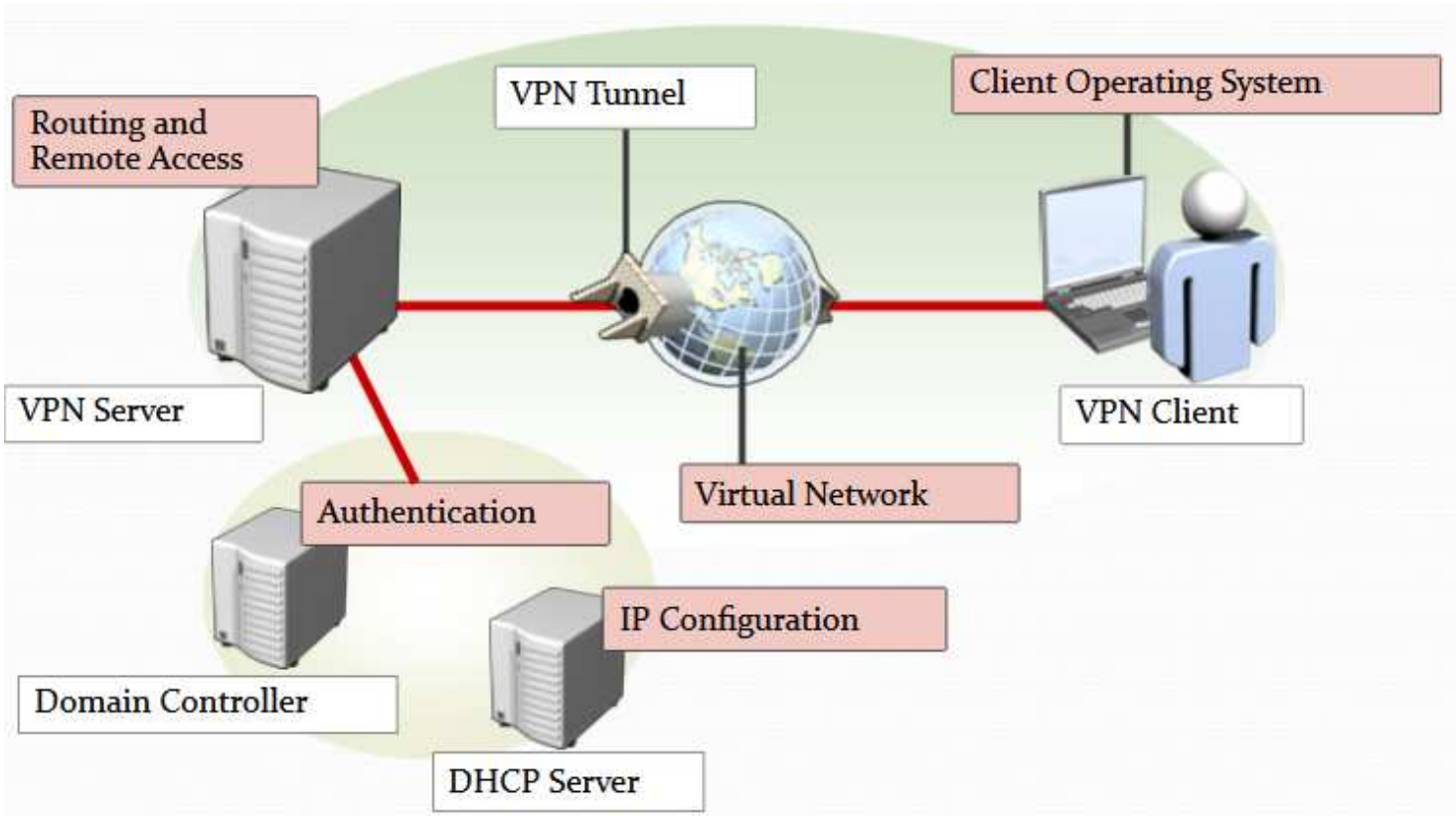
VPN autentifikačné protokoly

Protokol	Popis
PAP	Najmenej bezpečný (používa pain txt heslo)
CHAP	Heslo je kryptované ale dáta nie
MS-CHAP	Umožňuje kryptovať i dáta
MS-CHAPv2	Ponúka mutual autentifikáciu Kryptuje zvlášť prijaté a odoslané dáta
EAP-TLS	Najbezpečný protokol využívajúci CERT

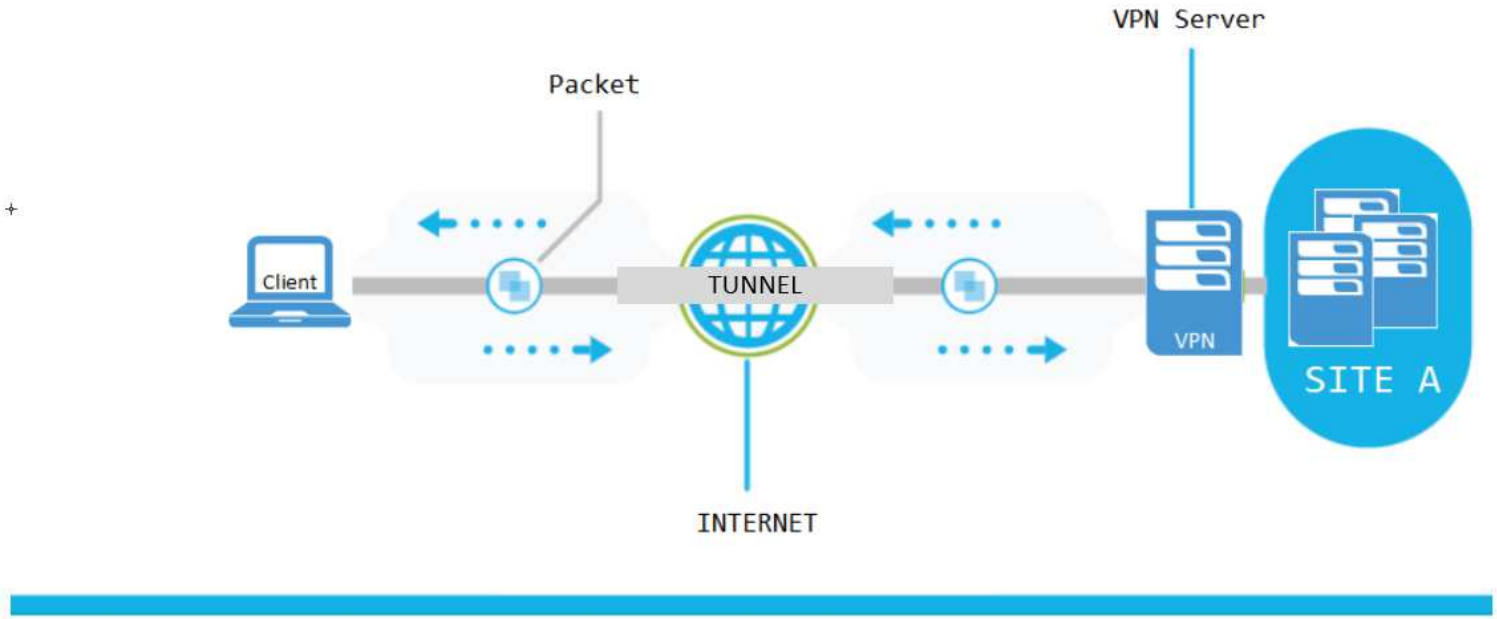
Komponenty VPN

- Autentifikačná a autorizačná autorita
- DHCP server
- VPN server
- VPN klient
- VPN tunel
- Tunelovací protokol

Komponenty VPN



Komponenty VPN



Windows VPN požiadavky

Server

- OS: Windows server 2008() a novší
- NET: 2 sieťové adaptéry (extNIC s defaultGW)

Infraštruktúra

- Autentifikačný server
- DHCP server

AlwaysON Windows VPN požiadavky

Server

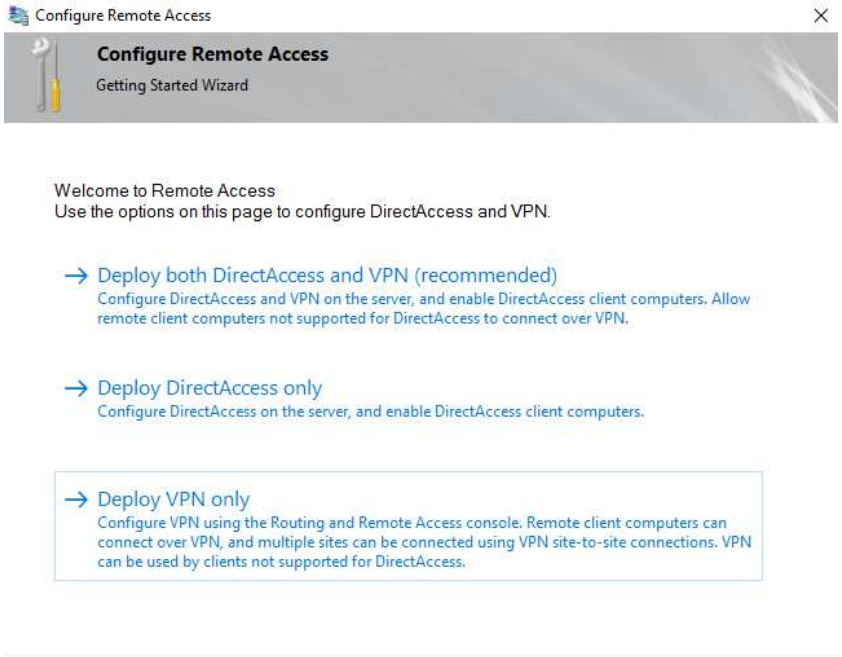
- OS: Windows server 2008() a novší
- NET: 2 sieťové adaptéry (extNIC s defaultGW)
- port 1723_TCP

Infraštruktúra

- AD DS
- CA
- DHCP server
- Radius server

Inštalácia VPN

1. **Inštalácia role REMOTE ACCESS (RAS)**
2. **Konfigurácia RAS**



Troubleshooting VPN

Error 800: VPN server nie je dostupný

Error 721: Vzdialený klient neodpovedá

Error 741: VPN server nie je dostupný

Error 800: VPN server nie je dostupný

Error 800: VPN server nie je dostupný

::PRACTICE A: Domain env

1. Inštalácia dc | Windows server 201x + 2vCPU + 3 GB RAM + 1xNIC + 50 GB HDD + 192.168.1.10/24 (IP)
2. Inštalácia domény (AD DS) na dc VM a DNS role.
3. Konfigurácia domény dual.lab
4. Inštalácia srv1 | Windows server 201x + 2vCPU + 2 GB RAM + 2xNIC + 50 GB HDD + 192.168.1.11/24 (IP0
5. Inštalácia cli | Windows 10 + 1vCPU + 2 GB RAM + 1xNIC + 50 GB HDD + 192.168.1.15/24 (IP)

::PRACTICE B: VPN server konfigurácia a test

1. Inštalácia role RAS a konfigurácia VPN
2. Test VPN z klienta CLI

Téma 2

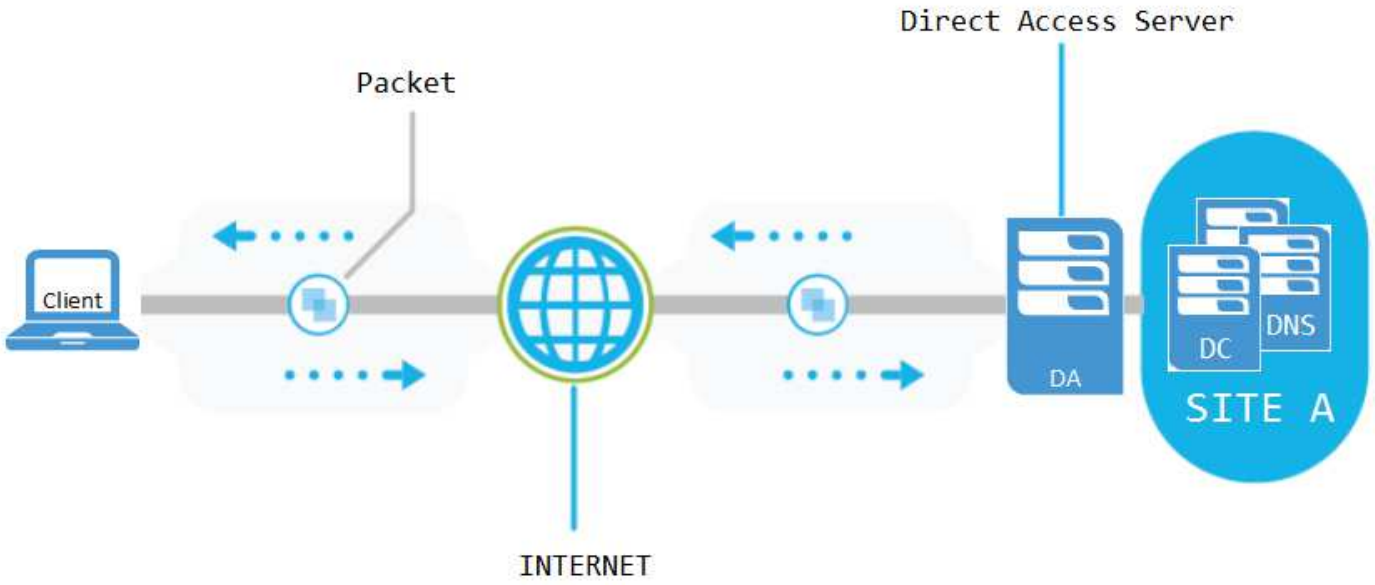
DA

Špecializované IKT systémy Windows

Čo je DAS ?

Direct Access Service

- Nová tech dostupná od windows server 2008 R2 / Win7
- Podpora IPSEC a CERT (incl IPv6)
- Permanentný AlwaysConnect klientov



DAS požiadavky

SERVER

- AD doménový level 2012 R2
- IPv6 (recommended)
- PKI (recommended)
- Klient musí byť členom rovnakej domény

KLIENT

Windows 7 a novšie

DAS inštalácia

2 možnosti inštalácie:

A. Single DA server
- FW musí byť povolený na všetkých profiloch
- Nepotrebuje PKI
- NAP nie je podporovaný
- Deployment guide

B. Single DA server s rozširujúcim nastavením
- FW musí byť povolený na všetkých profiloch
- Potrebuje PKI
- NAP je podporovaný
- Deployment guide

::PRACTICE C: Inštalácia single access DA

1. Inštalácia dc | Windows server 201x + 2vCPU + 3 GB RAM + 1xNIC + 50 GB HDD + 192.168.1.10/24 (IP)
2. Inštalácia domény (AD DS) na dc VM a DNS role.
3. Konfigurácia domény dual.lab
4. Inštalácia SRV1 | Windows server 201x + 2vCPU + 2 GB RAM + 2xNIC + 50 GB HDD + 192.168.1.11/24 (IP0
5. Inštalácia CLI | Windows 10 + 1vCPU + 2 GB RAM + 1xNIC + 50 GB HDD + 192.168.1.15/24 (IP)
6. Inštalácia a konfigurácia DA na SRV1

Ďakujem

Additional reading

https://docs.microsoft.com/sk-sk/windows-server/remote/remote-access/directaccess/single-server-advanced/deploy-a-single-directaccess-server-with-advanced-settings