Algebra
visoka škola za
primijenjeno računarstvo

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

KATEDRA ZA OPERACIJSKE SUSTAVE

Operacijski sustavi: mrežna infrastruktura i servisi

Lab 09 – VPN Network Access Protection

Zagreb, 2016.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Sadržaj

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Uvod

Tema današnje vježbe jesu **NAP** (eng. *Network Access Protection*) mehanizmi. NAP je zadužen za provjeru „zdravlja" klijenata koji se žele spojiti na domensku mrežu. Ovisno o zdravlju, NAP će dopustiti pristup mreži, potpuno izolirati klijenta ili mu dopustiti pristup samo najnužnijim resursima. Zdravlje klijenta određuje se prema nekoliko kategorija.

- **Windows vatrozid**: uključen na svim mrežnim vezama i na svim profilima.
- **Antivirusna aplikacija**: uključena i s instaliranim najnovijim definicijama.
- **Antispyware aplikacija**: isto kao i za antivirusnu aplikaciju.
- **Windows ažuriranja**: instalirana ažuriranja operacijskog sustava. Moguće je odrediti i vrstu ažuriranja koja nužno mora biti instalirana (npr. kritične sigurnosne nadogradnje).

Opišimo infrastrukturu koju želimo postići.

- **SERVERDC**: domenski kontroler domene racunarstvo.edu kojem smo instalirali uloge certifikacijskih servisa u prošloj vježbi. Njime ćemo se danas koristiti uglavnom za konfiguraciju potrebnih Group Policy objekata.
- **SERVER1**: poslužitelj na koji ćemo danas dodati RRAS ulogu i NAP mehanizme provjere zdravlja. Ujedno će služiti i kao pristupni server – RAS- na mrežu učionice.
- **CLI1**: klijentsko računalo s kojeg ćemo testirati funkcionalnost NAP mehanizama. Ovisno o postavljenim opcijama, ovo će računalo imati puni ili djelomični pristup mreži.

VPN NAP funkcionira relativno slično kao i DHCP NAP. Ideja je ista: smjestiti korisnika u izolaciju dok se ne isprave sigurnosni propusti. Ipak, VPN NAP vezan je za dodatne servise. Ponajprije moramo implementirati RRAS servis (sjetite se vježbe 4) koji će omogućiti VPN povezivost, tj. spajanje klijenata na RAS (eng. *Remote Access Server*) poslužitelj. Jednako tako, RAS poslužitelj mora biti potpisan odgovarajućim certifikatom. Kao metoda autentikacije upotrebljava se PEAP (eng. *Protected Extensible Authentication Protocol*) protokol. Mrežni je promet kriptiran, a ovaj se dio konfiguracije odrađuje preko Network Policy Servera.

U produkcijskom okruženju s implementiranim NAP-om preporučujem RADIUS autentikaciju. Drugim riječima, razdvojite uloge RAS-a i NPS-a na dva poslužitelja. Tako povećavate sigurnost jer RAS poslužitelj mora biti izložen Internetu, a NPS poslužitelj možete smjestiti u sigurniji dio mreže. Ovaj je scenarij dostupan za vježbu uz pomoć dodatne literature (na engleskom jeziku) i preko Projekta 3.

Ovime završava današnji uvod. Krenimo s vježbom.

Prije vježbe

1. Prijavite se na računalo kao **Administrator** s lozinkom **Pa$$w0rd**.
2. Kliknite na **Start**-> **Administrative Tools**-> **Hyper-V Manager**.
3. Provjerite jesu li sva virtualna računala isključena. Podsjetimo se, isključena računala kao oznaku statusa imaju **Off** ili **Saved**. Uključena računala imaju oznaku **Running**.
4. Primijenite *snapshot* **Lab8** na virtualnom računalu **KZOS-SERVERDC.**

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

5. Primijenite *snapshot* **Lab8** na virtualnom računalu **KZOS-SERVER1.**
6. Primijenite *snapshot* **Lab8** na virtualnom računalu **KZOS-CLI1.**

-----NAPOMENA-----

Današnja vježba se nastavlja na vježbu 8 – Certifikacijski servisi. Ukoliko niste odradili tu vježbu, odradite ju danas a ovu vježbu odradite kod kuće.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Pripremne radnje

Kako je opisano u uvodu, prije nego konfiguriramo NAP, moramo instalirati potrebne uloge. Instalacija se minimalno razlikuje od postupaka koje smo prošli u prethodnim vježbama.

Osnovna konfiguracija

U AD ćemo dodati dvije grupe. Jedna će poslužiti za smještaj računala koja podliježu NAP provjeri, a druga je namijenjena VPN korisnicima.

1. Prikažite **Hyper-V Manager** konzolu.
2. Pokrenite virtualno računalo **KZOS-SERVERDC**
3. Prijavite se na računalo **SERVERDC** kao **RACUNARSTVO\Administrator** s lozinkom **Pa$$w0rd**
4. Prikažite ekran **Start** i kliknite na **Active Directory Users and Computers**.
5. Prikazuje se konzola **Active Directory Users and Computers**. Unutar lijevog okna proširite domenu **racunarstvo.edu**.
6. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Racunala** i iz kontekstualnog izbornika odaberite **New**-> **Group**.
7. Prikazuje se ekran **New Object – Group**. U polje **Group name** upišite **NAP_Racunala**.
8. Unutar kategorije **Group Scope** postavite vrijednost **Domain local** i kliknite gumb **OK**.
9. Vraćate se u **Active Directory Users and Computers** konzolu. Unutar desnog okna desnim gumbom miša kliknite na grupu **NAP_Racunala** i iz kontekstualnog izbornika odaberite opciju **Properties**.
10. Prikazuje se ekran **NAP_Racunala Properties**. Kliknite na karticu **Members** i zatim kliknite gumb **Add**.
11. Prikazuje se ekran za odabir objekata. Kliknite gumb **Object Types.**
12. Prikazuje se ekran **Object Types**. Označite stavku **Computers** i kliknite gumb **OK**.
13. Vraćate se na ekran za odabir objekata. U polje **Enter the object names to select** upišite **CLI1** i kliknite gumb **OK**.
14. Vraćate se na ekran **NAP_Racunala Properties**. Kliknite gumb **OK.**
15. Vraćate se u **Active Directory Users and Computers** konzolu.

Sada ćemo izraditi grupu za korisnike:

1. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Korisnici** i iz kontekstualnog izbornika odaberite **New**-> **Group**.
2. Prikazuje se ekran **New Object – Group**. U polje **Group name** upišite **VPN_Korisnici**.
3. Unutar kategorije **Group Scope** postavite vrijednost **Domain local** i kliknite gumb **OK**.
4. Vraćate se u **Active Directory Users and Computers** konzolu. Unutar desnog okna desnim gumbom miša kliknite na grupu **VPN_Korisnici** i iz kontekstualnog izbornika odaberite opciju **Properties**.
5. Prikazuje se ekran **VPN_Korisnici Properties**. Kliknite na karticu **Members** i zatim kliknite gumb **Add**.
6. Prikazuje se ekran za odabir objekata. U polje **Enter the object names to select** upišite **`Admin1; Marko Tomić`** i kliknite gumb **OK**.
7. Vraćate se na ekran **VPN_Korisnici Properties**. Kliknite gumb **OK**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Poslužitelj SERVER1 moramo dodati u predefiniranu grupu **RAS** (eng. *Remote Access Server*) poslužitelja.

1. U lijevom oknu kliknite na organizacijsku jedinicu **Users**.
2. U desnom oknu desnim gumbom miša kliknite na grupu **RAS and IAS Servers** i iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se ekran **RAS and IAS Servers Properties**. Kliknite na karticu **Members** i zatim kliknite gumb **Add**.
4. Prikazuje se ekran za odabir objekata. Kliknite gumb **Object Types.**
5. Prikazuje se ekran **Object Types**. Označite stavku **Computers** i kliknite gumb **OK**.
6. Vraćate se na ekran za odabir objekata. U polje **Enter the object names to select** upišite **SERVER1** i kliknite gumb **OK**.
7. Vraćate se na ekran **RAS and IAS Servers Properties**. Kliknite gumb **OK**
8. Zatvorite **Active Directory Users and Computers** konzolu.

Promijenit ćemo TCP/IP postavke računala CLI1. Dotičnom računalu ćemo nekoliko puta tokom vježbe mijenjati mrežnu vezu. Ono će bit spojeno na virtualnu mrežu i na fizičku mrežu učionice, kako bi mogli testirati funkcionalnost VPN-a i VPN NAP-a. Stoga ćemo TCP/IP postavke postaviti na DHCP, ali ćemo odrediti i **zamjenske TCP/IP postavke** (eng. *Alternate Configuration*) koje će se koristiti u slučaju kad se DHCP poslužitelj ne može kontaktirati. Upravo je to slučaj sa fizičkom mrežom učionice – na njoj ne postoji DHCP poslužitelj.

1. Prikažite **Hyper-V Manager** konzolu.
2. Pokrenite virtualno računalo **KZOS-CLI1**
3. Prijavite se na računalu **CLI1** kao **RACUNARSTVO\Admin1** s lozinkom **Pa$$w0rd**
4. Prikažite ekran **Start**, upišite **ncpa.cpl** te pritisnite gumb **Enter**.
5. Prikazuje se prozor **Network Connections** s popisom mrežnih adaptera.
6. Desnim gumbom miša kliknite na adapter **LAN** i iz kontekstualnog izbornika odaberite opciju **Properties**.
7. Prikazuje se ekran **LAN Properties**. Kliknite na stavku **Internet Protocol Version 4 (TCP/IPv4)** i zatim kliknite gumb **Properties**.
8. Prikazuje se ekran sa postavkama mrežnog adaptera. Uključite opcije **Obtain an IP address automatically** i **Obtain DNS server address automatically** te kliknite gumb **OK**.
9. Vraćate se na ekran **LAN Properties**. Kliknite na stavku **Internet Protocol Version 4 (TCP/IPv4)** i zatim kliknite gumb **Properties**.
10. Prikazuje se ekran sa postavkama mrežnog adaptera. Kliknite na karticu **Alternate Configuration**.
11. Uključite opciju **User configured**.
12. Minimizirajte **Virtual Machine Connection** prozor.

Potražimo TCP/IP postavke fizičke mreže učionice:

13. Pokrenite **Command Prompt** na **fizičkom** računalu.
14. Upišite naredbu **`ipconfig /all`.**

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

15. Pronađite TCP/IP postavke fizičkog računala (IP adresa, DNS poslužitelj, mrežna maska i *default gateway*).

Postavke ćemo iskoristiti za virtualno računalo:

1. Vratite se na virtualno računalo **CLI1**.
2. Upišite TCP/IP postavke:
    a. **IP address**: IP adresa fizičkog računala uvećana za 50 na zadnjem oktetu (npr. fizičko računalo ima IP adresu 10.10.4.18 pa virtualnom računalu dodijelite adresu 10.10.4.68)
    b. **Subnet mask**: upišite vrijednost s fizičkog računala
    c. **Default gateway**: upišite vrijednost s fizičkog računala.
    d. **Preferred DNS server**: upišite vrijednost s fizičkog računala.
3. Isključite opciju **Validate settings, if changed, upon exit**.
4. Vraćate se na ekran **LAN Properties**. Kliknite gumb **Close**.
5. Ukoliko se prikaže **Networks** traka, kliknite opciju **No, don't turn on sharing or connect to devices**.
6. Zatvorite sve prikazane prozore na računalu **CLI1**.

Isključimo Windows Firewall:

1. Prikažite ekran **Start** i upišite **`cmd`**
2. Desnim gumbom miša kliknite na **Command Prompt** te iz trake na dnu ekrana kliknite gumb **Run as administrator**.
3. Prikazuje se **UAC** prozor. Kliknite gumb **Yes**.
4. Prikazuje se **Command Prompt** prozor.
5. Upišite naredbu **`netsh advfirewall set allprofiles state off`**
6. Naredba mora ispisati status **OK**.
7. Ne zatvarajte **Command Prompt**!

Provjerimo funkcionira li pristup fizičkoj mreži učionice:

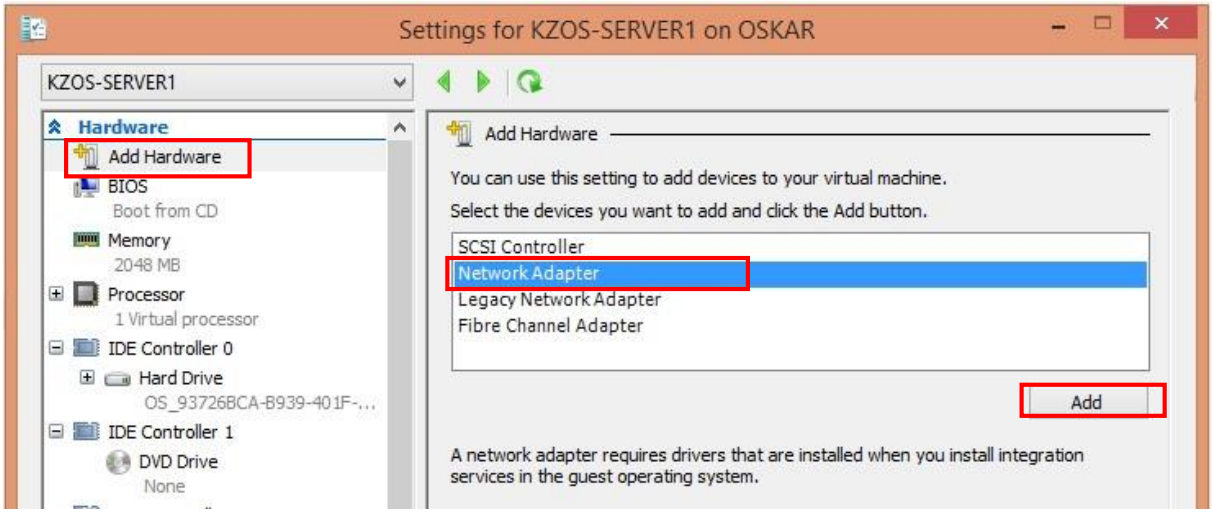
1. Na izborniku **Virtual Machine Connection** prozora kliknite **File-> Settings**.
2. Prikazuje se ekran **Settings for KZOS-CLI1**.
1. U lijevom oknu kliknite na stavku **Network Adapter**.
2. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Virtual Network** ili **External Network** (ovisi kako je konfiguriran naziv eksterne mreže na računalu na kojem radite; ako niste sigurni, pitajte asistenta).
3. Kliknite gumb **OK**.
4. Prikažite virtualno računalo **CLI1**.
5. Prikažite **Command Prompt**.
6. Upišite naredbu **`ping 8.8.8.8`**
7. Naredba mora vratiti odgovor.
8. Minimizirajte **Virtual Machine Connection** prozor.

Vježbu nastavljamo s konfiguracijom računala SERVER1.

Konfiguracija Hyper-V adaptera

Računalu SERVER1 dodajemo novi mrežni adapter. Njime ćemo se koristiti za pristup fizičkoj mreži učionice iz virtualne mreže, kao što smo radili u vježbi 4.

1. Prikažite **Hyper-V Manager** konzolu.
2. Desnim gumbom miša kliknite na računalo **KZOS-SERVER1** i iz kontekstualnog izbornika odaberite opciju **Settings**.
3. Prikazuje se ekran **Settings for KZOS-SERVER1**.
4. Iz lijevog okna kliknite na opciju **Add Hardware**, a iz pripadajućeg desnog okna odaberite opciju **Network Adapter** te kliknite gumb **Add**, kao što prikazuje sljedeća slika.



Slika 1. Dodavanje mrežnog adaptera

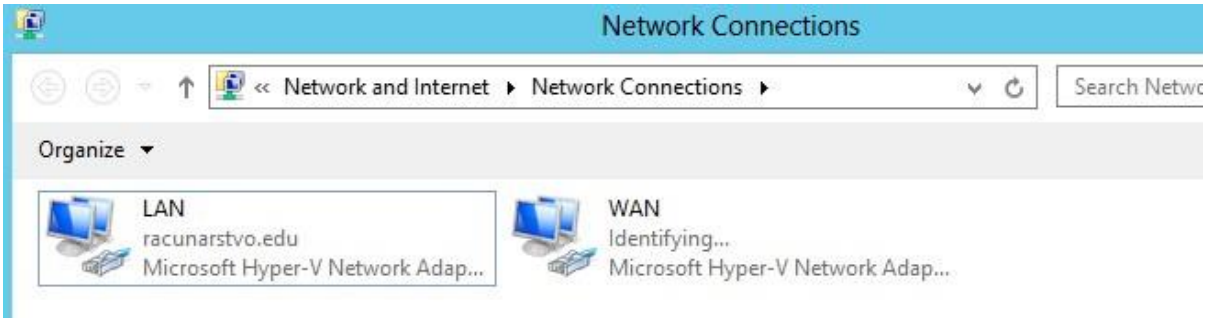
5. Novi je mrežni adapter dodan i označen. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Virtual Network** ili **External Network** (ovisi kako je konfiguriran naziv eksterne mreže na računalu na kojem radite; ako niste sigurni, pitajte asistenta).
6. Kliknite gumb **OK** i pokrenite računalo **SERVER1**.

Konfiguracija mrežnih postavki

Mrežni adapter postavljen je na DHCP postavke i inicijalno će dobiti APIPA konfiguraciju jer mreža učionice ne rabi DHCP. Stoga postavimo statičke TCP/IP postavke.

1. Prijavite se na računalo **SERVER1** kao **RACUNARSTVO\Administrator** s lozinkom **Pa$$w0rd**.
2. Prikažite ekran **Start** , upišite **`ncpa.cpl`** i pritisnite tipku Enter.
3. Prikazuje se **Network Connections** prozor s popisom mrežnih adaptera.
4. Desnim gumbom miša kliknite na **Ethernet** adapter i iz kontekstualnog izbornika odaberite opciju **Rename**.
5. Upišite **WAN** kao novo ime mrežnog adaptera i potvrdite tipkom **Enter**. Provjerite izgleda li popis mrežnih adaptera kao na sljedećoj slici.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 2. Adapteri računala SERVER1

6. Desnim gumbom miša kliknite na **WAN** adapter i iz kontekstualnog izbornika odaberite opciju **Properties.**
7. Prikazuje se ekran **WAN Properties**. Kliknite na stavku **Internet Protocol Version 4 (TCP/IPv4)** i zatim kliknite gumb **Properties**.
8. Označite opciju **Use the following IP address**
9. Upišite TCP/IP postavke:
    a. **IP address**: IP adresa fizičkog računala uvećana za 100 na zadnjem oktetu (npr. fizičko računalo ima IP adresu 10.10.4.18 pa virtualnom računalu dodijelite adresu 10.10.4.118)
    b. **Subnet mask**: upišite vrijednost s fizičkog računala
    c. **Default gateway**: upišite vrijednost s fizičkog računala.
10. Označite opciju **Use the following DNS server addresses**.
11. U polje **Preferred DNS server** upišite vrijednost s fizičkog računala.
12. Kliknite gumb **OK**.
13. Vraćate se na ekran **WAN Properties**. Kliknite gumb **OK**.
14. Zatvorite **Network Connections** prozor.

Provjerimo mogu li oba virtualna računala komunicirati putem fizičke mreže.

1. Prikažite ekran **Start** i upišite **`cmd`**
2. Desnim gumbom miša kliknite na **Command Prompt** te iz trake na dnu ekrana kliknite gumb **Run as administrator**.
3. Prikazuje se **Command Prompt** prozor.
4. Upišite naredbu **`netsh advfirewall set allprofiles state off`**
5. Naredba mora ispisati status **OK**.
6. Pomoću naredbe **`ping`** testirajte povezivost sa svojim virtualnim računalom **CLI1**.
7. Naredba mora vratiti odgovor.
8. Minimizirajte **Virtual Machine Connection** prozor.
9. Prebacite se na računalo **CLI1**.
10. Pomoću naredbe **`ping`** testirajte povezivost sa svojim virtualnim računalom **SERVER1**.
11. Naredba mora vratiti odgovor.

Računalo CLI1 ćemo opet spojiti na virtualnu mrežu:

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

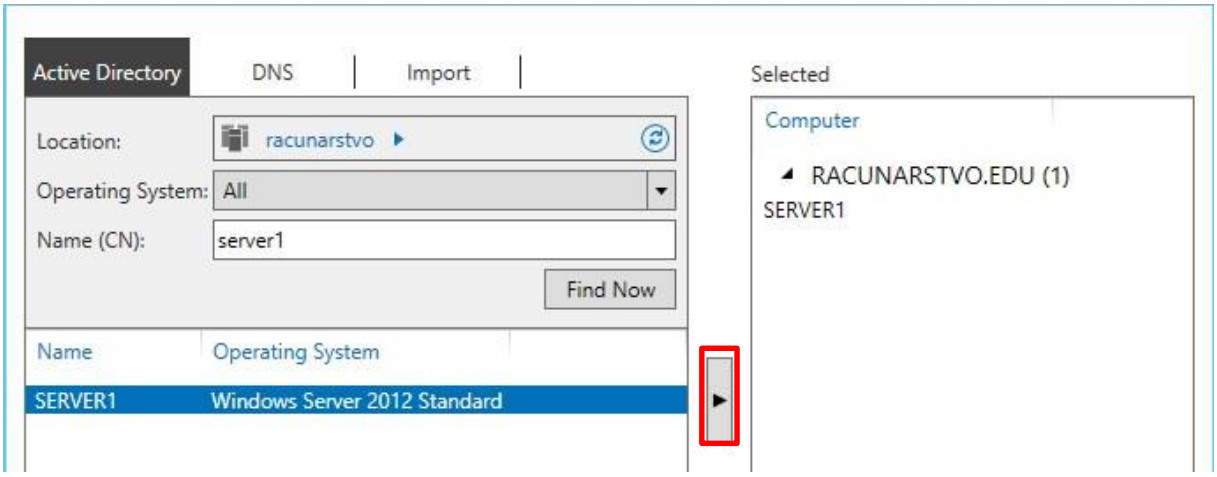
1. Na izborniku **Virtual Machine Connection** prozora kliknite **File-> Settings**.
2. Prikazuje se ekran **Settings for KZOS-CLI1**.
3. U lijevom oknu kliknite na stavku **Network Adapter**.
4. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Private 1** i kliknite gumb **OK**.
5. Prikažite **Command Prompt**.
6. Upišite naredbu **`ping SERVERDC`**
7. Naredba mora vratiti odgovor.
8. Zatvorite sve prikazane prozore na računalu **CLI1**.

Nastavljamo vježbu sa instalacijom uloga (eng. *Roles*).

Instalacija i konfiguracija uloga

Sada možemo instalirati sve potrebne uloge na računalu SERVER1. Nakon što smo omogućili pristup fizičkoj mreži učionice, instaliramo RRAS ulogu na računalu SERVER1. Ovu cjelinu vježbe ćemo iskoristiti i za demonstraciju udaljene instalacije uloga putem Server Manager konzole. Računalo SERVER1 moramo dodati na popis poslužitelja.

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite ekran **Start** i kliknite na **Server Manager**.
3. Prikazuje se **Server Manager** konzola. Kliknite na izbornik **Manage-> Add Servers**.
4. Prikazuje se ekran **Add Servers**. Kliknite na karticu **Active Directory**.
5. U polje **Name (CN)** upišite **SERVER1** i kliknite gumb **Find Now**.
6. Pretraga mora prikazati računalo **SERVER1**. Označite ga i dodajte pomoću gumba sa strelicom na popis poslužitelja (crveni okvir na donjoj slici).
7. Usporedite izgled svog ekrana s onime na donjoj slici.



Slika 3 Uređivanje popisa poslužitelja

8. Kliknite gumb **OK**. Vraćate se u **Server Manager** konzolu.

SERVER1 je dodan na popis poslužitelja. Instalirajmo potrebne uloge:

1. Unutar lijevog okna kliknite na stavku **All Servers**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

2. Unutar desnog okna desnim gumbom miša kliknite na računalo **SERVER1** i iz kontekstualnog izbornika odaberite opciju **Add Roles And Features**.
3. Prikazuje se ekran **Before you begin**. Kliknite gumb **Next**.
4. Prikazuje se ekran **Select installation type**. Ostavite predefinirane opcije i kliknite gumb **Next.**
5. Prikazuje se ekran **Select destination server**. Ostavite predefinirane opcije i kliknite gumb **Next.**
6. Prikazuje se ekran **Select server roles**. Označite stavke **Remote Access** i **Network Policy and Access Services**.
7. Prikazuje se ekran s informacijama o dodatnim komponentama. Kliknite gumb **Add Features**.
8. Vraćate se na ekran **Select server roles**. Kliknite gumb **Next**.
9. Prikazuje se ekran **Select features**. Kliknite gumb **Next**.
10. Prikazuje se ekran **Remote Access**. Kliknite gumb **Next**.
11. Prikazuje se ekran **Select role services**. Označite obje opcije i kliknite gumb **Next**.
12. Prikazuje se ekran **Web Server Role (IIS)**. Kliknite gumb **Next**.
13. Prikazuje se ekran **Select role services**. Ostavite predefinirane opcije i kliknite gumb **Next**.
14. Prikazuje se ekran **Network Policy and Access Services**. Kliknite gumb **Next**.
15. Prikazuje se ekran **Select role services**. Ostavite predefinirane opcije i kliknite gumb **Next**.
16. Prikazuje se ekran **Confirm installation selections**. Kliknite gumb **Install** i pričekajte da se završi instalacija uloga.
17. Kliknite gumb **Close**. Vraćate se u **Server Manager** konzolu.

Računalo SERVER1 moramo ponovno pokrenuti kako bi se završila instalacija uloga.

1. U desnom oknu desnim gumbom miša kliknite na računalo **SERVER1** i iz kontekstualnog izbornika odaberite opciju **Restart Server**.
2. Prikazuje se **Server Manager** prozor s potvrdom ponovnog pokretanja računala. Kliknite gumb **OK**.
3. Zatvorite sve prikazane prozore na računalu **SERVERDC**.

-----NAPOMENA-----

Administriranje uloga na udaljenom poslužitelju nije moguće direktno kroz Server Manager konzolu. Za tu radnju bi se poslužili, primjerice, Remote Desktop aplikacijom ili PowerShell konzolom.

U sljedećih nekoliko cjelina ćemo osigurati funkcionalnost RAS servisa.

Konfiguracija RRAS uloge

RRAS servisi su nakon instalacije uloge predefinirano isključeni. Potrebno ih je konfigurirati.

1. Prebacite se na računalo **SERVER1**.
2. Prijavite se na računalo **SERVER1** kao **RACUNARSTVO\Administrator** s lozinkom **Pa$$w0rd**
3. Prikažite ekran **Start** i kliknite na **Routing and Remote Access**.

4. Prikazuje se **Routing and Remote Access** konzola. Uočite da je računalo **SERVER1** unutar lijevog okna s crvenom strelicom. Ona označuje da je server isključen (u kontekstu RRAS uloge).
5. Unutar lijevog okna desnim gumbom miša kliknite na **SERVER1 (local)** i iz kontekstualnog izbornika odaberite opciju **Configure and Enable Routing and Remote Access**.
6. Prikazuje se čarobnjak za konfiguraciju. Kliknite gumb **Next**.
7. Prikazuje se ekran **Configuration**. Označite opciju **Custom configuration** i kliknite gumb **Next**.
8. Prikazuje se ekran **Custom Configuration**. Označite opcije:
    a. VPN access
    b. NAT
    c. LAN routing.
9. Kliknite gumb **Next**.
10. Prikazuje se ekran sa sažetkom odabranih opcija. Kliknite gumb **Finish**.
11. Prikazuje se poruka s informacijom o mogućem konfliktu s NPS servisom. Kliknite gumb **OK**.
12. Prikazuje se poruka o uspješnoj konfiguraciji RRAS-a. Kliknite gumb **Start service**.
13. Pričekajte pokretanje RRAS servisa. Uočite da je ikona računala SERVER1 u lijevom oknu sada sa zelenom strelicom.
14. Ne zatvarajte **Routing and Remote Access** konzolu!

Servis je uključen. Dodajmo mu NAT mogućnost.

Konfiguracija NAT mehanizma

NAT mehanizam koristi se za translaciju privatnih u javnu IP adresu i obratno. Uključujemo ga na IPv4 protokolu:

1. Unutar lijevog okna proširite mape **SERVER1(local)-> IPv4**.
2. Unutar lijevog okna desnim gumbom miša kliknite na stavku **NAT** i iz kontekstualnog izbornika odaberite opciju **New Interface**.
3. Prikazuje se ekran **New interface for IPNAT**. Označite stavku **WAN** i kliknite gumb **OK**.
4. Prikazuje se ekran **Network Address Translation Properties**. Odaberite opciju **Public interface connected to the Internet**.
5. Označite opciju **Enable NAT on this interface** i kliknite gumb **OK**.
6. Ne zatvarajte **Routing and Remote Access** konzolu!

Testiranje NAT-a

Provjerimo funkcionira li NAT najjednostavnijim mogućim testom: pristup web-stranici.

1. Prebacite se na računalo **SERVERDC**.
1. Prikažite ekran **Start**, upišite **cmd** i pritisnite tipku **Enter**.
2. Prikazuje se prozor **Command Prompt**.
3. Upišite naredbu **`ping 8.8.8.8`**
4. Naredba mora vratiti odgovor s adrese 8.8.8.8 (Googleov javni DNS server).
5. Upišite naredbu **`exit`**
6. Pokrenite **Internet Explorer** i posjetite **www.microsoft.com**
7. Stranica se mora prikazati.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

8. Zatvorite **Internet Explorer**.
9. Prebacite se na računalo **SERVER1**
10. Provjerite je li označena NAT mapa iz lijevog okna **Routing and Remote Access** konzole.
11. Osvježite prikaz ekrana pritiskom na tipku **F5**.
12. Desnim gumbom miša kliknite na **WAN** opciju i iz kontekstualnog izbornika odaberite opciju **Show Mappings**.
13. U novom se prozoru prikazuje tablica mapiranja lokalnih na javne IP adrese, kao na sljedećoj slici.

SERVER1 - Network Address Translation Session Mapping Table

Protocol	Direction	Private address	Private port	Public Address	Public Port	Remote Address	Rem
UDP	Outbound	10.10.10.1	57.292	10.10.0.242	62.507	213.199.180.53	53
UDP	Outbound	10.10.10.1	56.695	10.10.0.242	62.508	192.48.79.30	53
UDP	Outbound	10.10.10.1	58.330	10.10.0.242	62.509	70.37.135.11	53
UDP	Outbound	10.10.10.1	57.634	10.10.0.242	62.512	213.199.180.53	53
UDP	Outbound	10.10.10.1	58.516	10.10.0.242	62.513	70.37.135.14	53
UDP	Outbound	10.10.10.1	57.079	10.10.0.242	62.516	213.199.180.53	53
UDP	Outbound	10.10.10.1	58.607	10.10.0.242	62.519	192.12.94.30	53
UDP	Outbound	10.10.10.1	58.016	10.10.0.242	62.520	213.199.180.53	53
UDP	Outbound	10.10.10.1	56.603	10.10.0.242	62.521	192.54.112.30	53
UDP	Outbound	10.10.10.1	58.362	10.10.0.242	62.522	213.199.180.53	53
UDP	Outbound	10.10.10.1	57.294	10.10.0.242	62.523	173.245.58.141	53
UDP	Outbound	10.10.10.1	56.879	10.10.0.242	62.526	173.245.59.112	53
UDP	Outbound	10.10.10.1	56.787	10.10.0.242	62.533	208.84.2.53	53
UDP	Outbound	10.10.10.1	57.133	10.10.0.242	62.534	96.7.49.129	53

Slika 4. NAT tablica

-----NAPOMENA-----

Vrijednosti u stupcu Public Address razlikovat će se od studenta do studenta. Public Address jest IP adresa virtualnog računala na učioničkoj mreži. Vrijednost Private Address svim će studentima biti ista jer označuje lokalnu IP adresu domenskog kontrolera s kojeg ste pristupili adresi www.microsoft.com.

14. Zatvorite prozor s tablicom mapiranja.
15. Zatvorite **Routing and Remote Access** konzolu.

Potvrdili smo funkcionalnost NAT mehanizma. Prije konfiguracije VPN pristupa provjerimo stanje certifikacijskog servisa kojeg smo naslijedili iz osme vježbe.

Oporavak certifikacijskog servisa

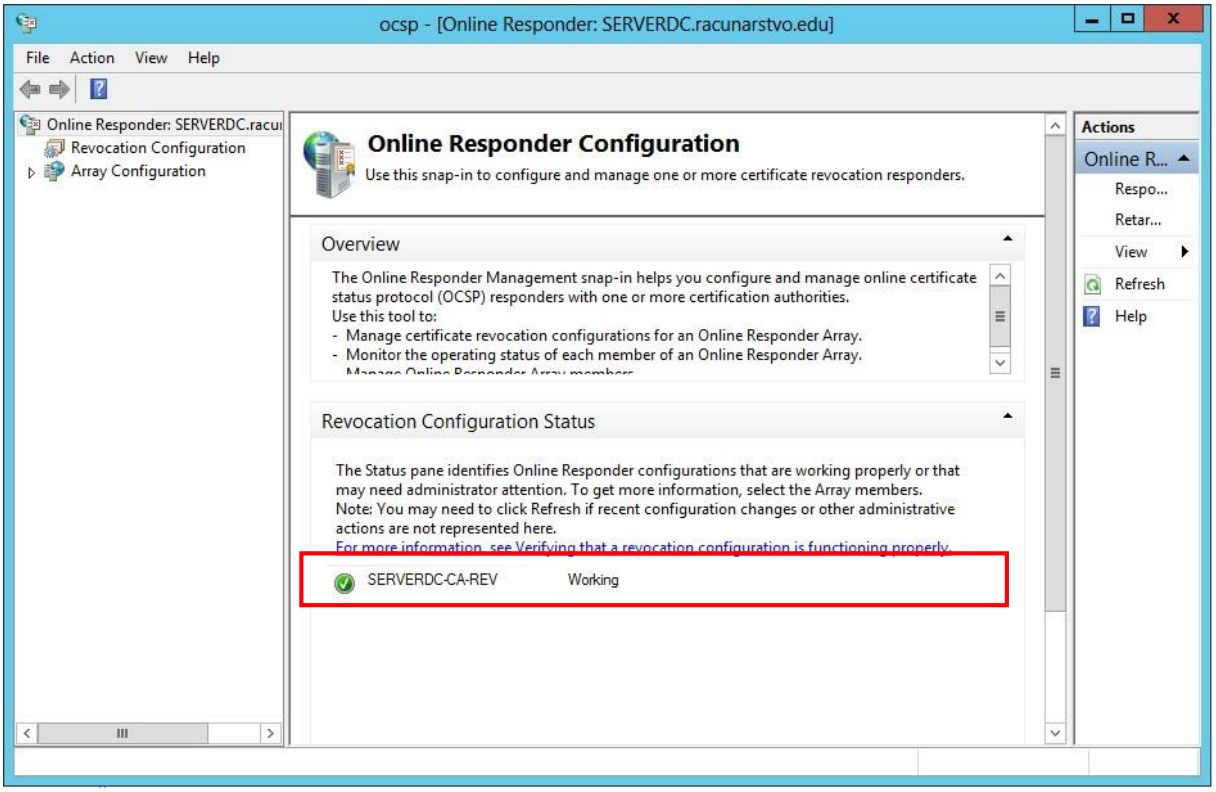
Za VPN NAP potrebni su certifikacijski servisi koje smo implementirali u 8. vježbi. Provjerimo stanje certifikacijskog servisa, s obzirom na to da je poslužitelj bio isključen dulje vrijeme (od zadnjeg snapshota).

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite ekran **Start** i kliknite na **Online Responder Management**.
3. Prikazuje se **Online Responder** konzola. Provjerite status konfiguracije za opoziv certifikata.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

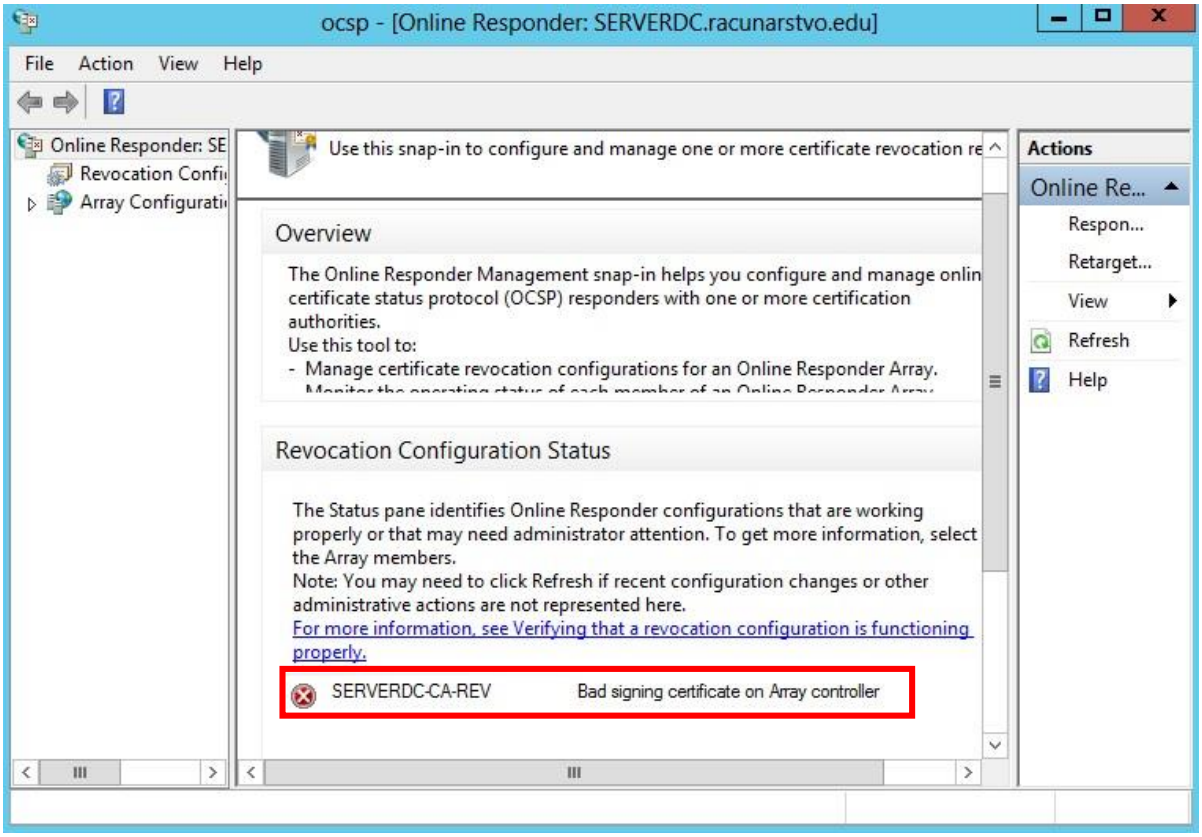
a. Ako je status ispravan, kao na **Slika 5. Ispravna konfiguracija za opoziv certifikata**), prijeđite na cjelinu **Definiranje predloška za RAS poslužitelj**. Eventualno pročitajte napomenu na kraju ove cjeline kako biste se upoznali s jednom greškom certifikacijskih servisa.

b. Ako je status neispravan, kao na **Slika 6. Neispravna konfiguracija za opoziv certifikata**), nastavite s postupkom za popravak. Objašnjenje kvara nalazi se na kraju ove cjeline.



Slika 5. Ispravna konfiguracija za opoziv certifikata

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 6. Neispravna konfiguracija za opoziv certifikata

4. Minimizirajte **Online Responder** konzolu.
5. Prikažite ekran **Start** i upišite **cmd**
6. Desnim gumbom miša kliknite na **Command Prompt** te iz trake na dnu ekrana kliknite gumb **Run as administrator**.
7. Prikazuje se **Command Prompt** prozor.
8. Upišite naredbu **`certutil -setreg ca\UseDefinedCACertInRequest 1`**
9. Upišite naredbu **`services.msc`**
10. Prikazuje se **Services** konzola. Unutar desnog okna desnim gumbom miša kliknite na servis **Active Directory Certificate Services** i iz kontekstualnog izbornika odaberite opciju **Restart**.
11. Pričekajte ponovno pokretanje certifikacijskog servisa i zatim zatvorite **Services** konzolu.
12. Prikažite **Online Responder** konzolu.
13. Unutar lijevog okna kliknite na opciju **Revocation Configuration**.
14. Unutar desnog okna desnim gumbom miša kliknite na **SERVERDC-CA-REV** i iz kontekstualnog izbornika odaberite opciju **Edit Properties**.
15. Prikazuje se **Properties for Revocation Configuration** prozor. Kliknite na karticu **Signing**.
16. Označite opciju **Use any valid OCSP signing certificate** i kliknite gumb **OK**.
17. Minimizirajte **Online Responder** konzolu.
18. Prikažite **Online Responder** konzolu.
19. Osvježite prikaz ekrana tipkom **F5**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

20. Provjerite je li status konfiguracije za opoziv sada **Working**, kao na Slika 5. Ispravna konfiguracija za opoziv certifikata.
21. Zatvorite **Online Responder** konzolu.

-----NAPOMENA-----

Prethodni je postupak oporavio certifikacijske servise. Do zastoja je došlo na komponenti *Online Responder*, koja je, podsjetimo se, zadužena za objavu liste opozvanih certifikata. Pobliže objasnimo grešku: *Online Responder* i sam mora biti potpisan odgovarajućim certifikatom. Mi smo ga u osmoj vježbi izdali na osnovi predloška **OCSP Response Signing**. Taj predložak ima predefinirano vrijeme ispravnosti izdanih certifikata od samo dva tjedna, a moguće ih je obnoviti u samo dva dana. Budući da su virtualna računala bila isključena dulje od tog vremena, *Online Responder* nije mogao obnoviti svoj certifikat i dobar je dio certifikacijske infrastrukture stao. Primjerice, novi klijent ne bi dobio certifikat iako smo u prošloj vježbi postavili automatsko izdavanje certifikata (engl. *Autoenrollment*). Rješenje problema je očito: obnoviti certifikat. Ipak, zahtjev za obnavljanjem certifikata nema tko „odraditi“ jer nam infrastruktura ne funkcionira. Stoga smo s pomoću naredbe ***certutil -setreg ca\UseDefinedCACertInRequest 1*** forsirali izdavanje OCSP certifikata na osnovi bilo kojeg certifikata (naravno, pod našim CA-om), tj. efektivno smo prevarili zadano vrijeme od 2 dana za obnovu. Uzevši u obzir sve navedeno, moram još jednom naglasiti važnost pozorne implementacije certifikacijskog servisa. Smjestite ga na redundantni poslužitelj čiji rad zatim stalno nadgledajte.

Nakon što smo oporavili certifikacijski servis, možemo definirati predložak za RAS poslužitelje.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

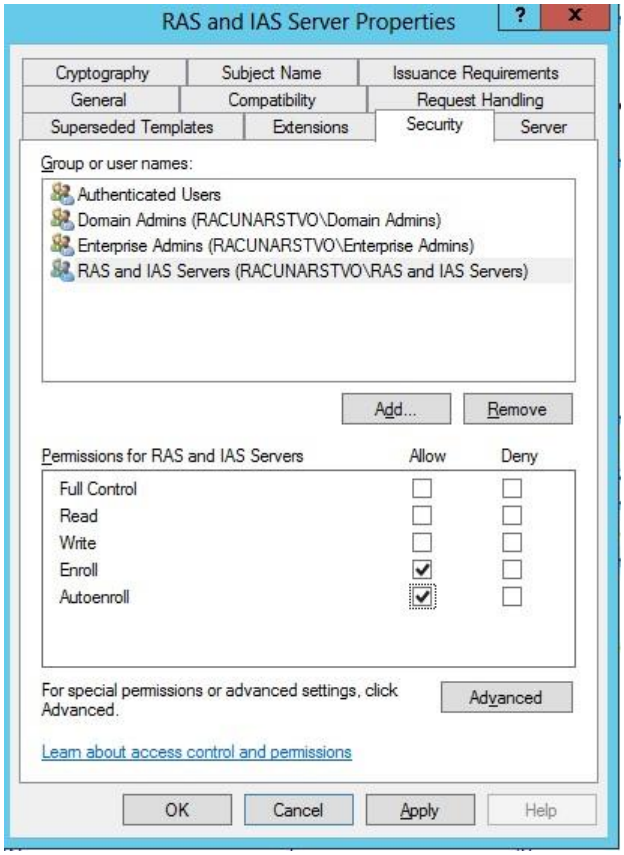
Konfiguracija VPN pristupa

Prvo ćemo konfigurirati osnovni, ne-NAP VPN pristup. Kad uspostavimo funkcionalni VPN možemo ga nadograditi NAP-om. Postupak je vrlo sličan onome iz četvrte vježbe, s izuzetkom što ćemo koristiti sigurniju metodu autentikacije baziranu na certifikatima.

Definiranje predloška za RAS poslužitelj

Računalo **SERVER1** je **RAS** (eng. *Remote Access Server*) **poslužitelj** te stoga mora imati odgovarajući certifikat. Izdat ćemo ga na osnovi predloška za RAS poslužitelje.

1. Prikažite ekran **Start** i kliknite na **Certification Authority**.
2. Prikazuje se **Certification Authority** konzola. Unutar lijevog okna proširite poslužitelj **SERVERDC-CA**.
3. U lijevom oknu desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite opciju **Manage**.
4. Prikazuje se **Certificate Templates** konzola. Desnim gumbom miša kliknite na predložak **RAS and IAS Server** i iz kontekstualnog izbornika odaberite opciju **Properties**.
5. Prikazuje se **RAS and IAS Server Properties** prozor. Kliknite na karticu **Security**.
6. Grupi **RAS and IAS Servers** postavite dozvole **Enroll** i **Autoenroll** kao na sljedećoj slici.



Slika 7. Dozvole za RAS and IAS Servers predložak

7. Kliknite gumb **OK** i zatvorite **Certificate Templates** konzolu.
8. Prikažite **Certification Authority** konzolu.

9. U lijevom oknu desnim gumbom miša kliknite na **Certificate Templates** mapu i iz kontekstualnog izbornika odaberite **New**-> **Certificate Template to Issue**.
10. Prikazuje se **Enable Certificate Templates** prozor. Označite predložak **RAS and IAS Servers** i kliknite gumb **OK**.
11. Ne zatvarajte **Certificate Authority** konzolu!

Certifikat će se izdati računalu **SERVER1** za neko vrijeme. Ubrzajmo postupak:

1. Prebacite se na računalo **SERVER1**.
2. Prikažite **Command Prompt**.
3. Upišite naredbu **`certutil -pulse`**.
4. Zatvorite **Command Prompt**.

-----NAPOMENA-----

Naredbom ***certutil –pulse*** forsirali smo izdavanje novog certifikata. Ta je naredba (logički) slična dobro nam poznatoj ***gpupdate*** naredbi, ali je specifična certifikacijskim servisima. Drugim riječima, njome ćete se koristiti kad ne želite čekati automatsko izdavanje certifikata (vrijeme osvježavanja Group Policyja), nego želite odmah izdati certifikate za koje je postavljeno automatsko izdavanje.

Provjerimo je li certifikat uspješno izdan:

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite **Certification Authority** konzolu.
3. Unutar lijevog okna kliknite na mapu **Issued Certificates**.
4. Provjerite je li izdan novi certifikat za računalo **SERVER1** na osnovi predloška **RAS and IAS Servers** (zadnje izdani certifikat) kao na sljedećoj slici.

Reques...	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date
2	RACUNARSTVO\Administrator	-----BEGIN CERTI...	Web Server (WebSer...	75000000027e1...	3.6.2014. 16:41
3	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	OCSP Response Sign...	750000000393d...	3.6.2014. 16:49
4	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	Domain Controller (...	7500000004dfe...	3.6.2014. 16:55
5	RACUNARSTVO\marko.tomic	-----BEGIN CERTI...	User (User)	7500000005541...	3.6.2014. 16:57
6	RACUNARSTVO\Administrator	-----BEGIN CERTI...	OSMIS korisnici (1.3....	75000000068b2...	3.6.2014. 17:42
7	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	Directory Email Repli...	7500000007d3f...	3.6.2014. 17:42
8	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	Domain Controller A...	75000000088f3...	3.6.2014. 17:42
9	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	Kerberos Authenticat...	750000000927f...	3.6.2014. 17:42
10	RACUNARSTVO\SERVERDC$	-----BEGIN CERTI...	OCSP Response Sign...	750000000a4b4...	3.6.2014. 17:42
11	RACUNARSTVO\ana.ivic	-----BEGIN CERTI...	OSMIS korisnici (1.3....	750000000ba38...	3.6.2014. 17:44
12	RACUNARSTVO\CLI1$	-----BEGIN CERTI...	OSMIS racunala (1.3....	750000000ca57...	3.6.2014. 17:44
13	RACUNARSTVO\Administrator	-----BEGIN CERTI...	EFS Recovery Agent (...	750000000d59f...	3.6.2014. 17:53
14	RACUNARSTVO\ana.ivic	-----BEGIN CERTI...	Basic EFS (EFS)	750000000e209...	3.6.2014. 17:59
15	RACUNARSTVO\SERVER1$	-----BEGIN CERTI...	OSMIS racunala (1.3....	750000000f320...	3.6.2014. 18:13
16	RACUNARSTVO\admin1	-----BEGIN CERTI...	OSMIS korisnici (1.3....	7500000010885...	3.6.2014. 18:13
17	RACUNARSTVO\admin1	-----BEGIN CERTI...	OSMIS korisnici (1.3....	7500000011511...	14.6.2014. 19:50
18	RACUNARSTVO\Administrator	-----BEGIN CERTI...	OSMIS korisnici (1.3....	75000000127d8...	14.6.2014. 19:53
19	RACUNARSTVO\SERVER1$	-----BEGIN CERTI...	RAS and IAS Server (...	7500000013823...	14.6.2014. 20:33

Slika 8. RAS certifikat za računalo SERVER1

5. Zatvorite sve prikazane prozore na računalu **SERVERDC**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Vježbu nastavljamo sa konfiguracijom NPS poslužitelja.

NPS konfiguracija

Prisjetimo se četvrte vježbe, NPS poslužitelj predefinirano ne dopušta spajanje VPN-om. Stoga moramo definirati pravilo koje će nam to omogućiti.

1. Prebacite se na računalo **SERVER1**.
2. Prikažite ekran **Start** i kliknite na **Network Policy Server**.
3. Prikazuje se konzola **Network Policy Server**. U lijevom oknu proširite mapu **Policies**.
4. U lijevom oknu desnim gumbom miša kliknite na mapu **Network Policies** i iz kontekstualnog izbornika odaberite opciju **New**.
5. Prikazuje se čarobnjak za izradu novog skupa postavki. U polje **Policy name** upišite **VPN Pristup**.
6. Iz izbornika **Type of network access server** odaberite opciju **Remote Access Server (VPN-Dial Up)** i kliknite gumb **Next**.
7. Prikazuje se ekran **Specify Conditions**. Kliknite gumb **Add**.
8. Prikazuje se ekran **Select condition**. U kategoriji **Groups** označite opciju **User Groups** i kliknite gumb **Add**.
9. Prikazuje se ekran **User Groups**. Kliknite gumb **Add Groups**.
10. Prikazuje se ekran za odabir objekata. U polje **Enter the object names to select** upišite **VPN_Korisnici**.
11. Kliknite na gumb **Check Names**. Ime grupe će se podcrtati. Kliknite gumb **OK**.
12. Vraćate se na ekran **User Groups**. Kliknite gumb **OK.**
13. Vraćate se na ekran **Specify Conditions**. Kliknite gumb **Next**
14. Prikazuje se ekran **Specify Access Permission**. Ostavite predefiniranu opciju **Access granted** i kliknite gumb **Next.**
15. Prikazuje se ekran **Configure Authentication Methods**. U kategoriji **EAP Types** kliknite gumb **Add**.
16. Prikazuje se ekran **Add EAP**. Označite stavku **Microsoft Protected EAP (PEAP)** i kliknite gumb **OK**.
17. Vraćate se na ekran **Configure Authentication Methods**. Kliknite gumb **Next**.
18. Prikazuje se ekran **Configure Constraints**. Ostavite predefinirane opcije i kliknite gumb **Next**.
19. Prikazuje se ekran **Configure Settings**. Ostavite predefinirane opcije i kliknite gumb **Next**.
20. Prikazuje se ekran sa sažetkom odabranih opcija. Kliknite gumb **Finish**.
21. Minimizirajte **Network Policy Server** konzolu.

Priključimo računalo CLI1 na fizičku mrežu.

1. Prebacite se na računalo **CLI1**.
2. Na izborniku **Virtual Machine Connection** prozora kliknite **File-> Settings**.
3. Prikazuje se ekran **Settings for KZOS-CLI1**.
4. U lijevom oknu kliknite na stavku **Network Adapter**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

5. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Virtual Network** ili **External Network** (ovisi kako je konfiguriran naziv eksterne mreže na računalu na kojem radite; ako niste sigurni, pitajte asistenta).
6. Kliknite gumb **OK**.

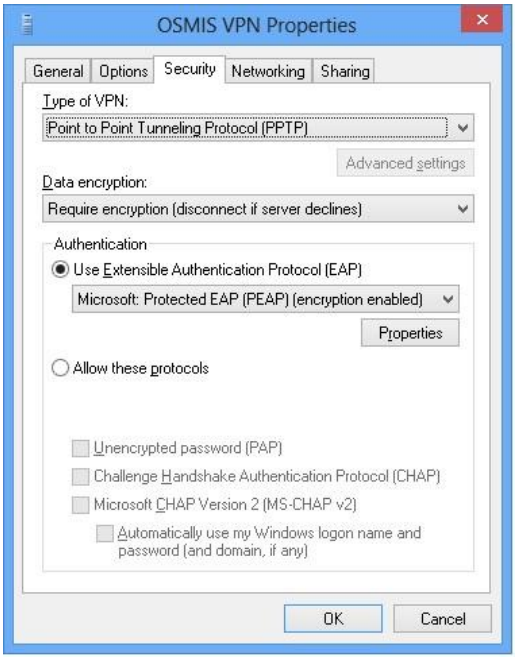
Izradimo VPN vezu.

1. Prikažite ekran **Start**, upišite **Control** i pritisnite tipku **Enter**.
2. Prikazuje se **Control Panel** prozor.
3. Kliknite na **Network and Internet**-> **Network and Sharing Center**.
4. Prikazuje se **Network and Sharing Center** prozor. Kliknite opciju **Set up a new connection or network**.
5. Prikazuje se čarobnjak za izradu mrežne veze. Odaberite opciju **Connect to a workplace** i kliknite gumb **Next**.
6. Prikazuje se ekran **How do you want to connect**. Odaberite opciju **Use my Internet connection (VPN)**.
7. Prikazuje se ekran **Type the Internet address to connect to**. U polje **Internet address** upišite IP adresu virtualnog računala SERVER1 na fizičkoj mreži (IP adresa fizičkog računala uvećana za 100).
8. U polje **Destination name** upišite **OSMIS VPN**.
9. Kliknite gumb **Create**.
10. Novostvorena VPN veza se prikazuje u rubnoj traci.
11. Zatvorite sve prikazane prozore na računalu **CLI1**.

Novostvorenoj VPN vezi moramo konfigurirati sigurnosne postavke:

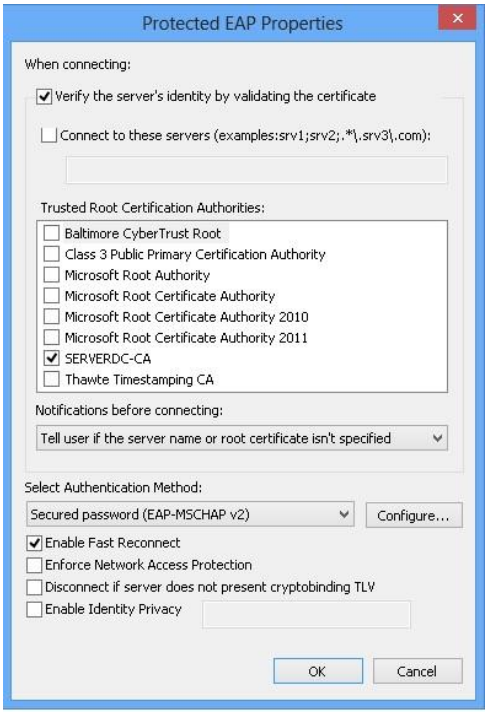
1. Prikažite ekran **Start**, upišite **`ncpa.cpl`** i pritisnite tipku **Enter**.
2. Prikazuje se **Network Connections** prozor.
3. Desnim gumbom miša kliknite na **OSMIS VPN** vezu i iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se prozor **OSMIS VPN Properties**. Kliknite na karticu **Security**.
5. Postavite opcije:
    a. Izbornik **Type of VPN**: odaberite **Point to Point Tunneling Protocol (PPTP)**.
    b. Uključite opciju **Use Extensible Authentication Protocol (EAP)**
    c. Izbornik **EAP**: odaberite opciju **Microsoft: Protected EAP (PEAP) (encryption enabled)**.
6. Usporedite postavljene opcije s onima na sljedećoj slici.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 9. Sigurnosne postavke OSMIS VPN veze

7. Kliknite gumb **Properties**.
8. Prikazuje se ekran **Protected EAP Properties**. Postavite opcije:
    a. isključite opciju **Connect to these servers**
    b. Kategorija **Trusted Root Certification Authorities**: označite stavku **SERVERDC-CA**
    c. Izbornik **Select Authentication Method:** odaberite (ako već nije) **Secured password (EAP-MSCHAP v2)**
9. Usporedite postavljene opcije s onima na sljedećoj slici.



Slika 10 EAP postavke

10. Kliknite gumb **OK.**
11. Vraćate se na ekran **OSMIS VPN Properties**. Kliknite gumb **OK**.
12. Vraćate se na **Network Connections** ekran. Ne zatvarajte ga!

VPN veza je stvorena i konfigurirana za PEAP autentikaciju.

Testiranje VPN veze

Provjerimo funkcionira li VPN veza.

1. Desnim gumbom miša kliknite na **OSMIS VPN** vezu i iz kontekstualnog izbornika odaberite opciju **Connect / Disconnect**.
2. Prikazuje se traka **Networks**. Kliknite na vezu **OSMIS VPN** i zatim kliknite gumb **Connect**.
3. Popunite pristupne podatke:
    a. **User name**: admin1@racunarstvo.edu
    b. **Password**: Pa$$w0rd
4. Kliknite gumb **OK**.
5. Pričekajte dok se VPN veza ne spoji.
6. VPN veza je spojena. U traci **Networks** je status **Connected**, kako prikazuje sljedeća slika.

Slika 11 VPN veza je spojena

Prilikom konfiguracije PEAP protokola računalo SERVERDC smo označili kao certifikacijski autoritet od povjerenja. Da nismo, prilikom spajanja VPN veze prikazala bi se greška kao na sljedećoj slici. Greška bi se prikazala samo kod prvog spajanja VPN-om.

Slika 12 Nepoznat certifikat

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Na prozor s postavkama PEAP protokola ćemo se vratiti pri kraju vježbe. Na njemu ćemo uključiti NAP s klijentske strane, jednom kad ga konfiguriramo. Za sada, računalo CLI1 ćemo ponovno spojiti na virtualnu mrežu.

1. Na izborniku **Virtual Machine Connection** prozora kliknite **File-> Settings**.
2. Prikazuje se ekran **Settings for KZOS-CLI1**.
3. U lijevom oknu kliknite na stavku **Network Adapter**.
4. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Private 1** i kliknite gumb **OK**.
5. Prikažite **Command Prompt**.
6. Upišite naredbu **`ping SERVERDC`**
7. Naredba mora vratiti odgovor.
8. Zatvorite sve prikazane prozore na računalu **CLI1**.

Sad kada imamo funkcionalan VPN pristup možemo implementirati VPN NAP.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

VPN NAP

VPN NAP se, po pitanju potrebnih komponenti, značajno ne razlikuje od komponenti DHCP NAP-a koje smo upoznali u prošloj vježbi. I ovdje ćemo morati definirati zdravstvene kriterije te kriterije provjere.

Konfiguracija GP objekta

VPN NAP će provjeriti zdravlje klijenata koji se na internu mrežu priključuju VPN vezom. Kao i kod DHCP NAP-a, moramo izraditi odgovarajući GP objekt. Njegove postavke će uključiti VPN NAP i pokrenuti NAP klijentski servis.

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
3. Prikazuje se **Group Policy Management** konzola. U lijevom oknu proširite mape **forest: racunarstvo. edu** i **Domains** i na kraju proširite domenu **racunarstvo.edu**.
4. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Racunala** i iz kontekstualnog izbornika odaberite opciju **Create a GPO in this domain, and Link it here...**
5. Prikazuje se **New GPO** prozor. U polje **Name** upišite **NAP_VPN** i kliknite gumb **OK**.
6. U lijevom oknu desnim gumbom miša kliknite na GPO **NAP_VPN** i iz kontekstualnog izbornika odaberite opciju **Edit**.
7. Prikazuje se **Group Policy Management Editor** konzola. Proširite mapu **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **Network Access Protection**-> **NAP Client Configuration.**
8. U lijevom oknu kliknite na stavku **Enforcement Clients**.
9. U desnom oknu desnim gumbom miša kliknite na **EAP Quarantine Enforcement Client** te i iz kontekstualnog izbornika odaberite opciju **Enable**.
10. U lijevom oknu kliknite na mapu **User Interface Settings**.
11. U desnom oknu desnim gumbom miša kliknite na stavku **User Interface** te iz kontekstualnog izbornika odaberite opciju **Properties**.
12. Prikazuje se **User Interface Properties** prozor. Popunite podatke.
    a. Polje **Title**: upišite **Obavijest administratora**
    b. Polje **Description**: upišite **VPN veza zahtijeva Firewall. Upravo ga uključujemo.**
13. Kliknite gumb **OK**.

Uključimo NAP klijentski servis.

1. U lijevom oknu proširite mapu **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **System Services**.
2. U desnom oknu dvostrukim klikom otvorite servis **Network Access Protection Agent**.
3. Prikazuje se ekran **Network Access Protection Agent Properties**. Uključite opciju **Define this policy setting** i zatim kliknite stavku **Automatic**.
4. Kliknite gumb **OK** i zatvorite **Group Policy Management Editor** konzolu.

Sigurnosnim filtriranjem ćemo GP objekt primijeniti samo na određena računala.

1. Prikažite u **Group Policy Management konzolu**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

2. U lijevom oknu označite GPO **NAP_VPN**. U desnom oknu u kategoriji **Security Filtering** označite grupu **Authenticated User** i kliknite gumb **Remove**.
3. Prikazuje se prozor s potvrdom uklanjanja grupe. Kliknite gumb **OK**.
4. U istoj kategoriji kliknite gumb **Add**.
5. Otvara se ekran za odabir objekata. U polje **Enter the object names to select** upišite **NAP_Racunala** i kliknite gumb **OK**.
6. Zatvorite **Group Policy Management** konzolu.
7. Prikažite ekran **Start**, upišite **cmd** i pritisnite tipku **Enter**.
8. Prikazuje se **Command Prompt** prozor. Upišite naredbu **`gpupdate /force`**
9. Na pitanje o odjavi korisnika odgovorite sa **Y**.
10. Prijavite se na računalo **SERVERDC** kao **RACUNARSTVO\Administrator** s lozinkom **Pa$$w0rd**

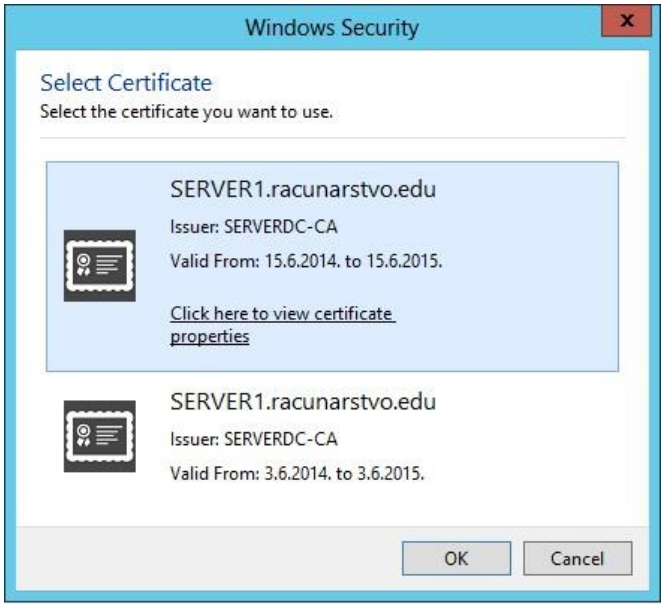
Sada možemo konfigurirati NPS poslužitelj.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Konfiguracija NPS poslužitelja za VPN NAP

Kao i u prošloj vježbi, konfiguracija NAP-a uključuje definiranje pravila za korištenu metodu provjere (DHCP ili, u današnjem slučaju, VPN) te definiranje kriterija za provjeru zdravlja klijenata. Odmah ćemo definirati i poslužitelj namijenjen automatskom usklađivanju klijenata sa NAP zahtjevima (eng. Autoremediation server).

1. Prikažite ekran **Start** i kliknite na **Network Policy Server**.
2. Prikazuje se konzola **Network Policy Server**. U lijevom oknu kliknite na stavku **NPS (local)**. Zatim u središnjem oknu kliknite na opciju (hiperveza) **Configure NAP**.
3. Prikazuje se ekran **Select Network Connection Method For Use with NAP**. Postavite opcije:
   a. Izbornik **Network connection method**: odaberite **Virtual Private Network (VPN)**
   b. Polje **Policy name**: upišite **OSMIS VPN NAP**.
4. Kliknite gumb **Next**.
5. Prikazuje se ekran **Specify NAP Enforcement Servers Running VPN Server**. Naš SERVER1 je i VPN poslužitelj i NPS poslužitelj stoga nam RADIUS nije potreban. Ostavite predefinirane opcije i kliknite gumb **Next**.
6. Prikazuje se ekran **Configure Machine Groups**. NAP računala smo konfigurirali putem Group Policyja. Ostavite predefinirane opcije i kliknite gumb **Next**.
7. Prikazuje se ekran **Configure an Authentication Method**. Kliknite gumb **Choose**.
8. Prikazuje se **Windows Security** ekran. Označite **NOVIJI** certifikat (izdan s današnjim datumom, kao na donjoj slici) i kliknite gumb **OK**.



Slika 13 Odabir novijeg certifikata

9. Vraćate se na ekran **Configure an Authentication Method**. Kliknite gumb **Next**.
10. Prikazuje se ekran **Specify a NAP Remediation Server Group and URL**. Kliknite gumb **New Group**.
11. Prikazuje se ekran **New Remediation Server Group**. Kliknite gumb **Add**.
12. Prikazuje se ekran **Add New Server**. Popunite podatke:

a. Polje **Friendly name**: upišite **SERVER1**
b. Polje **IP address or DNS name**: upišite **10.10.10.2**
c. Kliknite gumb **OK**.

13. Vraćate se na ekran **New Remediation Server Group.** U polje **Group Name** upišite **Domenski servisi** i kliknite gumb **OK**.
14. Vraćate se na ekran **Specify a NAP Remediation Server Group and URL**. Kliknite gumb **Next**.
15. Prikazuje se ekran **Define NAP Health Policy**. Ostavite predefinirane opcije i kliknite gumb **Next**.
16. Prikazuje se ekran sa sažetkom postavljenih opcija. Kliknite gumb **Finish**.
17. Ne zatvarajte **Network Policy Server** konzolu!

Zdravstveni kriterij će bit Windows Firewall. Definirajmo uvjete.

1. U lijevom oknu proširite mapu **Network Access Protection**-> **System Health Validators**-> **Windows Security Health Validator**.
2. Desnim gumbom miša kliknite na stavku **Settings** i iz kontekstualnog izbornika odaberite opciju **New**.
3. Prikazuje se ekran **Configuration Friendly Name**. U polje **Friendly Name** upišite **Firewall** i kliknite gumb **OK.**
4. Prikazuje se ekran **Windows Security Health Validator**. Isključite sve opcije osim one u kategoriji **Firewall Settings**. Kliknite gumb **OK**.
5. Ne zatvarajte **Network Policy Server** konzolu!

Uvjet za vatrozid asocirat ćemo s NAP postavkama, kao i kod DHCP NAP-a.

1. U lijevom oknu proširite mapu **Policies** i kliknite na stavku **Health Policies**.
2. U desnom oknu dvostrukim klikom otvorite svojstva stavke **OSMIS VPN NAP Compliant**.
3. Prikazuje se prozor s svojstvima NAP postavki. Postavite opcije:
   a. **Policy name**: ostavite **OSMIS VPN NAP Compliant**
   b. **Client SHV checks**: odaberite opciju **Client passes one or more SHV checks**
   c. **SHVs used in this health policy**: vrijednost u izborniku **Setting** postavite na **Firewall**.
4. Kliknite gumb **OK**.
5. Dvostrukim klikom otvorite svojstva stavke **OSMIS Noncompliant.**
6. Prikazuje se prozor sa svojstvima NAP postavki. Postavite opcije:
   a. **Policy name**: ostavite **OSMIS VPN NAP Noncompliant**
   b. **Client SHV checks**: odaberite opciju **Client fails one or more SHV checks**
   c. **SHVs used in this health policy**: vrijednost u izborniku **Setting** postavite na **Firewall**.
7. Kliknite gumb **OK**.

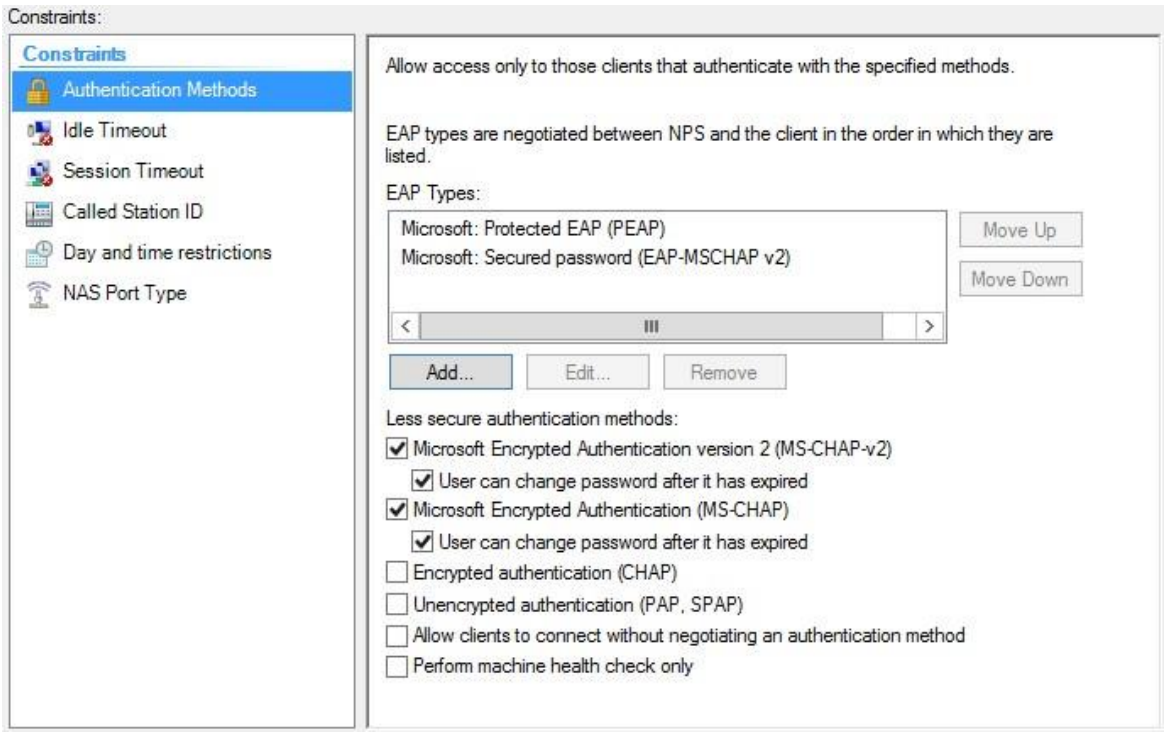
Sada definiramo uvjete za spajanje VPN vezom. Prvo ćemo onemogućiti staro pravilo koje je omogućavalo spajanje VPN-om bez NAP-a:

1. U lijevom oknu, unutar mape **Policies,** kliknite na stavku **Network Policies**.

2. U desnom oknu desnim gumbom miša kliknite na stavku **VPN Pristup** te iz kontekstualnog izbornika odaberite opciju **Disable**.

Sada definiramo nova pravila za VPN NAP:

3. U desnom oknu desnim gumbom miša kliknite na stavku **OSMIS VPN NAP Compliant** te iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se ekran **OSMIS VPN NAP Compliant Properties**. Kliknite na karticu **Constraints**.
5. U lijevom oknu kliknite na stavku **Authentication Methods**.
6. U desnom oknu kliknite gumb **Add**.
7. Prikazuje se ekran **Add EAP**. Označite stavku **Microsoft: Protected EAP (PEAP)** i kliknite gumb **OK**.
8. Vraćate se na ekran **OSMIS VPN NAP Compliant Properties**. U desnom oknu ponovno kliknite na gumb **Add**.
9. Prikazuje se ekran **Add EAP**. Označite stavku **Microsoft: Secured password (EAP-MSCHAP v2)** i kliknite gumb **OK**.
10. Vraćate se na ekran **OSMIS VPN NAP Compliant Properties**. Usporedite svoje postavke s onima na sljedećoj slici.



Slika 14. Autentikacijske postavke VPN pristupa

11. Kliknite gumb **OK**. Vraćate se u **Network Policy Server** konzolu.
12. Ponovite prethodni postupak (koraci 1 – 10) za **OSMIS VPN NAP Noncompliant** i **OSMIS VPN NAP Non NAP-Capable** postavke VPN veza.

S obzirom na to da smo definirali vlastite postavke za priključenje preko VPN-a, moramo onemogućiti predefinirane Microsoftove:

1. U lijevom oknu, unutar mape **Policies,** kliknite na stavku **Connection Request Policies**.
2. U desnom oknu, desnim gumbom miša kliknite na stavku **Microsoft Routing and Remote Access Service Policy** i iz kontekstualnog izbornika odaberite opciju **Disable**.
3. Zatvorite **Network Policy Server** konzolu.

I za kraj konfiguracije računala SERVER1, ponovno ćemo pokrenuti RRAS servise. Napravili smo znatne izmjene pa nije loša ideja (radi smanjenja potencijalnih problema) ponovno pokrenuti servis.

1. Prikažite ekran **Start** i kliknite na **Routing and Remote Access**.
2. Prikazuje se **Routing and Remote Access** konzola.
3. Unutar lijevog okna desnim gumbom miša kliknite na poslužitelj **SERVER1** i iz kontekstualnog izbornika odaberite **All Tasks**-> **Restart**.
4. Pričekajte ponovno pokretanje RRAS servisa i zatim zatvorite **Routing and Remote Access** konzolu.

Posvetimo se sada konfiguraciji klijenta.

Konfiguracija klijenta

Ažurirajmo konfiguraciju na računalu CLI1.

1. Prikažite ekran **Start** i upišite **cmd**
2. Desnim gumbom miša kliknite na **Command Prompt** te iz trake na dnu ekrana kliknite gumb **Run as administrator**.
3. Prikazuje se **UAC** prozor. Kliknite gumb **Yes**.
4. Prikazuje se **Command Prompt** prozor.
5. Na pitanje o odjavi korisnika odgovorite s **Y**.
6. Prijavite se na računalo **CLI1** kao **RACUNARSTVO\Admin1** s lozinkom **Pa$$w0rd.**

Provjerimo stanje NAP klijentskog servisa.

1. Prikažite ekran **Start** i upišite **cmd**
2. Desnim gumbom miša kliknite na **Command Prompt** te iz trake na dnu ekrana kliknite gumb **Run as administrator**.
3. Prikazuje se **UAC** prozor. Kliknite gumb **Yes**.
4. Prikazuje se **Command Prompt** prozor.
5. Upišite naredbu **`netsh nap client show state`**
6. Naredba ispisuje stanje NAP klijentskog servisa. Pronađite redak **Status** i uvjerite se da ima oznaku **Enabled.**

-----NAPOMENA-----
Ukoliko NAP klijentski servis nije pokrenut (status Disabled), ponovno pokrenite računalo **CLI1**. Zatim pokrenite Command Prompt kao Administrator jer će nam trebati u nastavku vježbe.

Provjerimo status vatrozida. Za uspješnu demonstraciju NAP-a mora bit isključen:

1. Upišite naredbu **`netsh advfirewall set allprofiles state off`**

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

2. Naredba mora ispisati status **Ok**.
3. Upišite naredbu **`netsh advfirewall show allprofiles`**
4. Uvjerite se da je vatrozid isključen na svim profilima.

Priključimo računalo CLI1 na fizičku mrežu učionice.

1. Na izborniku **Virtual Machine Connection** prozora kliknite **File-> Settings**.
2. Prikazuje se ekran **Settings for KZOS-CLI1**.
3. U lijevom oknu kliknite na stavku **Network Adapter**.
4. Unutar desnog okna iz izbornika **Virtual switch** odaberite opciju **Virtual Network** ili **External Network** (ovisi kako je konfiguriran naziv eksterne mreže na računalu na kojem radite; ako niste sigurni, pitajte asistenta).
5. Kliknite gumb **OK**.
6. Prikažite virtualno računalo **CLI1**.
7. Prikažite **Command Prompt**.
8. Pomoću naredbe ping provjerite vezu prema računalu SERVER1 (IP adresa fizičkog računala uvećana za 100).
9. Naredba mora vratiti odgovor.

Na VPN vezi OSMIS VPN moramo uključiti NAP prisilu:

1. Upišite naredbu **`ncpa.cpl`**
2. Prikazuje se **Network Connections** prozor.
3. Desnim gumbom miša kliknite na vezu **OSMIS VPN** te iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se prozor **OSMIS VPN Properties**. Kliknite na karticu **Security**.
5. U kategoriji **Authentication** kliknite gumb **Properties**.
6. Prikazuje se **Protected EAP Properties** prozor. Označite opciju **Enforce Network Access Protection** i kliknite gumb **OK**.
7. Vraćate se na prozor **OSMIS VPN Properties**. Kliknite gumb **OK**.
8. Vraćate se u **Network Connections** prozor. Ne zatvarajte ga!

Provjerimo funkcionira li VPN NAP mehanizam.

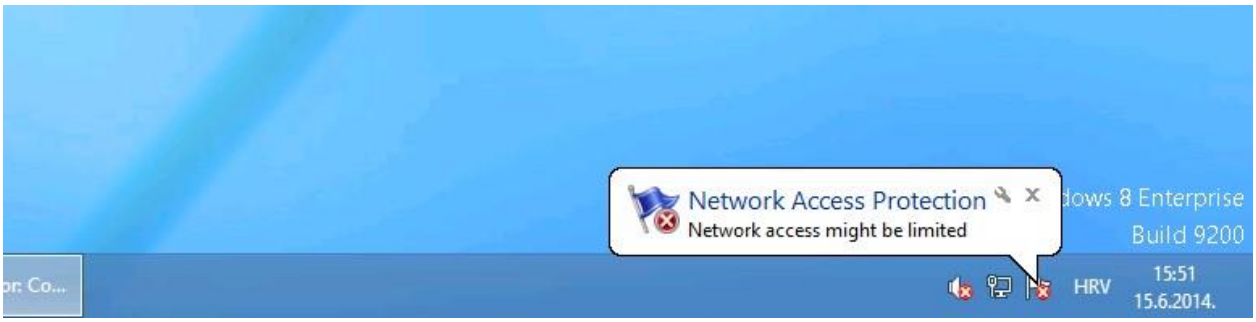
1. Desnim gumbom miša kliknite na OSMIS VPN te iz kontekstualnog izbornika odaberite opciju **Connect / Diconnect**.
2. Prikazuje se rubna traka. Kliknite na **OSMIS VPN** vezu i zatim kliknite gumb **Connect**.
3. VPN veza je spojena.

Uspješno smo se spojili VPN-om iako je vatrozid isključen? Provjerimo, za svaki slučaj njegov status.

1. Prikažite **Command Prompt**.
2. Upišite naredbu **`netsh advfirewall show allprofiles`**

Ispis naredbe nam daje do znanja da je vatrozid ipak uključen. Uključio ga je NAP mehanizam jer smo konfigurirali automatsko usklađivanje sa NAP kriterijima. Ukoliko ga opet isključimo, primijetit ćemo NAP obavijest.

1. Upišite naredbu **`netsh advfirewall set allprofiles state off`**
2. Nakon sekundu-dvije u obavijesnoj se traci prikazuje **NAP obavijest**, kao sljedećoj slici. Kliknite na nju. Ako niste stigli, ponovno isključite vatrozid i obavijest će se ponovno pojaviti.



Slika 15 NAP obavijest

3. Kad ste kliknuli na obavijest, prikazuju se informacije o postupku usklađivanja računala sigurnosnim zahtjevima NAP-a. Uočite i tekst koji smo definirali preko Group Policyja, kao na slici u nastavku. Kliknite gumb **Close**.

Slika 16 VPN NAP informacije

Ovime smo potvrdili funkcioniranje VPN NAP mehanizma i završili današnju vježbu.

Rezultat vježbe

Rezultat današnje vježbe jesu izmjene na svim virtualnim računalima, i to redom:

1. **SERVERDC** izmjene:

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

   a. grupa NAP_Racunala s računalom CLI1
   b. GP objekt VPN_NAP s filtriranjem na grupu NAP_Racunala. GP objekt sadržava postavke NAP klijentskog servisa i konfiguraciju teksta poruke koji se prikazuje u slučaju neispravnih zdravstvenih uvjeta.
   c. RAS/IAS predložak za izdavanje certifikata
   d. (**OPCIONALNO**): oporavljen certifikacijski servis

2. **SERVER1** izmjene:
   a. implementiran RAS poslužitelj s NAT-om i VPN-om
   b. implementiran NPS poslužitelj s postavkama:
      i. uvjet je uključeni Windows Firewall
      ii. NPS postavke VPN NAP-a preko PEAP enkripcije s automatskim ispravljanjem propusta iii. izdan certifikat na osnovi RAS/IAS predloška
3. **CLI1** izmjene:
   a. VPN konekcija prema IP adresi računala SERVER1 na fizičkoj mreži
   b. VPN konekcija upotrebljava PEAP enkripciju s forsiranim NAP-om.

Današnja vježba ne zahtijeva *snapshot*.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Što treba znati nakon ove vježbe?

1. Konfigurirati VPN NAP
2. Omogućiti izoliranim klijentima pristup određenim resursima (npr. nekom poslužitelju)
3. Konfigurirati automatsko usklađivanje s NAP standardima

Dodatna literatura

- Popis čestih grešaka kod povezivanja VPN-om:

http://blogs.technet.com/b/rrasblog/archive/2009/08/12/troubleshooting-common-vpn-relatedhttp://blogs.technet.com/b/rrasblog/archive/2009/08/12/troubleshooting-common-vpn-related-errors.aspxerrors.aspx

- Technet upute za implementaciju VPN NAP-a http://technet.microsoft.com/en-us/library/cc770422(v=ws.10).aspx

- Neke česte pogreške kod NAP-a http://technet.microsoft.com/en-us/library/dd348494(v=ws.10).aspx

- **Microsoftove detaljne upute za implementaciju VPN NAP-a s RADIUS autentikacijom. Preporučujem odraditi.**

http://www.microsoft.com/en-us/download/details.aspx?id=5536

- Specifikacija PEAP protokola. Tehnička dokumentacija (u rangu RFC-ova).

http://msdn.microsoft.com/en-us/library/cc238354(v=prot.13).aspx