SEMINARSKA NALOGA

VPN (Virtual Private Network)

Predmet: RAČUNALNIŠKE KOMUNIKACIJE IN OMREŽJA 2

Kazalo vsebine

KLJUČNE BESEDE

VPN – Virtual Private Network

Client – računalnik klient, kateri se povezuje na gostitelja

Host – računalnik gostitelj, na katerega se povezujemo

Protokol - je formalen opis pravil za izmenjavo sporočil, ki jih je potrebno spoštovati, da se lahko med seboj sporazumevajo računalniški sistemi v omrežju.

Port(vrata)- vmesnik, skozi katerega pošiljamo in prejemamo podatke.

Enkripcija- postopek kodiranja poljubnih podatkov tako, da do njih ne more dostopati nihče drug, razen vas samih.

UVOD

VPN oz Navidezno privatno omrežje se največ uporablja v podjetjih kjer zaposleni delajo tudi izven delavnega časa. VPN se uporablja za prenos podatkov med dvema ali več omrežij, ki niso v istem zasebnem omrežju. Nekateri strežniki vas zaradi varnosti pri pristopu preverjajo. Če se izkaže, da vaša IP številka ni na seznamu zaželenih računalnikov ali skupine računalnikov vam strežnik dostop prepreči. Rešitev je VPN, ki omogoči povezavo v določeno omrežje. Tako dobimo IP številko omrežja in nemoteno dostopamo do omrežja. VPN nam dovoljuje da dostopamo do službenega :

- poštnega odjemalca
- dostop do datotek na strežniku in varen prenos teh datotek
- varen prenos datotek med službenim in domačim računalnikom

DEFINICIJA VPN-ja

Kratica VPN pomeni Virtual Private Network ali navidezno zasebno omrežje. VPN vam omogoča, da se preko VPN vmesnika, ne glede na to, kje se nahajate, z uporabo modema ali obstoječega omrežja, direktno povežete na računalniško omrežje fakultete. VPN za prenos podatkov uporablja internet. Le-ta se vzpostavi med dvema ali več točkama in preko njega poteka prenos podatkov. Največkrat se Vpn uporablja za povezavo, ki preko interneta povezujeje zasebno omrežje podjetja in oddaljeno mesto ali zaposlenega. Za vzpostavitev takega tunela morati napravi na obeh koncih tunela uporabljati isti protokol za vzpostavitev tunela. Ti so zaščiteni z požarnim zidom z močno enkripcijo in se razpakirajo šele na svoji destinaciji, na drugem koncu tunela. Tako lahko zunanji opazovalec - hecker vidi le, da promet poteka, nikakor pa ne vidi, kateri podatki se znotraj paketov nahajajo.

Način uporabe Vpn-ja:

Uporabnik v omrežje

Ta VPN nacin dovoljuje klientu da uporabi VPN za povezavo med njegovim podjetjem in njegovim domačim ali službenim računalnikom

Omrezje v omrežje

Ta VPN nacin povezuje dve omrezji preko VPN povezave. Ta nacin zdruzuje dva razlicna omrezja v enega in eliminira potrebo po geografsko razprostranem omrezju (Wide Area Network-WAN).

Glavne lastnosti

- Varnost: skoraj vse VPN storitve uporabljajo javno omrežje. Problem zasebnosti in varnosti se rešuje s šifriranjem ali s tehnikami, ki logično ali fizično ločijo promet enega uporabnika od ostalih.
- Zmogljivost: zmogljivost VPN storitve je odvisna od omrežja ponudnika storitve, obremenitve le-tega z ostalimi uporabniki. VPN storitev mora vsebovati mehanizem za zagotavljanje zmogljivosti.
- Upravljanje in administracija: premiki, dodajanja in spremembe VPN omrežja postanejo težavne, ker mora podjetje poskrbeti, da se pri tem ne spremenijo varnostni ukrepi.
- Razširljivost

Prednosti VPN-ja

- razširi geografsko povezljivost

- izboljša varnost
- omogoča uporabo požarnega zidu za prenos zaupnih podatkov podjetja,
- omogoča uporabo xDSL, kabelske povezave povezave za vzpostavitev varne VPN povezave,
- zmanjša stroške delovanja v primerjavi z WAN-om,
- skrajša čas prenosa in zmanjša stroške prenosa za oddaljene uporabnike,
- izboljša storilnost,
- omogoča združljivost širokopasovnega omrežja,
- omogoča hitrejšo donosnost naložbe kot WAN,
- omogoča razširitev zaradi velikega števila tunelov (do32)

Možnosti uporabe (službena) :

- poštnega odjemalca
- dostop do datotek na strežniku in varen prenos teh datotek
- varen prenos datotek med službenim in domačim računalnikom

Potrebna oprema:

- matična lokacija (strežnik): → ADSL dostop ali najeti vod s statično IP številko
- oddaljene lokacije (klienti): → kabelski internet, ADSL, ...

PRTOTOKLI VPN-ja

SSL (Secure Socket Layer)

je protokol, ki ga je razvil Netscape za oddajanje zaupnih dokumentov preko interneta. SSL deluje v navezi z uporabo digitalnega potrdila, ki omogoča kodiranje podatkov med strežnikom in odjemalcem preko SSL protokola in s tem zagotavlja visoko stopnjo varnosti za komunikacijo.Po dogovoru se morajo strani, ki zahtevajo SSL protokol uporabljajo starni s https protokol. Na strežniku mora biti nameščen certifikat z zasebnim ključem. SSL certifikat je digitalno potrdilo, ki omogoča kodiranje podatkov med strežnikom in odjemalcem preko SSL protokola in s tem zagotavlja visoko stopnjo varnosti za komunikacijo. Potrdilo vsebuje informacije o njegovemu imetniku in izdajatelju.

Enkripcija s simetričnim ključem

Za to enkripcijo se za kodiranje in dekodiranje uporablja isti ključ. Uporaba simetrirčne enkripcije je smoternejšča če imamo za pošiljanje večje količine podtkov, saj je hitrejša od asimetrične enkripcije. Ta način do neke mere omogoča tudi preverjanje, s kom komunikacija v resnici poteka, saj podatke zakodirane z enim ključem lahko dekodira le oseba z tem istim ključem. Torej, dokler je ključ znan le dvema stranema, sporočila med njima ne morejo biti dekodirana z nobenim drugim ključem. Oseba z pridobljenim ključem lahko, ne le dekodira sporočila, temveč tudi zakodira nova, spremenjena ter jih pošlje, kot bi jih poslal nekdo izmed pravih lastnikov ključev. Enkripcija s simetričnim ključem igra pomembno vlogo v protokolu SSL.

Enkripcija z javnim ključem

Uporablja se 2 ključa. Eden je vedno javen in vsakemu viden. Javen kjuč se uporablja za zakodiranje vsebine. Drugi ključ pa je zaseben in mora biti na varem. Za njega mora vedeti samo lastnik. S tem pa se vsebino odkodira. Podatki zakodirani z javnim ključem so lahko dekodirani le z pripadajočim privatnim ključem. Enkripcije z javnim kjučen je počasnejša od simetrične enkripcije. Uporabljaja se jo tudi za pošiljanje manjših količin podatkov. To enkripcijo se uporablja tudi v SSL protokolu.

Tuneliranje tehnika prenosa podatkov enega podatkovnega omrežja po komunikacijski strukturi drugega, na podlagi posebnega protokola za tuneliranje

Point–to–Point Tunneling Protocol (PPTP, protokol za tuneliranje iz točke v točko)
Protokol omogoča, da ustvarimo varno virtualno privatno omrežje (VPN), ki omogoča uporabniku dostop na strežnik skupnega omrežja preko varne neposredne povezave preko interneta. Celoten okvir sloja podatkovne povezave, ki ga ustvari aplikacija, je enkapsuliran v IP datagram. Ta postopek krši pravila Open Systems Interconnection (OSI) referenčnega modela, toda zagotavlja, da je celoten PPP okvir kriptiran v IP datagramu.
Razvit s strani Microsoft in Ascend. Zagotovi varno (šifriranje) povezavo.

Generic Routing Encapsulation (GRE)
GRE omogoča več kot do sedaj obravnavani L2 tunelski protov
Lahko prenaša tudi druge protokole, ne samoIPv4

Uporabljen kot delček protokola PPTP za prenos dejanskih podatkov

Point–to–Point Protocol (PPP)

Protokol na sloju podatkovne povezave, ki uporablja klicno linijo od uporabnika do terminalskega strežnika ponudnika internetnih storitev. V nasprotju z njenim predhodnikom Serijskim Linijskim internetnim Protokolom (SLIP), PPP vsebuje podporo za več protokolom omrežnega sloja, protokolov za opazovanje kvalitete povezave in protokolov za dokaz pristnosti, odkrivanje napak, varnost, dinamično naslavljanje IP. PPP se uporablja za povezavo med samo dvema računalnikoma in zato ne potrebuje toliko možnosti kot pa protokoli lokalnih omrežij, kot so polja za naslov za vsak paket in mehanizem za dostop do medija (media access control, MAC).

Layer 2 Tunneling Protocol (L2TP)

Ta deluje kot PPTP samo z to razliko, da ne vključuje enkripcije podatkov. L2TP je protokol 2. sloja, ki tunelira PPP bloke med dostopovnim krmilnikom ISP in omrežnim strežnikom. Za transport uporablja UDP tako za upravIjalska sporočila kot za podatke. Za šifriranje uporablja IPSec ESP. Glava L2TP se uporablja za enkapsulacijo glave in koristne vsebine PPP.
L2TP podpira več sil1lultanih tunelov za vsakega uporabnika.

Ipsec

IPsec omogoča ovijanje (encapsulation), šifriranje prometa za namen prenosa preko IP omrežja zaščito pred ponavljanjem podatkov. Infrastruktura je javni internet, zato je treba dati ustrezen poudarek tudi kvaliteti storitve prenosa preko javnega medija. Za varnost je poskrbljeno, saj so uporabljeni mehanizmi avtentikacije in močnega šifriranja. Poleg koristne vsebine se lahko šifrira tudi glava IP paketa, celotni IP paket se nato še ovije v drug IP paket.

Obstajata dva načina delovanja protokola IPsec:

- Transportni način

Transportni način delovanja je osnovni način delovanja protokola IPsec. Uporablja se za zaščito protokolov višjih nivojev oz. aplikacij, šifrira se samo koristna vsebina, ne pa glava IP paketa. Transportni način se uporablja pri komunikaciji dveh gostiteljskih sistemov (host). Pri komunikaciji dveh IPsec komunikacijskih naprav oz. varnostnih prehodov (security gateway) se uporablja tunelski način. Pojem »varnostni prehod« označuje napravo, ki izvaja IPsec funkcije v korist tretjega sistema. Na varnostni prehod se priključi LAN segment, kjer se lahko uporabljajo zasebne IP številke. Ob vzpostavitvi tunela med dvema točkama se na začetku izvrši še avtentikacija.

- Tunelski način

Posebnost je t.i. zunanja glava, ki omogoča tuneliranje. Na oddajni strani se celoten izvorni paket naloži v paket IPsec, ki po omrežju potuje v skladu z navodili zunanje glave. Zunanja glava omogoča npr. poljubne (tudi zasebne) naslove v originalnem paketu, kar je nadvse uporabno pri gradnji navideznih zasebnih omrežij. V primeru učinkovitega šifriranja podatkov prisluškovalec vidi samo zunanjo glavo in tako lahko sklepa le o začetni in končni točki tunela, nič pa ne ve, kdo je v resnici pošiljatelj in kdo prejemnik vsebine. Poleg tega je prisluškovalcu skrit tudi paket TCP, na podlagi katerega bi lahko sklepal o vrsti podatkov.

Zašifrirano je vse od glave omrežnega sloja naprej, torej vsi podatki, ki niso potrebni za usmerjanje paketov:

IPSec sestavljajo:

- dogovor o načinu šifriranja in izmenjava ključev (Key Management),
- preverjanje nespremenjenosti podatkov in overjanje brez šifriranja (Authentication Header - AH)
- šifriranje vsebine (Encapsulating Security Payload - ESP).
- Šifrirani algoritmi
- avtentikacijski algoritmi
- domena interpretacije
- upravljanje s kjuči

ŠIFRIRANJE PODATKOV

AH (Authentication Header) tu se ne kodirajo poatki v paketu ampak se patetku doda digitalni podpis. Z digitalnim podpisom prejemnik preveri paket. Ali je bil spremenjen na poti in izvor paketa.

ESP (Encapsulating Security Payload) tu se zakodira celoten paket mu doda novo IP glavo ki ni zakodirana. Tu kot izvor navede svojo IP številko, namesto dejanskega naslovnika pa navede njegovega posrednika. Pri tem načinu kodiranja se paketi direktno usmerijo proti prejemniku paketa.

ESP zahteva implementacijo šifrirnih algoritmov tudi, če ne bodo uporabljeni. Če potrebujemo samo overjanje, je uporaba protokola AH veliko bolj racionalna kot uporaba ESP. Običajno je ESP

vključen v AH.

Digitalno potrdilo javnega ključa (public key certificate) je digitalni dokument, ki potrjuje povezavo med javnim ključem in osebo ali institucijo ali strežnikom. Z njim preverimo, če javni ključ pripada tistemu kateremu mislimo damu pripada. Potrdilo vsebuje javni ključ in informacijo o njegovem imetniku, ki ju podpiše oseba ali institucija, ki ji zaupamo. Potrdila so objavljena v splošno dostopnih imenikih ali na spletnih straneh.

Oblika digitalnega potrdila po standardu **ISO/IEC X.509V3**:

Podatkovni del:

- verzija
- serijska številka (enolična za potrdila posameznega overitelja)
- algoritmi in parametri (SHA1 in RSA)
- izdajatelj (overitelj javnih ključev)
- čas veljavnosti od -do
- prejemnik digitalnega potrdila (njegovo ime, drugi podatki o njem)
- podatki o njegovem javnem ključu:
  - algoritem
  - parametri
  - javni ključ
- enolična oznaka uporabnika
- razširitve
- digitalen podpis teh podatkov, ki je narejen z zasebnim ključem CA

Podpisni del:

- algoritem digitalnega podpisa
- digitalen podpis teh podatkov (uporabljen je zasebni ključ overitelja)

OVERITELJ (Certification Authority – CA)

Overitelj (Certification Authority - CA) je ustanova, ki je pooblaščena za izdajo digitalnih potrdil ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Overitelj prejema zahteve:

- za izdajo digitalnih potrdil,
- izvaja ustrezno identifikacijo bodočih imetnikov,
- izdaja digitalna potrdila in skrbi za register izdanih potrdil, saj so informacije o izdanih potrdilih javnega značaja (razen v zaprtih sistemih).
- za preklic digitalnih potrdil in informacije o preklicih osvežuje v registru preklicanih potrdil, ki je prav tako javnega značaja.

Vsak overitelj objavi svoj javni ključ in dokumente o overiteljskih politikah (Certification Policies), ki opisujejo različne podprte postopke, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ. Celoten proces izdajanja posameznih skupin digitalnih potrdil natančno določa overiteljska politika.Pomembno je tudi, da overitelj poskrbi za varnost svojega zasebnega ključa, saj bi bila sicer potrdila, ki jih je izdal, brez pomena - še več, lahko bi prišlo do poneverb, ki bi jih prepozno opazili. Hraniti ga morajo na dobro zaščitenem računalniku.

POŽARNI ZID IN VPN

V primeru da imamo vklopljen požarni zid se zna zgoditi da nam VPN povezava ne bo delovala. Za to moramo odpreti nekatera vrata(porte):

· požarni zid mora dovoljevati uporabo TCP porta 1723 (PPTP)

· požarni zid mora dovoljevati uporabo protokola IP protocol 47 Generic Routing Encapsulation

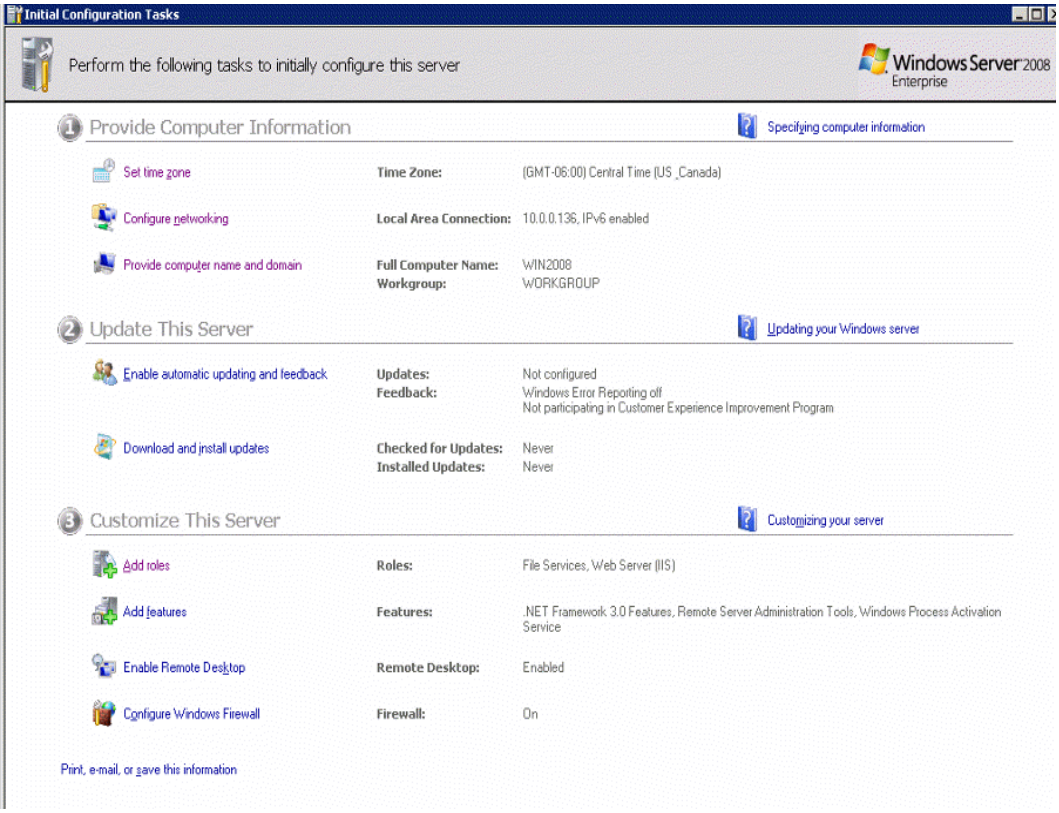
- Odpre se nam okno **Omrežne Povezave**. Znotraj njega vidimo obstoječe mrežne povezave (modemske, omrežne in VPN). Nas zanimajo tiste, ki se nahajajo v razdelku **Lan ali Hitri Internet**. Ikona z napisoma **Povezava Lokalnega Omrežja** predstavlja mrežno kartico na računalniku. Ključavnica v njenem desnem zgornjem kotu pa pomeni, da je na računalniku vklopljen požarni zid. Z miško označimo ikono **Povezava Lokalnega Omrežja** kliknemo na desno miškino tipko in izberemo **Lastnosti**.
- Prikaže se nam okno **Povezava Lokalnega Omrežja Lastnosti** z tremi zavihki.
- Izberemo zavihek **Advanced** in nato kliknemo na gumb **Možnosti**
- Recimo, da smo se odločili, da bo požarni zid ostal vklopljen, kljub temu pa bi radi imeli dostop do datotek v skupni rabi na svojem računalniku.. Izberemo zavihek

Exceptions. Prikaže se nam se seznam 14 servisov, ki jih požarni zid spušča na računalnik. če slučajno ni kljukice na kvadratku z napisom **File and Printers Sharing**, jo obvezno naredimo.

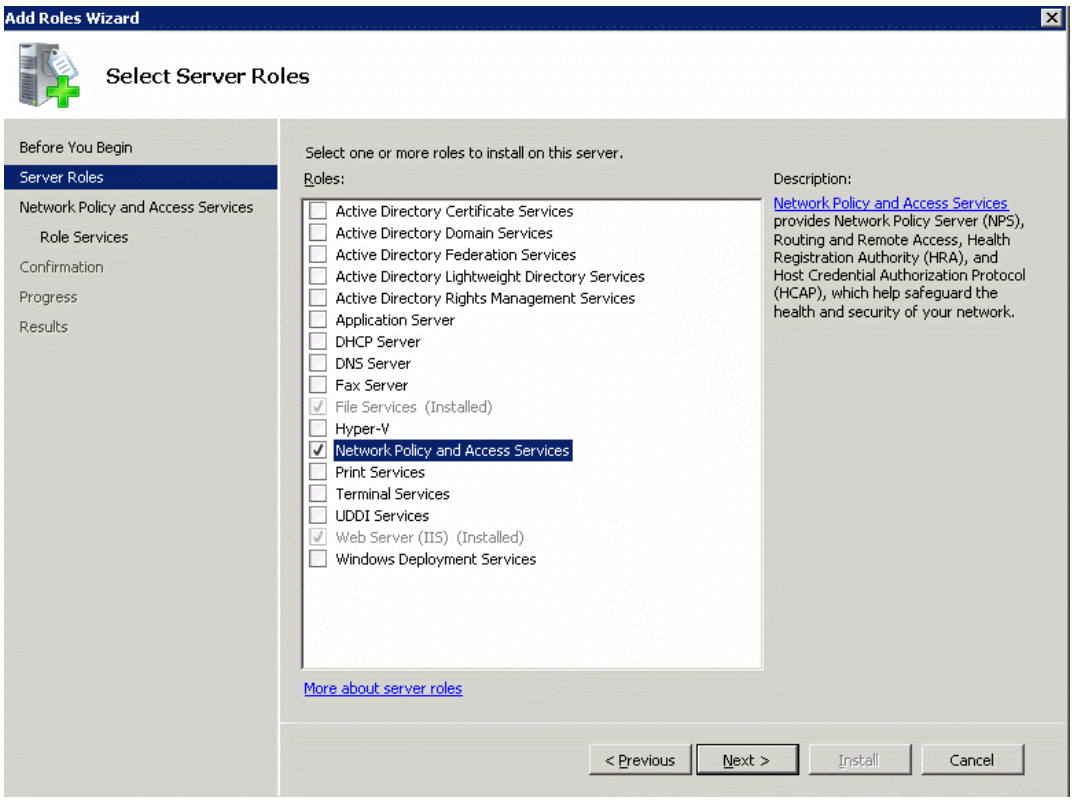
- Označimo izbiro **File and Printer Sharing** in kliknemo na gumb **Edit**. Prikaže se nam okno **Edit a Service**. Sedaj vidimo seznam portov, ki jih **File and Printer Sharing** uporabljajo za dostop do datotek v skupni rabi.
- Označimo prvega izmed njih in kliknemo na tipko **Change Scope**. V okenčku, ki se nam odpre vidimo vir naših težav. **Scope** (območje) iz katerega dovolimo dostop, do map skupni rabi je **My network (subnet) only**. Omejeni smo torej na naše domače omrežje. če je računalnik na kakšnem drugem omrežju potem ne more pristopati do map v skupni rabi na našem računalniku.
- Stvar spremenimo tako, da kliknemo na krogec **Any computer (including those on the Internet)**. Kliknemo na gumb **OK**.
- Postopek ponovimo še za preostale porte (TCP 445, UDP 137 in UDP 138). Ko končamo mora vrednost **Scope** pri vseh štirih biti **Any**

KONFIGURIRANJE SERVER 2008

- Open the Windows 2008 **Server Manager** or **Initial Configuration Tasks.**
- Click the **Add Roles**.

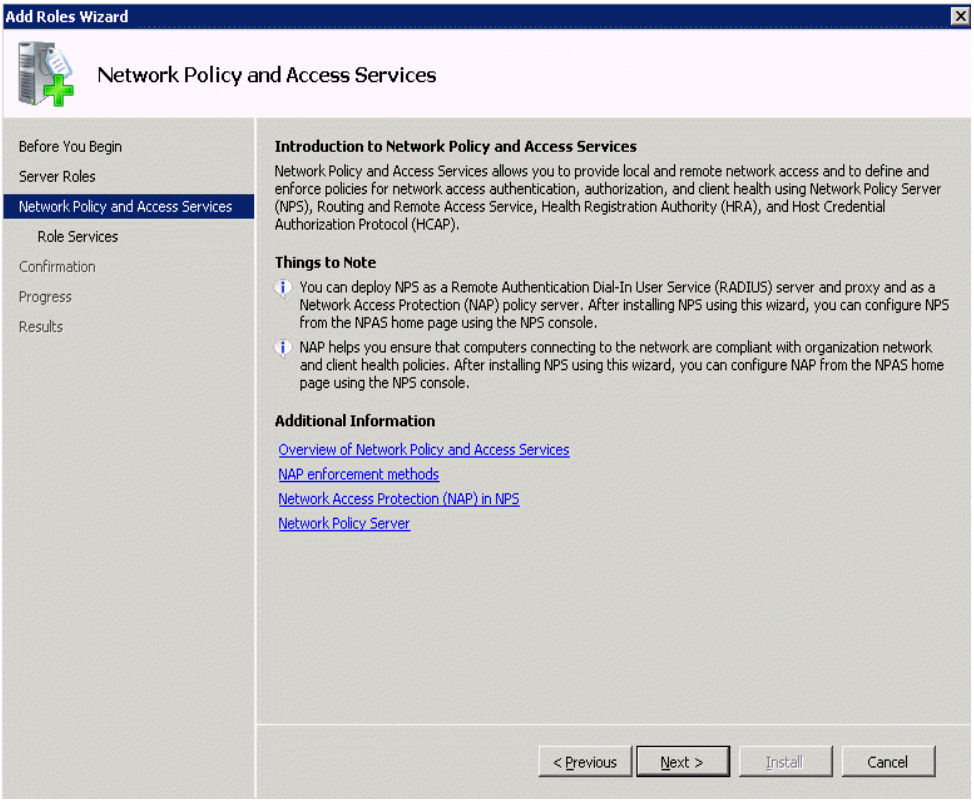


✘ Skip the **Before You Begin** page.

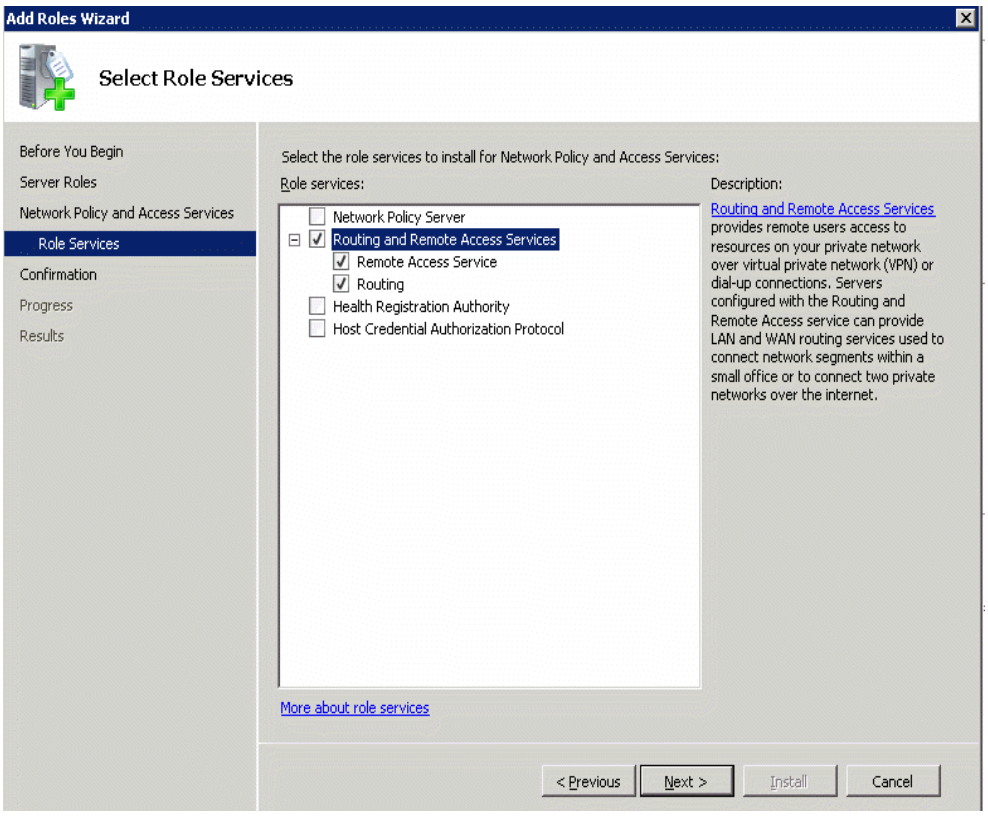


✘ In **Server Roles**, check **Network Policy and Access Services**. Click **Next**.

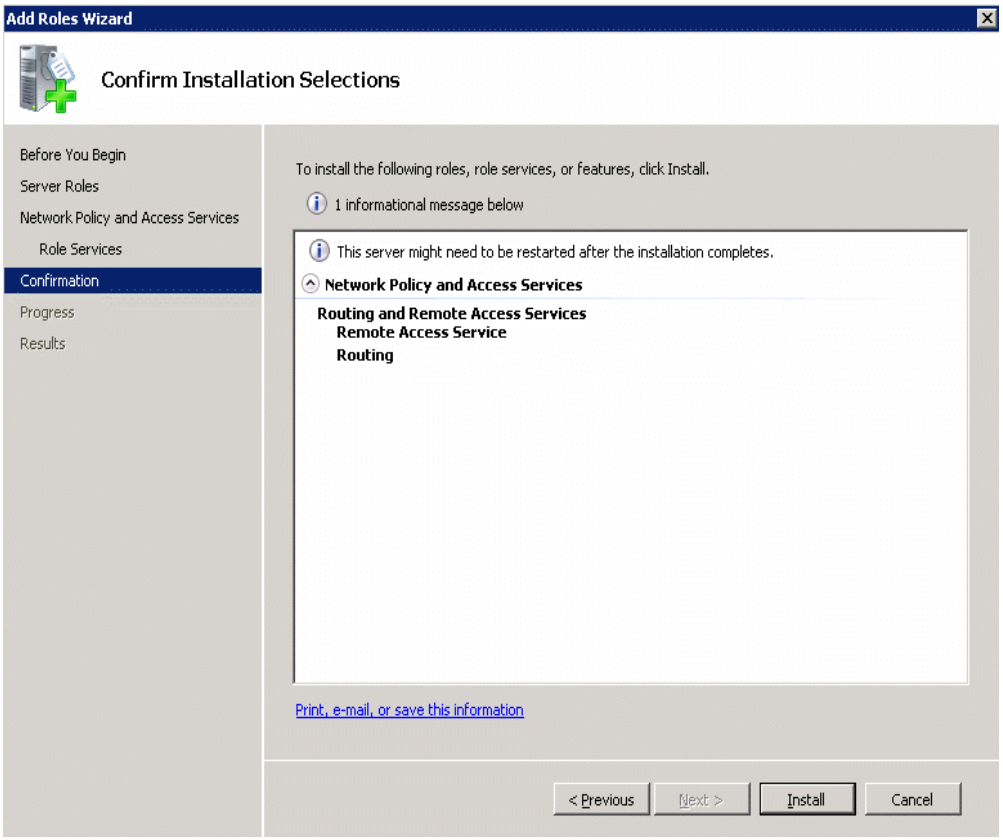
✘ Read the information on the **Network Policy and Access Services** page. Click **Next**.



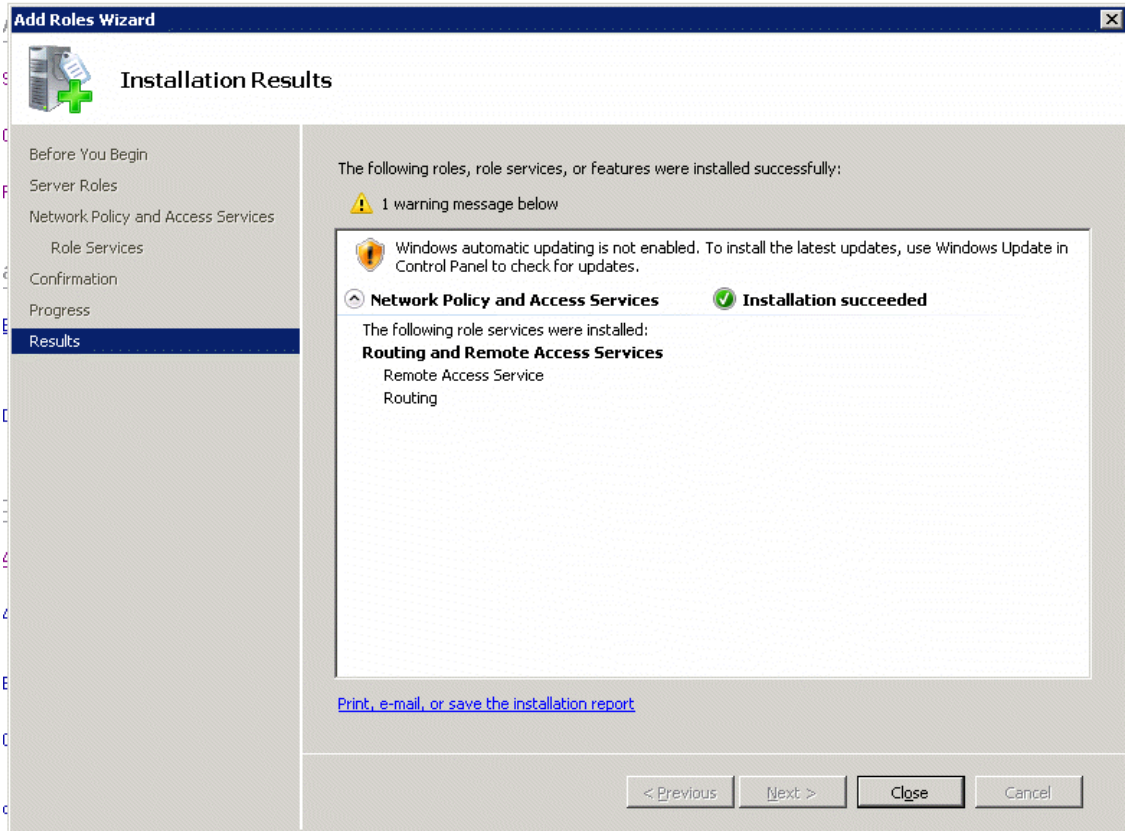
✘ On the **Select Role Services** page, check the **Routing and Remote Access Services** and make sure the **Remote Access Service** and **Routing** are checked. Click **Next**.



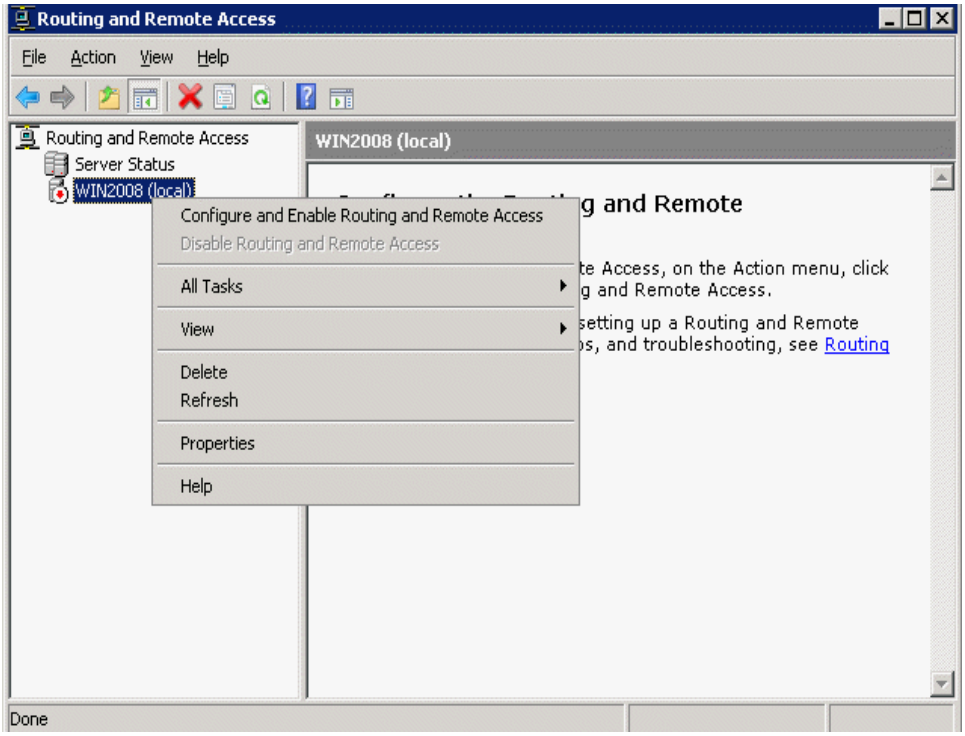
✘ Click **Install** on the **Confirm Installation Selections** page.



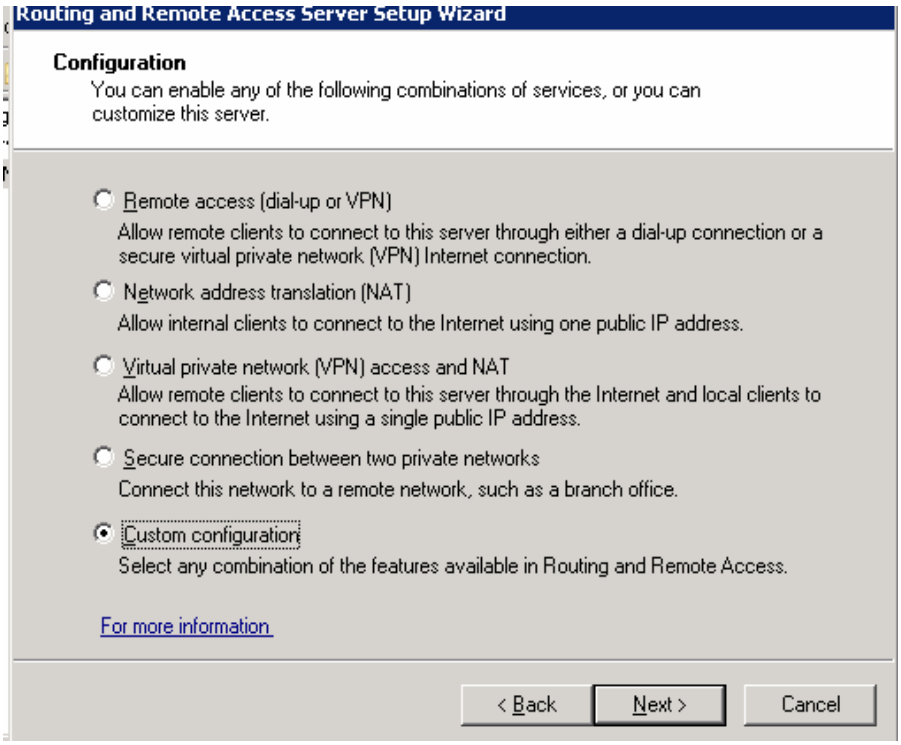
✘ Click **Close** on the **Installation Results** page



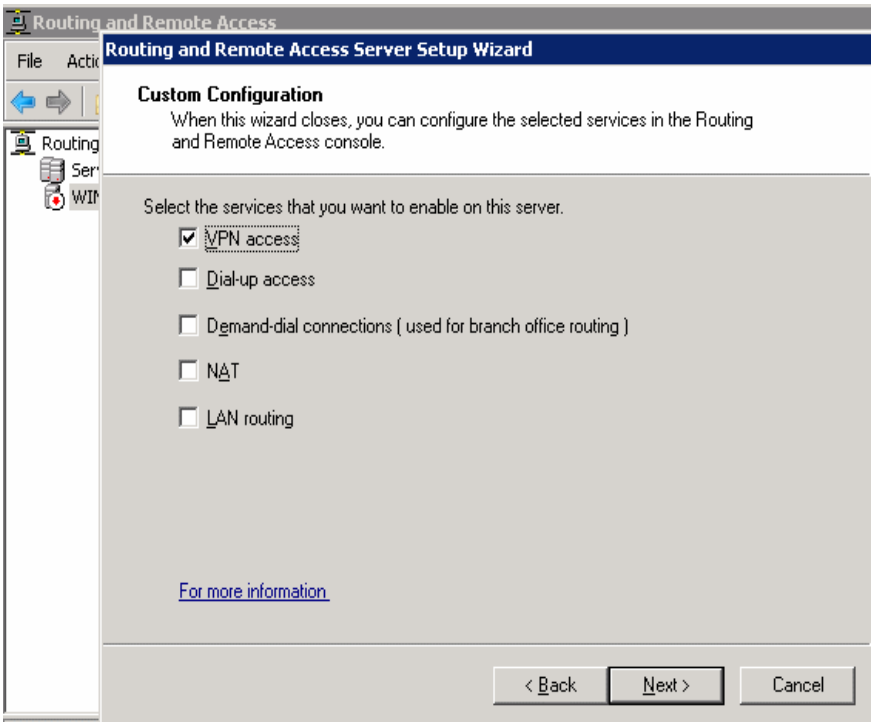
✘ To configure **RRAS**, open the **Server Manager**, expand the **Roles** node in the left pane of the console. Expand the **Network Policy and Access Services** node and click on the **Routing and Remote Access** node. Or you can go to **Administrative Tools**>**Routing and Remote Access.** Right click on the **Routing and Remote Access** node and click **Configure and Enable Routing and Remote Access**



✘ . If you have just one NIC, Select **Custom configuration**.



✘ After click **Next**, select **VPN access**.

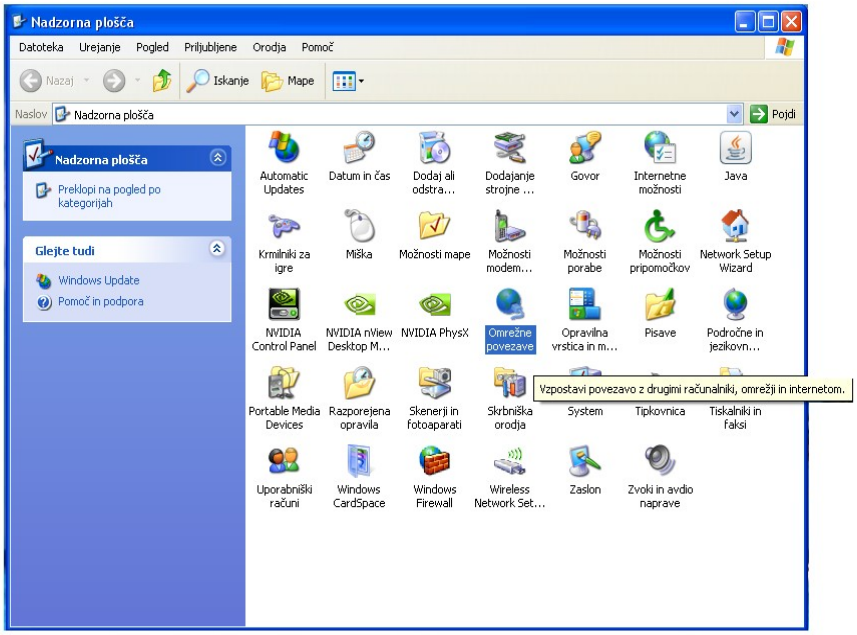


- Follow the instruction to finish the configuration.

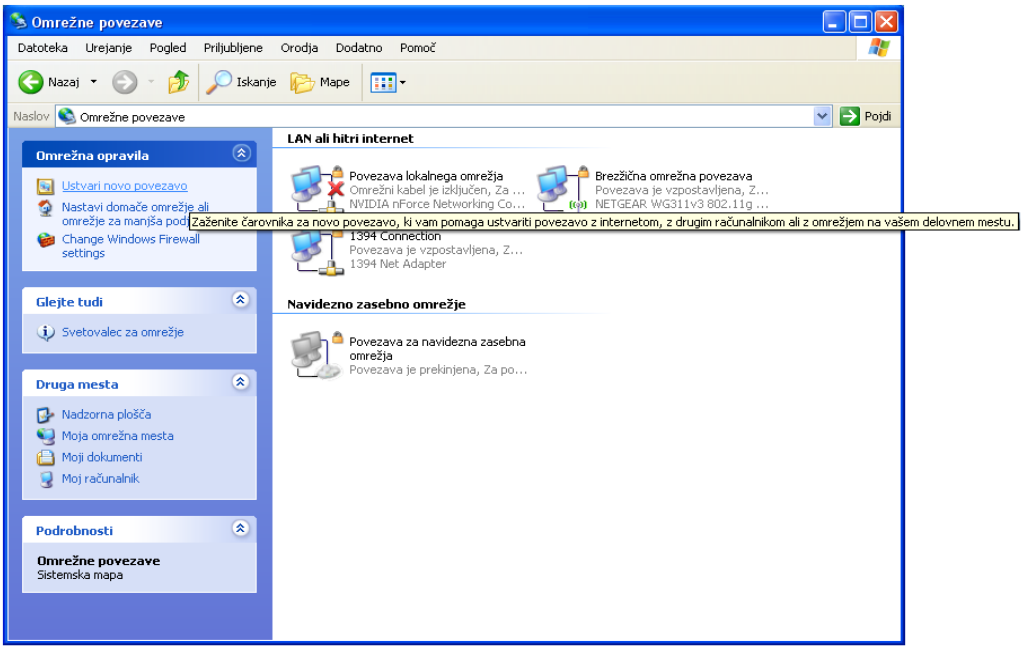
KONFIGURIRANJE POVEZAVE VPN (na klientu)

- Kliknmo **Start** in nato **Nadzorna plošča**.

✘ Na nadzorni plošči dvokliknite **Omrežne povezave**.

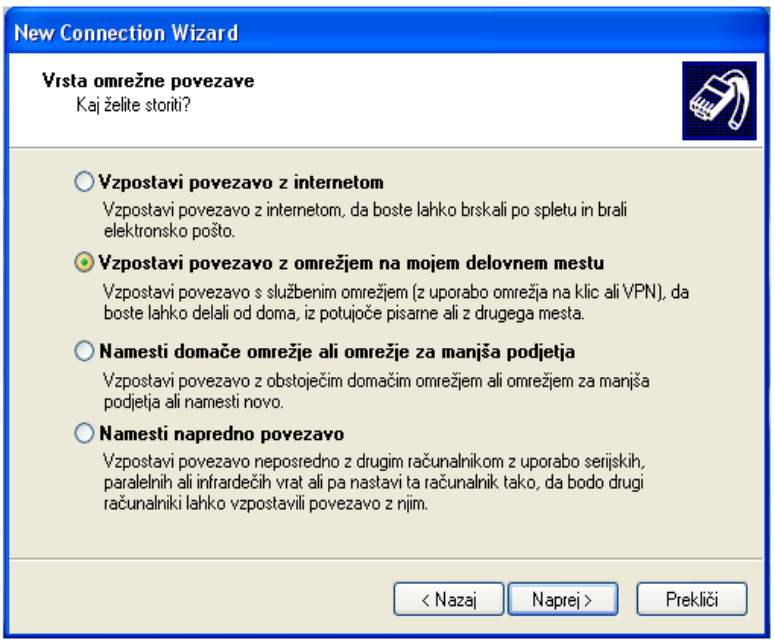


✘ Kliknemo **Ustvari novo povezavo**.

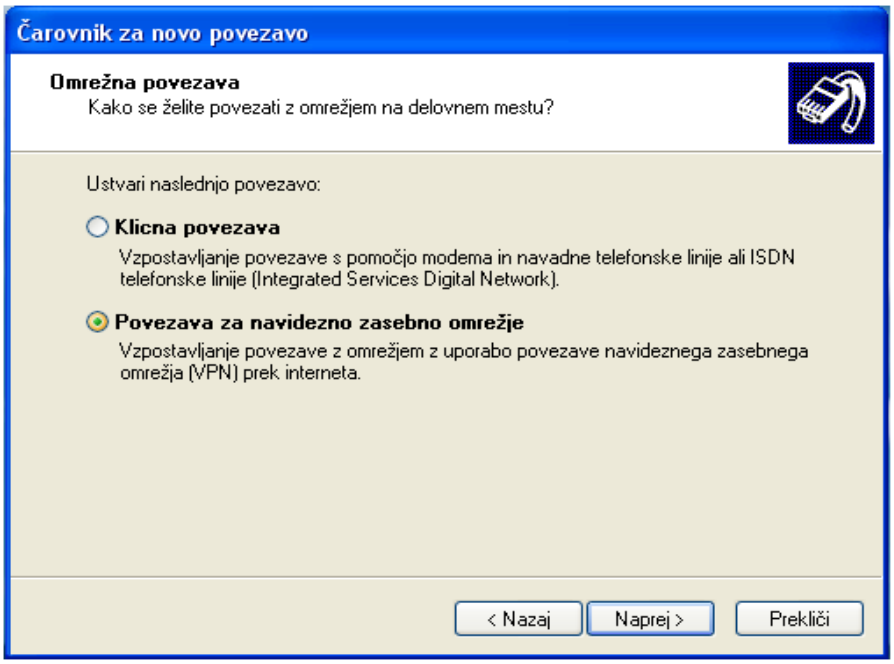


✘ V čarovniku za novo povezavo kliknite **Naprej**.

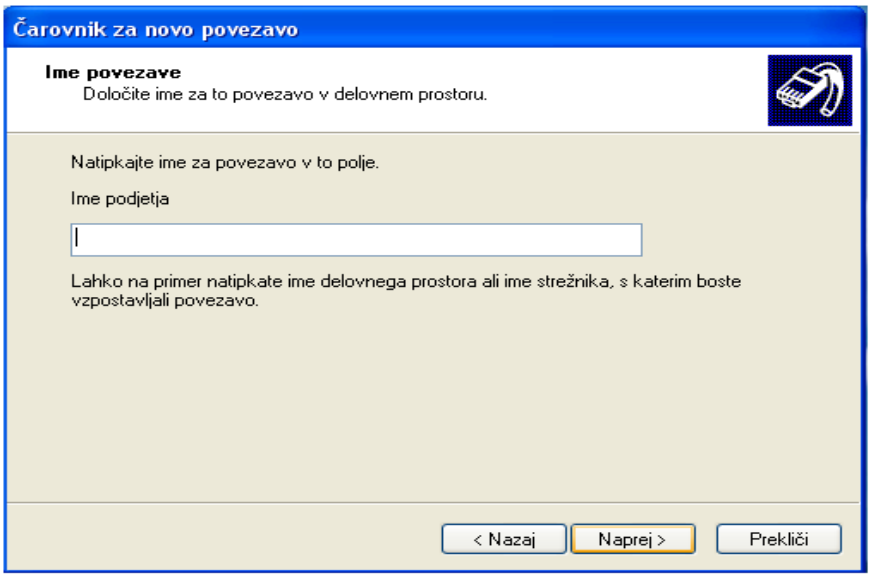
✘ Kliknemo **Vzpostavi povezavo z omrežjem na mojem delovnem mestu** in nato še **Naprej**.



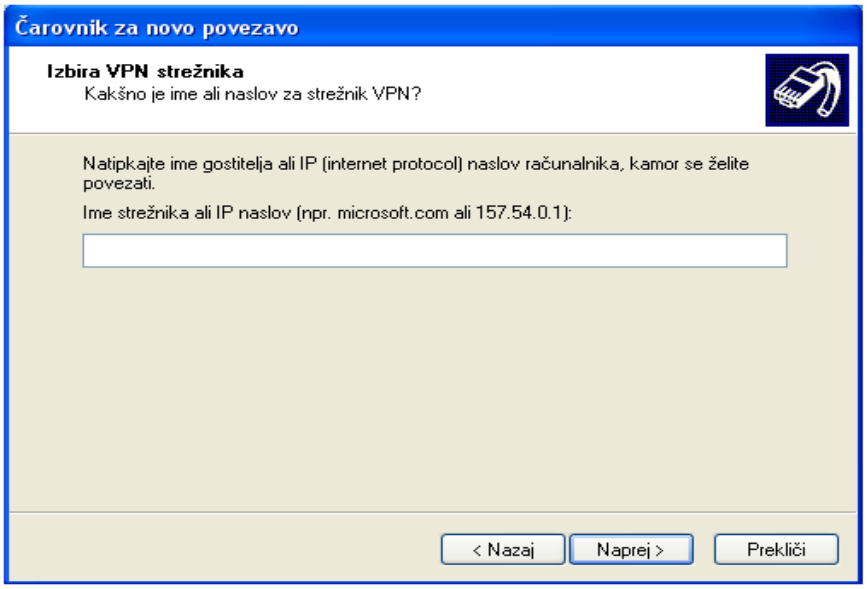
✘ Kliknemo **Povezava za navidezno zasebno omrežje** in nato še **Naprej**.



✘ Vnesemo i**me podjetja ali opisno ime za povezavo** in nato kliknemo **Naprej**.

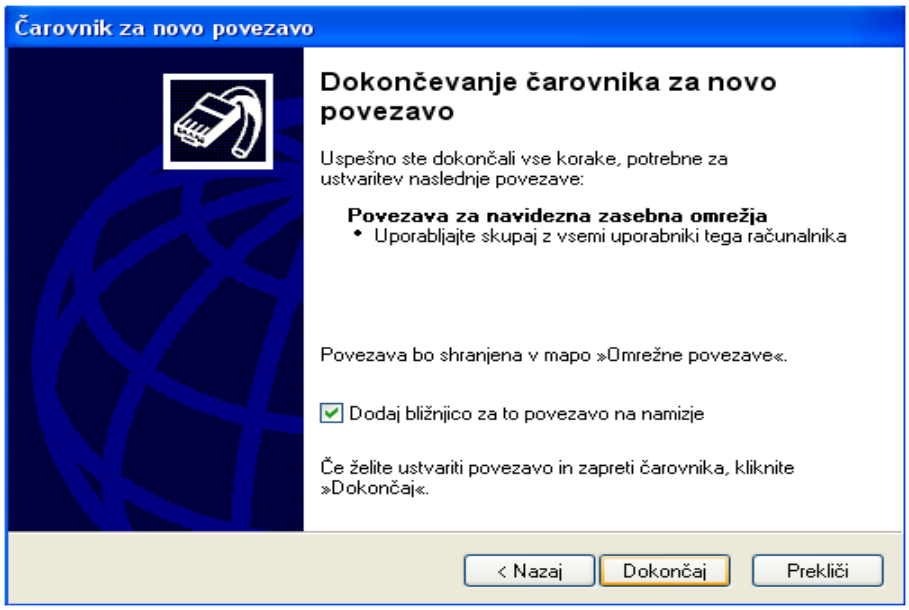


- **Vnesemo ime gostitelja ali naslov IP računalnika**, s katerim želimo vzpostaviti povezavo, in nato kliknemo **Naprej**.



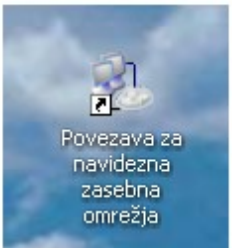
- Če želimo, da je povezava na voljo vsem, ki se prijavijo v računalnik, kliknemo Lahko jo uporabljajo vsi, če pa želimo, da je na povezava na voljo le takrat, ko se v računalnik prijavite sami, kliknemo Samo za mojo uporabo in nato kliknemo **Naprej**.

- Če želimo ustvariti bližnjico na namizju, izberemo potrditveno pole **Dodaj bližnjico za to povezavo na namizje** in nato kliknemo **Dokončaj**.



VZPOSTAVITEV VPN POVEZAVE

- dvokliknete na ikono na namizju oz **Start**, pokažite na Poveži se in nato med možnimi povezavami izberemo **našo VPN povezavo**

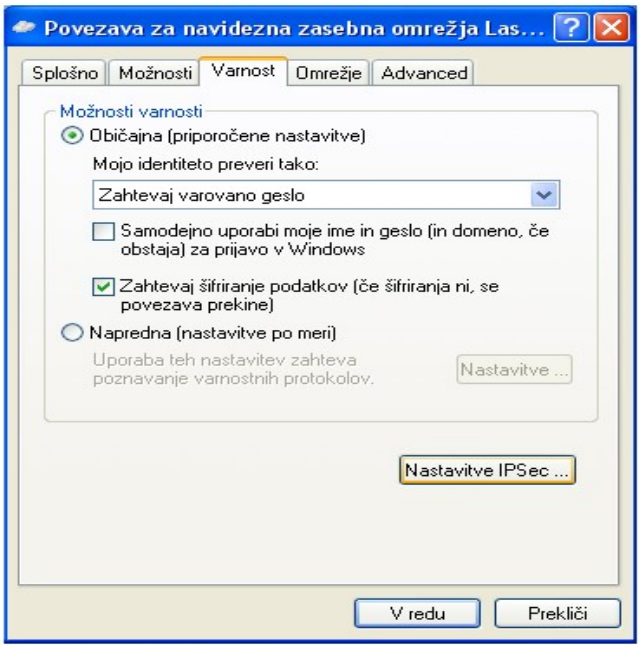


- Prikaže se nam obrazec za vzpostavitev povezave: Vanj vpišemo uporabniško ime , geslo in ime domene. Kliknemo na **Lastnosti** Nato kliknemo na gumb **Poveži**.

- ✘ Izberemo zavihek Varnost. In preverimo če imamo:

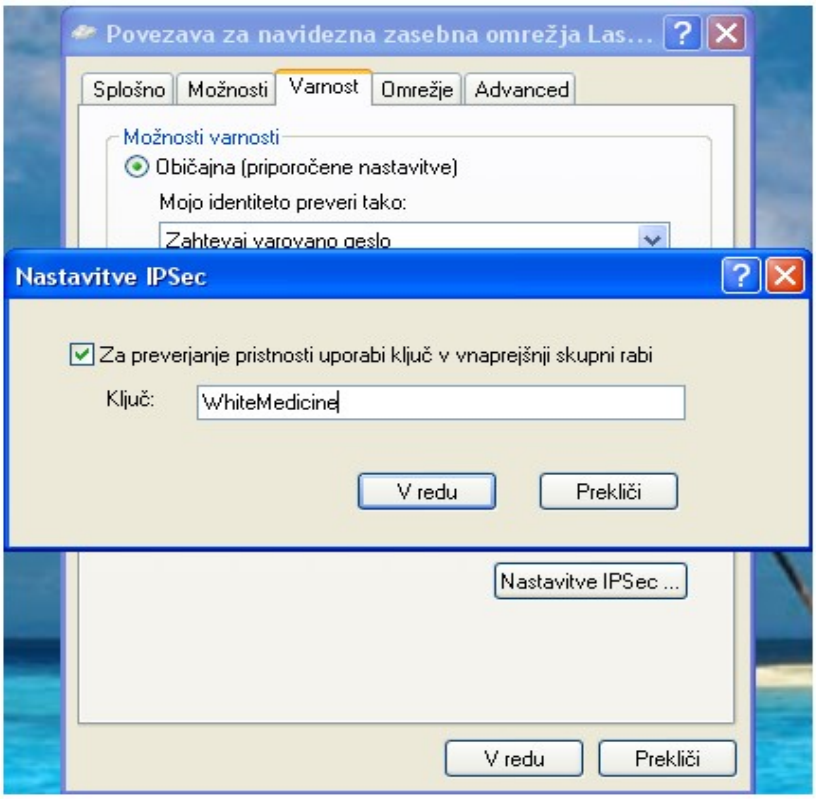
- Običajna (priporočene nastavitve)

- Zahtevaj šifriranje podatkov.

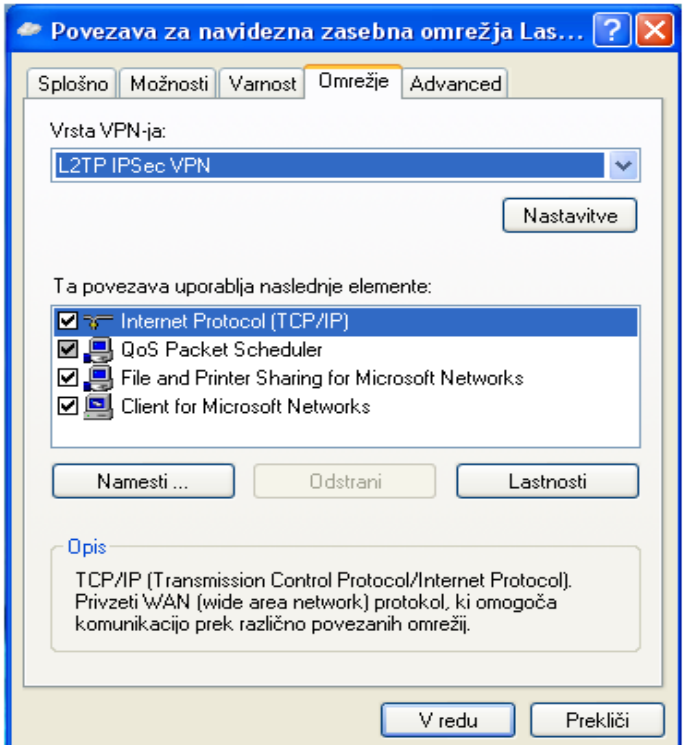


Potem kliknemo še na **Nastavitve IPSec**

- Damo klikico na Za preverjanje prisotnosti uporabi ključ vnaprejšnji skupni rabi**.** Vpišemo želen ključ za avtanikacijo: In **V redu**.

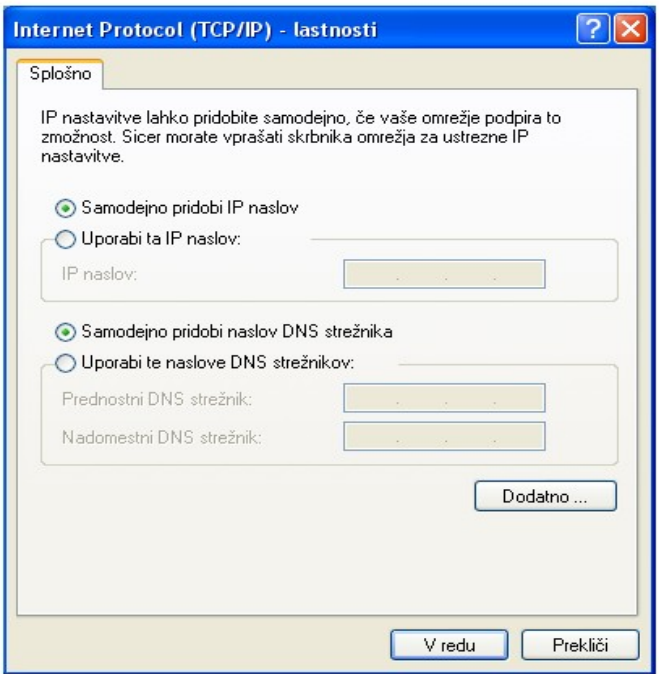


✘ Kliknemo na zavihek Omrežje. Vrsta VPN-ja izberemo **L2TP IPSec VPN**. Kliknemo **Internet Protocol (TCP/IP)** in izberemo Lastnosti

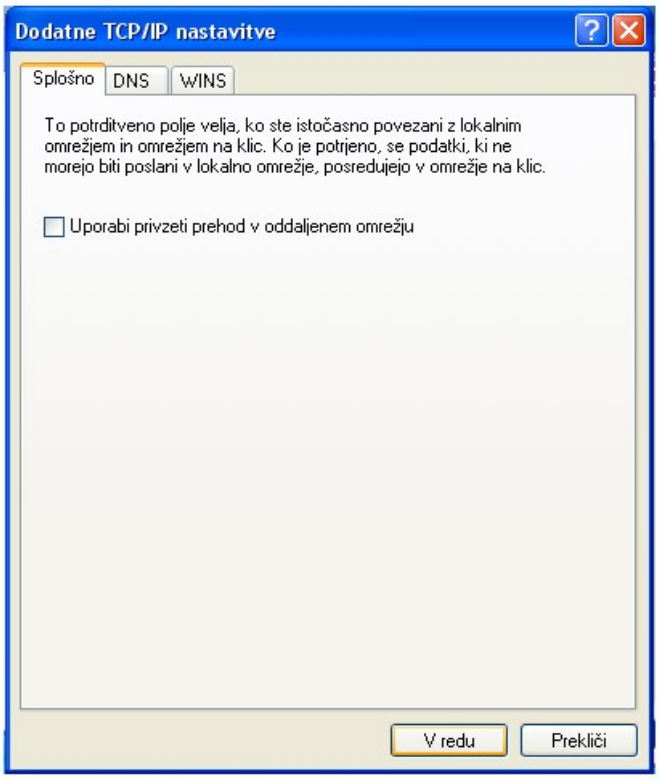


✘ *Preverimo če imamo označeno na*, kliknemo na Dodatno**.**

- Samodejno pridobi IP naslov
- Samodejno pridobi naslov DNS strežnika



✘ V zavihku **Splošno**. Odznačimo ***Uporabi prevzeti prehod v oddaljenemu omrežju***. In potrdimo s klikkom na **V redu**



- spodnjem desnem kotu prikaže nova ikona povezave v obliki dvojnega računalnika. To pomeni, da se je vaš računalnik preko VPN povezave uspešno povezal na omrežje podjetja.
- Za prekinitev VPN povezave z desno miškino tipko kliknite na ikono povezave in nato kliknite izbiro **Prekini povezavo**.

SKLEP

Z VPN-jem tako lahko dostopamo iz zunanjega omrežja v službeno omrežje hitro in enostavno. Je dokaj varna povezava med omrežjema. Seveda moramo vse podatke ki jih prenašamo med omrežjema kodirati. Sama namestitev ni problem. Problem lahko nastane s požarnim zidom, ki morda nima odprtih več portov(vrat).

LITERATURA IN VIRI

http://www.depts.ttu.edu/ithelpcentral/solutions/vpn/xp/index.php

http://www.i19777.net/forum/showthread.php?t=5485

http://support.microsoft.com/kb/314076

http://en.wikipedia.org/wiki/Virtual_private_network

http://support.microsoft.com/kb/314076

http://www.davidorlo.com/?tag=server-2008-vpn