

## Varnost omrežij

### 1 Orodja za spremljanje prometa v omrežju

Zagotavljanje varnosti komunikacij in omrežij si težko zamišljamo brez zmogljivih orodij za spremljanje stanja in prometa (dogajanja) v omrežju in vanj priključenih napravah.

#### *Orodja ukazne vrstice Windows*

Namenjena so predvsem za preverjanje in spreminjanje omrežnih nastavitev računalnika. Med najbolj uporabnimi so:

- ipconfig
- netstat
- net

#### *Naloge:*

Odprite ukazno vrstico računalnika in izvedite spodnje naloge:

1. Z ukazom **ipconfig -?** preverite vse možnosti tega orodja.
  - a. Poiščite ukaz s katerim izpišete vse podrobnosti mrežnih vmesnikov vašega računalnika.
  - b. Poiščite in uporabite ukaz s katerim ponastavite mrežne nastavitve računalnika.
2. Z ukazom **netstat -?** preverite vse možnosti tega orodja.
  - a. Poiščite ukaz s katerim izpišete statistiko na vmesniku Ethernet.
  - b. Izpišite samo aktivne TCP povezave.
  - c. Izpišite usmerjevalno tabelo računalnika.
  - d. Izpišite kateri programi sodelujejo v vzpostavljenih povezavah.
3. Z ukazom **net help** preverite vse možnosti tega orodja.
  - a. Z ukazom **net use** preverite uporabo mrežnih virov.
  - b. Z ukazom **net view** preverite kateri računalniki so priključeni v omrežje.
  - c.

#### *Analizator prometa in protokolov Wireshark*

Za analizo prometa na računalniku priključenem v omrežje, uporabimo program Wireshark. Če ga na računalniku še ni, ga prenesemo s strani <http://www.wireshark.org/> in namestimo.

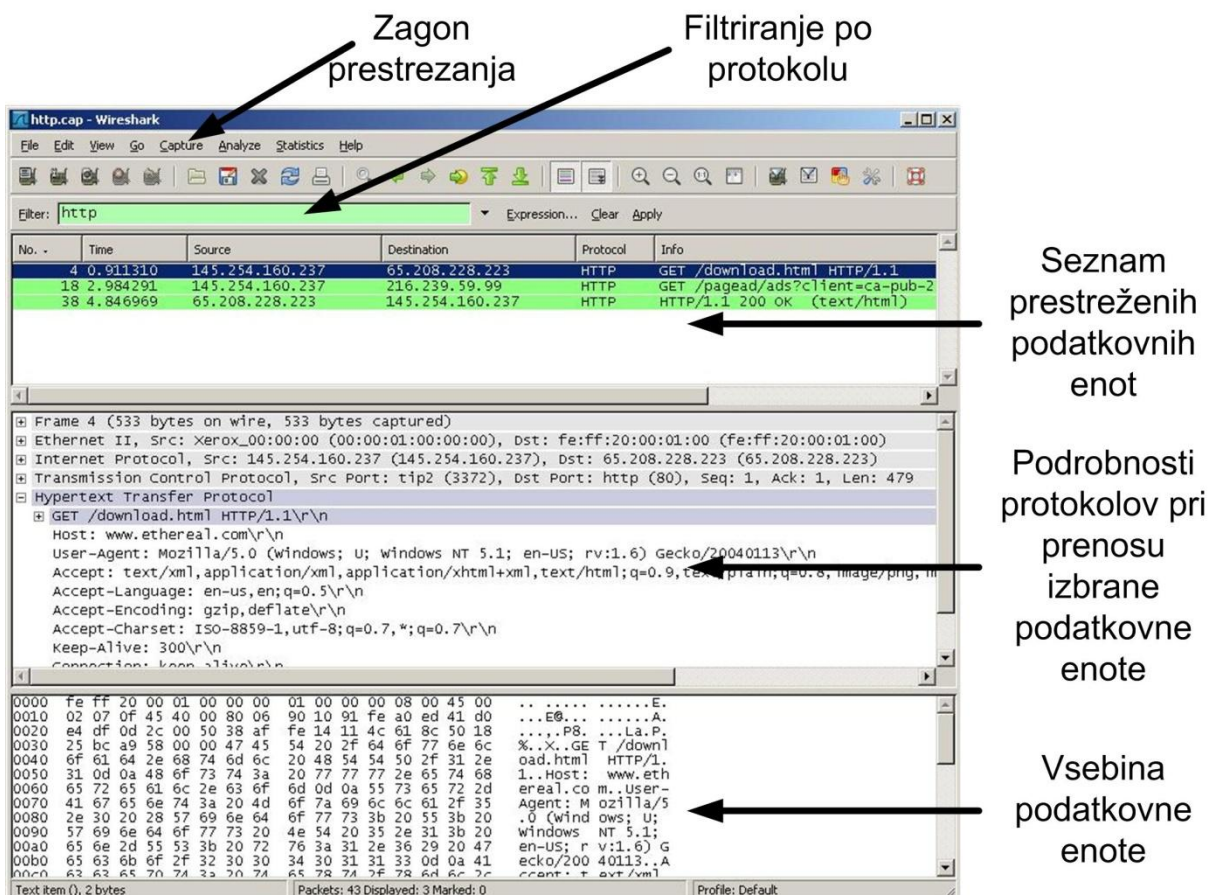
#### *Prestrezanje prometa*

- a. Najprej določimo mrežni vmesnik na katerem bomo prestrezali promet: izvedemo ukaz **Capture|Interfaces** in izberemo želeni vmesnik (v našem primeru bo to mrežna kartica Ethernet).
- b. Prestrezanje prometa začnemo z ukazom **Capture|Start** ali klikom na ustrezno ikono v orodjarni.
- c. Prestrezanje zaključite s **Capture|Stop** ali klikom na ustrezno ikono v orodjarni.

Uporaba preprostih filtrov

Wireshark omogoča filtriranje prometa ob zajemu (capture) in ob prikazu (display). Slika 1 prikazuje uporabo prikaznega filtra, ki na zaslon prikaže samo podatkovne enote protokola HTTP. Bolj zahtevne filtre lahko naredimo tako, da kliknemo na gumb **Expression** in izberemo pogoje filtriranja.

Slika 1 prikazuje prestrežen promet in nekatere podrobnosti protokolov in podatkovnih enot.



Slika 1: Analizator prometa in protokolov v omrežju (Wireshark).

Naloge:

1. Izdelajte filter, ki prikaže podatkovne enote protokola IP, ki imajo izvor ali cilj na vaši številki IP.
2. Izdelajte filter, ki prikaže komunikacijo z vašega računalnika na TCP port 80.

## 2 Prestrežanje nezavarovanih podatkov

Prenos nešifriranih podatkov preko nezavarovanih prenosnih poti je (lahko) nevarno početje. Poglejmo si dva primera prestrežanja nezavarovanih podatkov. Pri vseh primerih uporabimo program Wireshark.

### *Prestrežanje gesla na nezavarovani povezavi*

Poskusili bomo prestreči geslo uporabnika ob njegovi prijavi na strežnik FTP. Uporabili bomo program Wireshark in prestregli podatke prijave uporabnika na nezavarovani povezavi v lokalnem omrežju.

#### **Podatki o strežniku FTP:**

naslov IP: 212.235.190.214  
vrata: 2121  
uporabnik: vaje  
geslo: varkom

#### *Naloge:*

1. Nastavite prikazni filter tako, da bo prikazoval le podatkovne enote, ki se izmenjajo med našim računalnikom in strežnikom FTP.
2. Poženite prestrežanje prometa in se prijavite na strežnik FTP
3. Odjavite se s strežnika FTP in končajte s prestrežanjem prometa.
4. V prestreženih podatkovnih enotah poiščite uporabniško ime in geslo s katerim ste se prijavili na strežnik FTP.

### *Prestrežanje spletnih strani*

Poskusili bomo prestreči ogledano spletno stran, ki deluje po protokolu HTTP. Ker prenos podatkov preko HTTP povezave ni zavarovan, ima vsakdo možnost prestreči promet med vašim računalnikom in spletnimi strežniki in tako dobi vpogled v vsebino komunikacije.

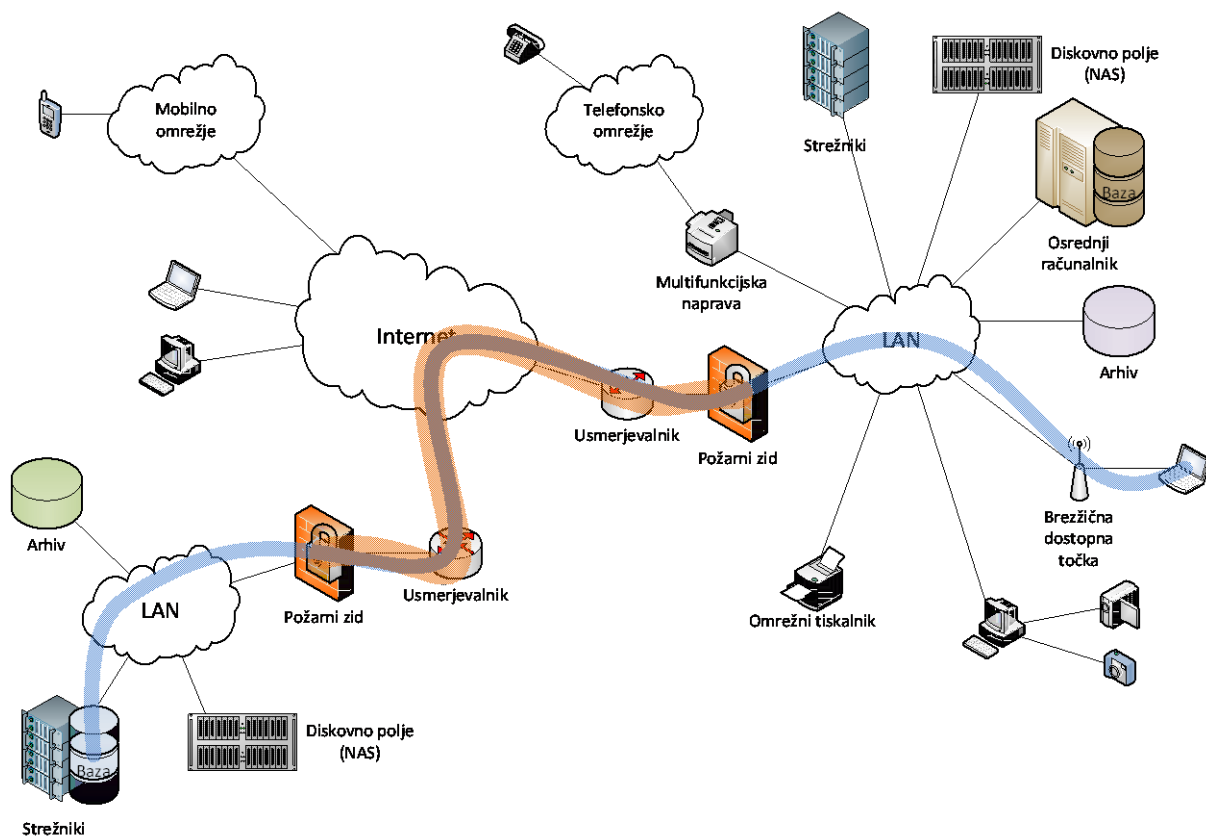
#### *Naloge:*

1. Zaženite spletni brskalnik in počistite zasebne podatke (zgodovino, piškotke itd.).
2. Poženite prestrežanje prometa.
3. Filtrirajte podatke po protokolu HTTP.
4. Ugotovite kateri IP naslov ustreza vašemu računalniku in kateri je naslov strežnika, ki vam je posredoval spletno stran.
5. Viri, ki jih je spletni strežnik poslal vašemu brskalniku, so označeni kot HTTP/1.1 200 OK (vrsta dokumenta). Izmed vseh virov, ki jih je spletni strežnik posredoval vašemu računalniku, izberite prvega, ki se nanaša na HTML dokument (text/html) (Slika 2).
6. Z desnim miškinim gumbom kliknite na »line-based text data« v srednjem oknu in izberite **Copy | Bytes | Printable Text Only**.
7. Kopiran tekst shranite v nov HTML dokument in ga odprite z brskalnikom.

### 3 Vzpostavljanje varnih prenosnih poti

Vzpostavljanje varnih prenosnih poti pride v poštev predvsem pri prenosu podatkov preko omrežij, ki niso naša last. Največkrat je primer prenos preko omrežja Internet. Varnostna tveganja lahko odpravimo z vzpostavitvijo navideznega zasebnega omrežja (VPN), ki se večinoma izvedejo s pomočjo vzpostavljanja tunelov.

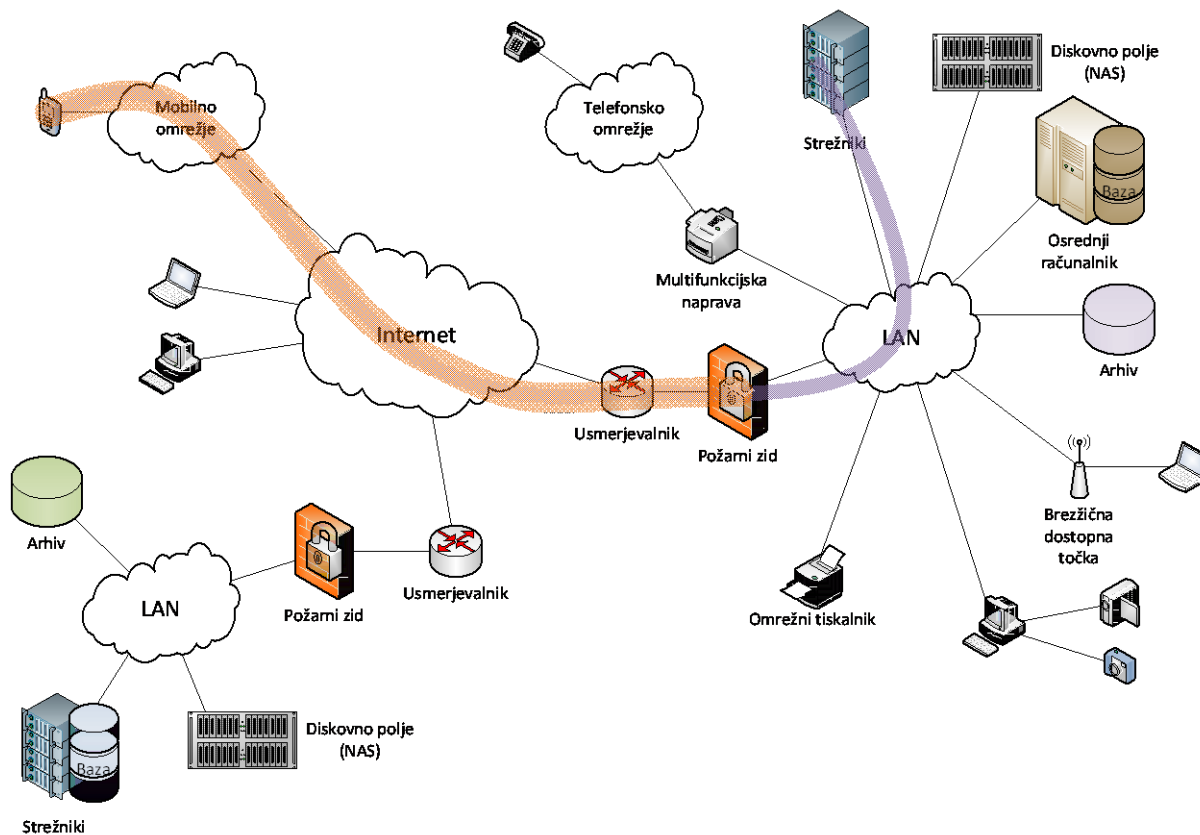
Slika 2 prikazuje primer, ko VPN vzpostavimo s pomočjo tunela med robnima usmerjevalnikoma ločenih delov zasebnega omrežja. Tipičen primer je povezovanje več oddaljenih lokacij nekega podjetja. Tunel je za promet transparenten in mora poskrbeti, da so podatki, ki se prenašajo skozenj, varni (šifrirani). Tunel je navadno vzpostavljen stalno.



Slika 2: Vzpostavitev tunela med robnima usmerjevalnikoma na ločenih delih zasebnega omrežja.

Slika 3 prikazuje primer, ko VPN vzpostavimo med končno napravo priključeno v (javno) oddaljeno omrežje in robnim usmerjevalnikom. Tipičen primer je povezovanje zaposlenih, ki se nahajajo na oddaljenih lokacijah, z zasebnim omrežjem podjetja. Tunel se navadno vzpostavi ob potrebi po izmenjavi podatkov in se po koncu le te poruši.

Obstaja cela množica načinov in protokolov za vzpostavljanje tunelov. Najpogosteje se uporablja protokol IPSec, ki izpolnjuje večino varnostnih zahtev, to je zaupnost, avtentičnost in verodostojnost podatkov, ki se prenašajo preko njega.



Slika 3: Tunnel med terminalom v (javnem) mobilnem omrežju in robnim usmerjevalnikom zasebnega omrežja.

### Vzpostavitev tunela in preverjanje njegove varnosti

Vzpostavili bomo IPSec tunel med dvema računalnikoma na lokalnem omrežju in preverili prenos podatkov skozenj.

#### Vzpostavitev tunela IPSec med Windows 7 računalniki

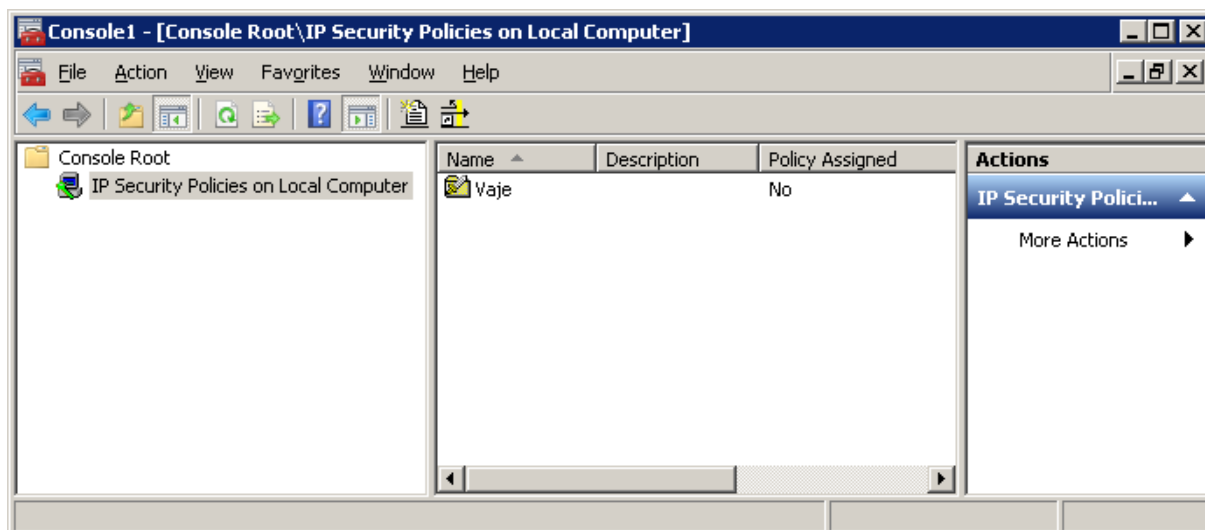
Za vzpostavitev tunela med dvema Windows 7 računalniki je potrebno vzpostaviti ustrezne IP varnostne politike.

Odpremo Windows MMC (Microsoft Management Console): pojdite na **Start Menu**, v iskalno okence odtipkajte **MMC** in pritisnite Enter. Odpre se konzola. Izberite ukaz **File | Add/Remove Snap-in** in s seznama izberete **IP Security Policy Management** ter izberete **OK**.

Izberete ukaz **Action | Create IP Security Policy** in sledite čarovniku. Izberete **Next**, kot ime varnostne politike vpišete **Vaje**, dvakrat pritisnete **Next** in zaključite s **Finish** in **OK**.

Slika 4 prikazuje stanje konzole po izvedbi zgornjega postopka.

**Vzpostavitev tunela IPSec naredite po navodilih asistenta.**



Slika 4: Vzpostavitev varnostne politike v Windows 7.

### Varen prenos podatkov skozi vzpostavljen tunel

Preden se lotimo pošiljanja podatkov skozi tunel, moramo preveriti ali med računalniki na končnih točkah tunela lahko vzpostavimo komunikacijo. To bomo preverili s pošiljanjem ICMP sporočil **ping**. Ker pa imajo Windows 7 računalniki v osnovi vključen požarni zid, ki ne dovoljuje odgovorov na ICMP sporočila, moramo vzpostaviti novo izjemo, ki bo znotraj lokalnega omrežja to dovoljevala. Izvedemo ukaze:

- **Control Panel --> System and security --> Windows Firewall --> Advanced settings --> Inbound rules --> New rule --> Custom rule,**
- zatem v meniju **Protocol and ports** na levi izberemo **Protocol type: ICMPv4,**
- kliknemo **Next** in v naslednjem oknu
  - za local IP address izberemo Any IP address in
  - za remote IP address vpišemo naše lokalno podomrežje 192.168.0.0/24,
- nekajkrat kliknemo Next, določimo ime ICMP local in izjema je vzpostavljena.
- S sosedom preverimo ali se njegov računalnik odziva na naše ping-e.

### Naloge:

1. Vzpostavite IPSec tunel med vašim in sosedovim računalnikom.
2. Preverite povezljivost med obema računalnikoma:
  - a. ko je tunel neaktiven,
  - b. ko je tunel aktiven.
3. Z analizatorjem Wireshark spremljajte promet med računalnikoma in ga filtrirajte tako, da:
  - a. boste spremljali samo promet protokola ICMP,
  - b. boste spremljali samo promet med obema računalnikoma,
  - c. boste zaznali promet skozi tunel.