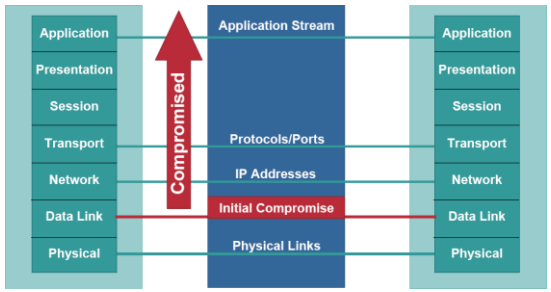
Varnostne naprave

Ljubljana, maj 2011

Umestitev varnostnih naprav

- Glede na sloje na katerem naprava oz mehanizem deluje
  - Ethernet stikalo, usmerjevalnik IP, požarna pregrada, sistem za preprečevanje vdorov (IPS), aplikacijski prehod
- Glede na varnostne funkcije in vrsto zaščite
  - Statični in dinamični filtri, proxy in snooping funkcije, poglobljen pregled vsebine
  - Zaščita kontrolne ravnine – npr. filtriranje sporočil IGMP
  - Zaščita podatkovne ravnine – npr. dovoljen dostopa do strežnika samo na TCP port 80
- Komunikacijski model OSI
  - posamezen sloj se ne zaveda "ogroženosti" drugega
  - varnost sistema je enaka varnosti najšibkejšega člena



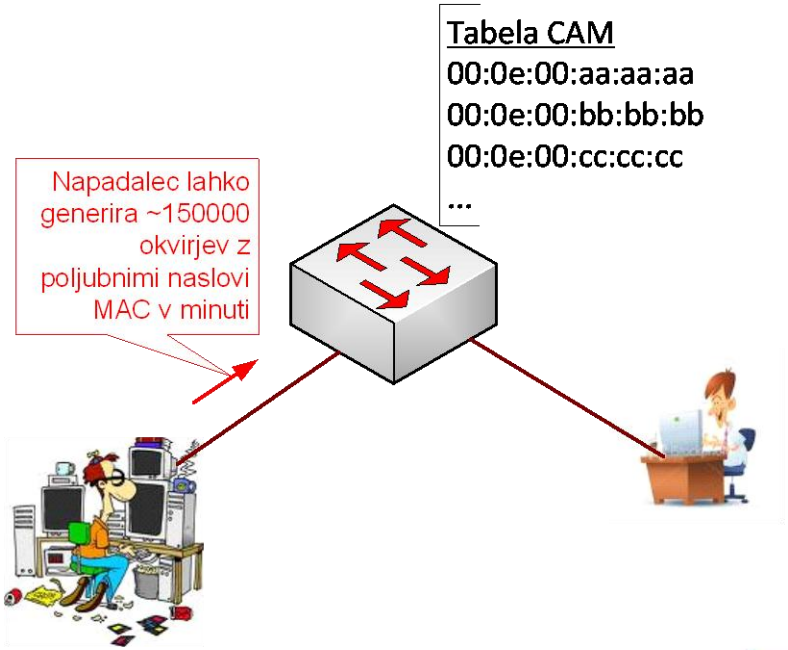
Ethernet varnostni mehanizmi

Napadi na Ethernet mehanizme

- Tipični napadi
  - poplavljanje tabele MAC
  - VLAN hopping
  - zastrupljanje tabel ARP
  - napadi na DHCP

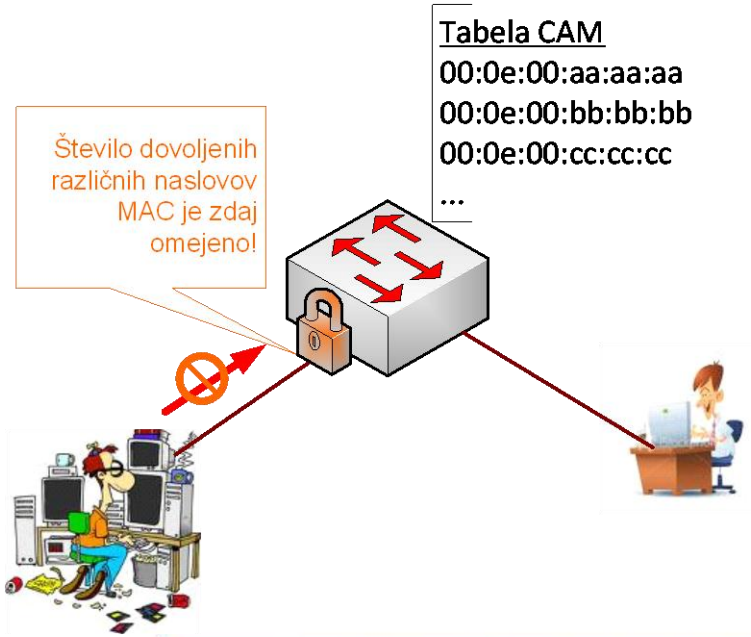
Manipulacije z naslovi MAC 1/2

- **Preplavljanje tabele MAC (angl. MAC Overflow)**
  - **napad izkorišča**
    - **način vpisovanja naslovov MAC v MAC-tabelo**
    - **končno velikost tabele MAC**
  - **stikalo posreduje ves promet, ki je namenjen na neznani naslov MAC (neznani izhoden vmesnik) na vse aktivne izhodne vmesnike**
  - **stikalo preide v HUB način delovanja**



Manipulacije z naslovi MAC 2/2

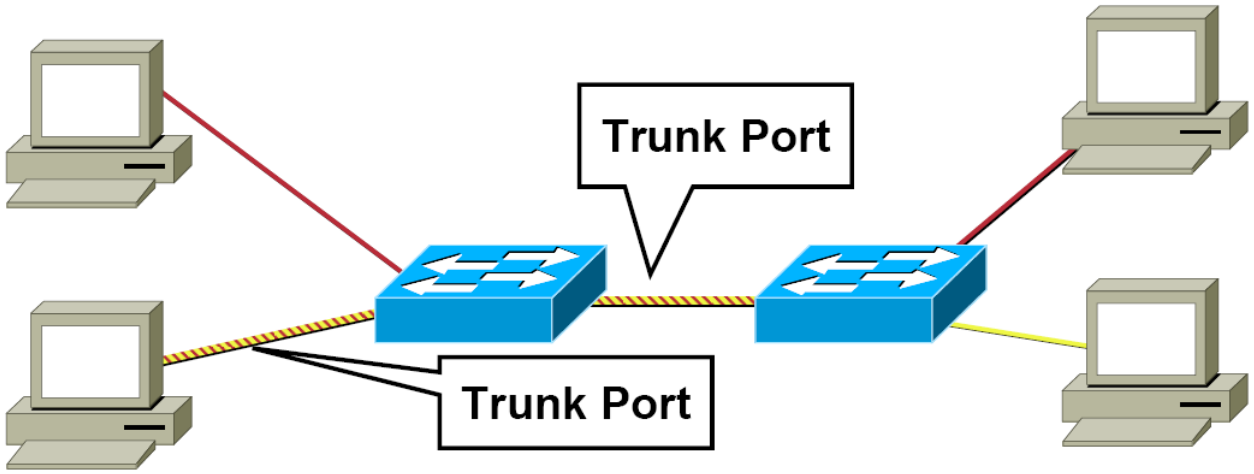
- Zaščitni mehanizem
  - PORT SECURITY
    - omejuje število MAC-naslovov, ki jih lahko stikalo registrira na posameznem vmesniku
    - določa obnašanje vmesnika v primeru poskusa preseganja limite
      - dekativacija vmesnika
  - Filtriranje naslovov MAC
    - kreirajo se pravila za filtriranje Ethernet okvirjev glede na naslove MAC-vira in/ali ponora



VLAN hopping

- Iskorišča lastnosti povezav tipa trunk
- Switch spoofing
  - napadalec predstavi svojo povezavo kot povezavo tipa trunk
  - s tem postane član vseh omrežij VLAN

- Zaščitni mehanizem
  - Pravilna implementacija in nastavitev stikala

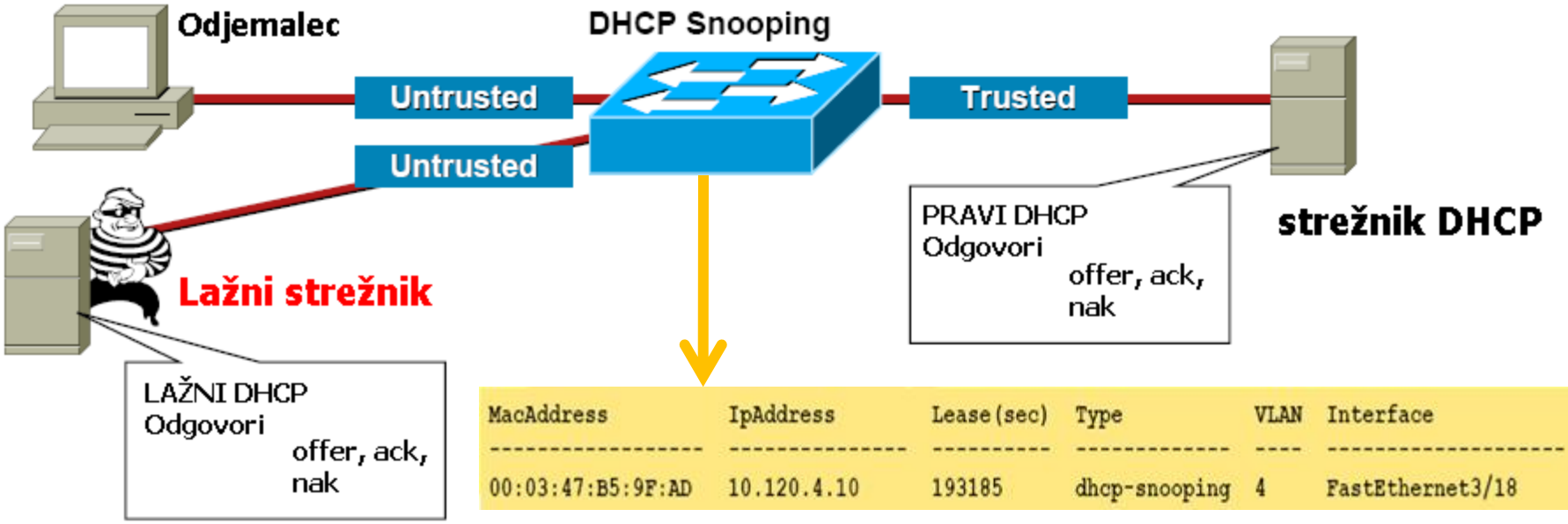


Napadi na DHCP

- "DHCP Starvation"
  - napadalec pošilja veliko število DHCP-zahtev z različnimi izvornimi naslovi MAC
  - strežnik DHCP izčrpa nabor naslovov, ki jih ima na voljo za dodeljevanje uporabnikom
    - napad tipa DoS – onemogočanje storitve DHCP
  - Zaščitni mehanizem
    - omejevanje števila različnih MAC-naslovov na posameznem vmesniku stikala Ethernet
- Kraja identitete strežnika DHCP "Rogue attack"
  - napadalec se predstavlja kot strežnik DHCP
  - dodeljuje nelegitimne nastavitvene parametre
  - lahko preusmeri promet na svojo napravo
  - Zaščitni mehanizem
    - DHCP snooping

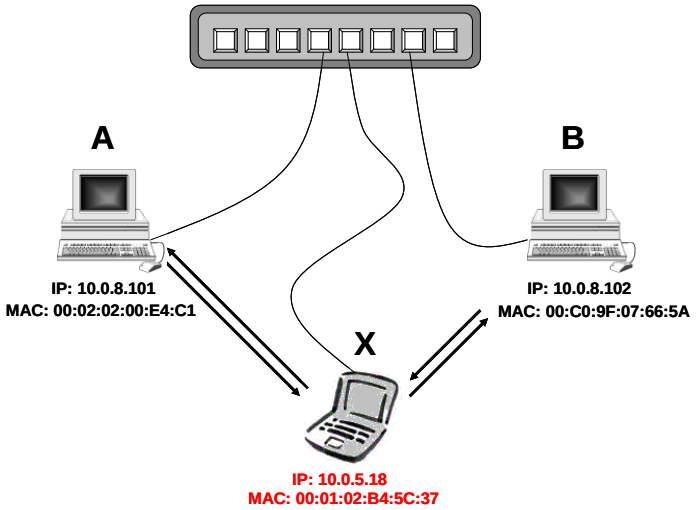
DHCP snooping

- Mehanizem implementiran na stikalu Ethernet
  - stikalo pregleduje vsebino sporočil DHCP
- Stikalo gradi dinamično tabelo o dodeljenih naslovih IP
  - Tabela gradi kombinacije vnosov MAC – IP, veljavnost dodeljenega naslova in druge parametre



Zastrupljanje tabele ARP 1/2

- **Zastrupljanje tabele ARP**
  - ustvarijo se napačne relacije med naslovi IP in MAC



Gostitelj	Naslov IP	Naslov MAC
A	10.0.8.101	00:02:02:00:E4:C1
B	10.0.8.102	00:C0:9F:07:66:5A
X	10.0.5.18	00:01:02:B4:5C:37

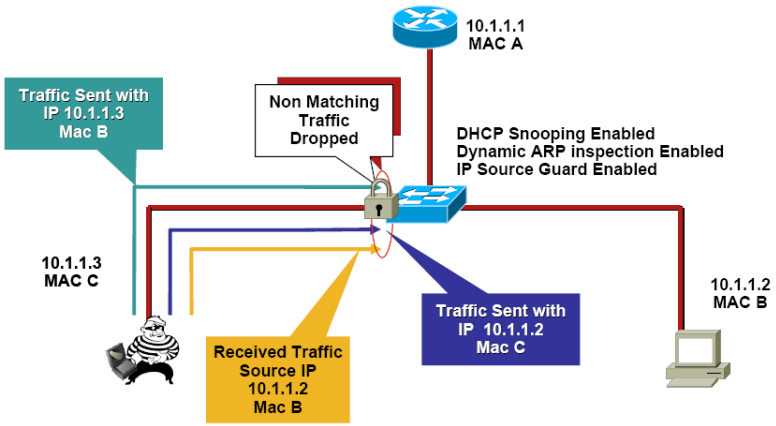
- **PC X izvaja napad zastrupljanja tabel ARP**
  - PC X posreduje nelegitimen odgovor ARP gostitelju PC A, v kateremu sporoča
    - "Jaz sem 10.0.8.102 (PC B), moj naslov MAC je 00:01:02:B4:5C:37"
  - PC X posreduje nelegitimen odgovor ARP gostitelju PC B, v kateremu sporoča
    - "Jaz sem 10.0.8.101 (PC A), moj naslov MAC pa se glasi 00:01:02:B4:5C:37"
  - Napadalec lahko pregleduje sporočila, ki si jih posredujeta gostitelja PC A in PC B

Zastrupljanje tabele ARP 2/2

- Zaščitni mehanizem “Dynamic ARP Inspection”
  - pregledovanje posredovanih sporočil ARP
  - izkorišča podatkovno bazo, ki jo gradi mehanizem “DHCP snooping”
  - dovoljuje ARP-sporočila z IP-MAC preslikavo, ki se ujema z vpisi v tabeli “DHCP snooping”

Spoofing

- Pošiljanje paketov z nelegitimnim izvornim naslovom
  - nelegitimen MAC
    - napadalec pošilja okvirje z nelegitimnim MAC-naslovom
  - nelegitimen IP
    - napadalec pošilja okvirje z nelegitimnim IP-naslovom
- Zaščitni mehanizem
  - IP Source Guard
    - pregleduje tabelo DHCP snooping za vsak paket, ki prehaja prek Ethernet stikala
    - pogleda že prisotne naslove: IP, MAC ali IP in MAC



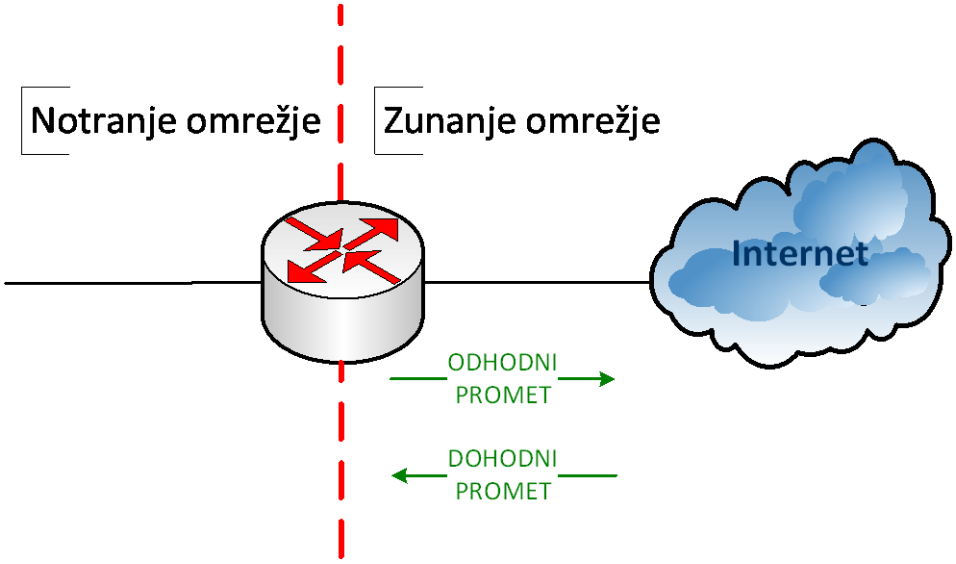
Varnostni mehanizmi IP

Varnostni mehanizmi IP

- **Dodatne varnostne funkcionalnosti omogočajo omrežnim napravam vpeljavo širokega nabora varnostnih storitev**
  - skrivanje naslovne sheme in topologije omrežja
    - mehanizem NAT in PAT na usmerjevalniku/požarni pregradi
  - nadzor dostopa do omrežja, naprav in omrežnih storitev na osnovi filtriranja prometa
    - Statični filtri na usmerjevalniku – filtri na naslove IP in port TCP/UDP
    - Dinamični filtri na požarni pregradi – filtri na naslove IP in port TCP/UDP
  - poglobljen pregled vsebine paketov, do aplikacijskega nivoja
    - Preverjanje ali je promet na vratih številka 80 (TCP) res HTTP
    - Sistemi IDS/IPS
  - emulacija odjemalcev
    - Aplikacijski prehodi, proxy naprave

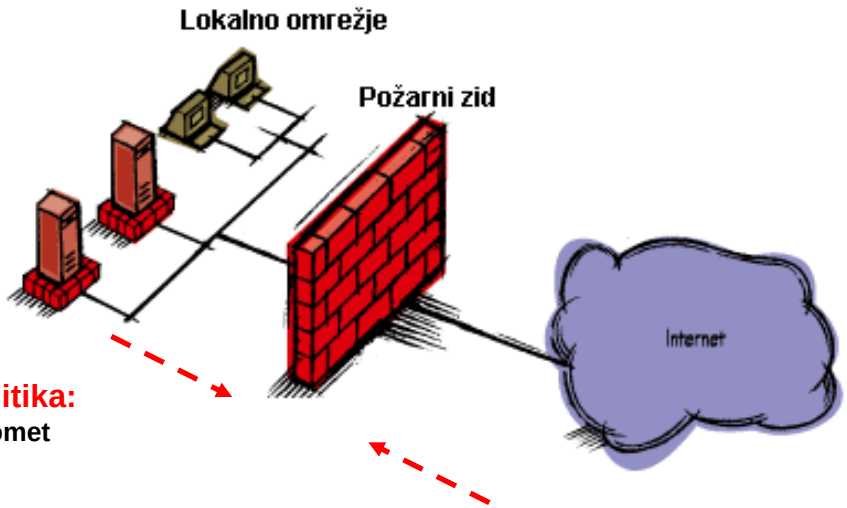
Filtri za nadzor dostopa

- Predstavljajo osnoven nivo kontrole prometnih tokov
- Na podlagi kriterijev (naslov IP, port TCP/UDP) določajo ali podatkovne enote (paket IP) posredovati naprej ali jih blokirati
  - odločitveni kriterij
    - izvorni/ponorni naslov IP, izvorna/ponorna številka vrata TCP/UDP in druge posebnosti protokolov
  - onovna naloga vključenega filtra
    - paket posreduj naprej
    - blokiraj paket



Požarni zid

- Loči lokalno omrežje od zunanjega omrežja
  - Zagotovi večji nivo varnosti uporabnikom v lokalnem omrežju
  - Namenska naprava oziroma funkcionalnost
  - Implementira se bolj "inteligentna" kontrola prometa



Odhodna politika:
- Dovoli ves promet

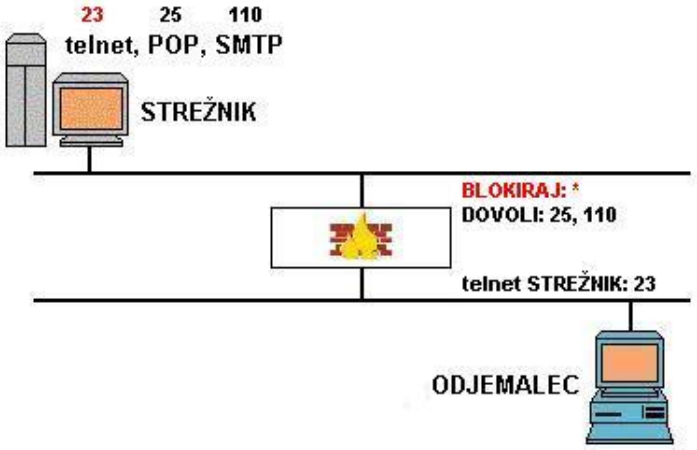
Dohodna politika:
- Dovoli ves promet, ki je bil vzpostavljen iz lokalnega omrežja
- blokiraj vse ostalo

Požarni zid

- Požarni zid je dober toliko, kot njegova varnostna politika
- Osnovne naloge:
  - dovoli
  - blokiraj
- Oblike implementacije:
  - namenska omrežna naprava
  - programski modul na gostitelju, ki komunicira z obstoječim skladom TCP/IP
- Delitev požarnih zidov:
  - paketno sito (Packet Filter)
  - sistem popolnega nadzora (Stateful Inspection System)
  - aplikacijski prehod

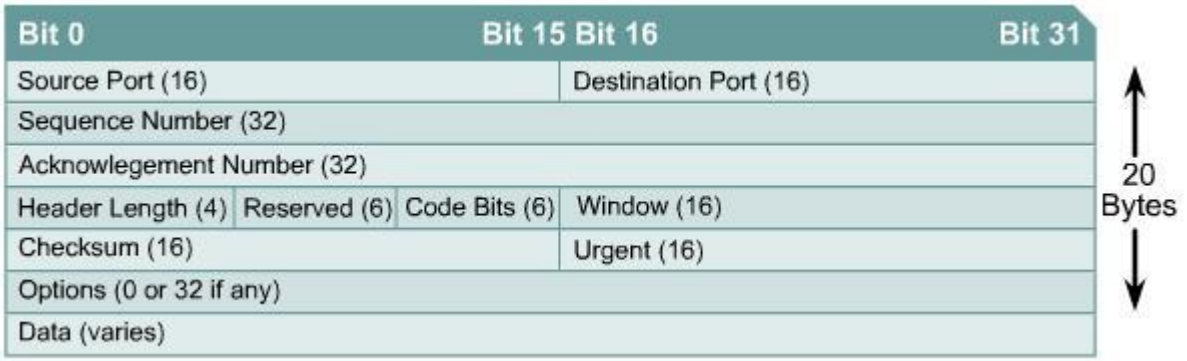
Požarni zid

- **Način kreiranja varnostne politike:**
  - vse, kar ni eksplicitno prepovedano, je dovoljeno
    - primer varnostne politike iz domačega omrežja v internet
  - vse, kar ni ekplicitno dovoljeno, je prepovedano
    - primer varnostne politike iz interneta v domače omrežje
- **Nastavitev varnostne politike glede na naslovov IP ter vrata TCP/UDP:**
  - Strežnik lahko gosti več storitev (npr. HTTP in FTP)
  - Požarni zid zapira / odpira ustrezna vrata (porte) do strežnika

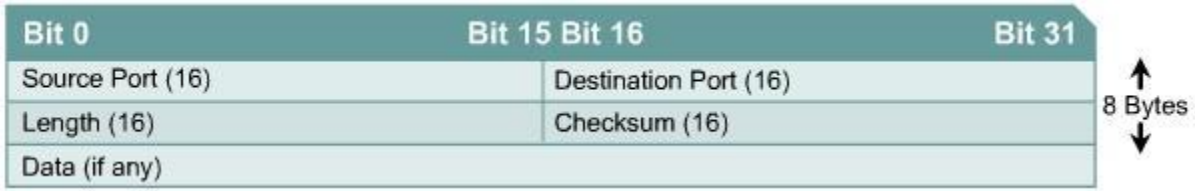


Požarni zid – zavedanje seje

- **Uporaba polja TCP SYN v zaglavju segmenta TCP:**
  - **dovoljene so le predhodno vzpostavljene zveze**
  - **pobudnik zveze postavi zastavico SYN, prenehanje zveze FIN**
    - **požarni zid poleg IP naslova in porta TCP/UDP pregleduje tudi vrednost zastavic SYN in FIN – zavedanje seje**



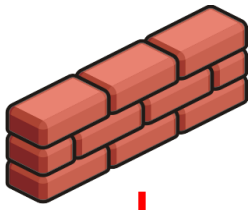
- **UDP je nepovezavno orientiran protokol:**
  - **uporaba časovnikov – UDP sej je odprta 30 sekund**



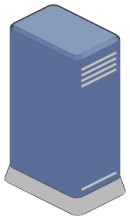
Požarni zid – zavedanje stanja seje

IP = 1.1.1.1

Domače omrežje



Internet



IP = 2.2.2.2

SYN = 1	S TCP = 2000 D TCP = 80	S IP = 1.1.1.1 D IP = 2.2.2.2

Zahteva za komunikacijo s spletnim strežnikom

Požarni zid zgradi tabelo z vnosom:
Dovoli zahteve iz interneta
SIP = 2.2.2.2 & DIP= 1.1.1.1
STCP = 80 & DTCP = 2000
Blokiraj vse ostale zahteve z interneta

S IP = 2.2.2.2 D IP = 1.1.1.1	S TCP = 80 D TCP = 2000	SYN = 1 ACK=1

Odgovor spletnega strežnika poslan odjemalcu

FIN = 1	S TCP = 2000 D TCP = 80	S IP = 1.1.1.1 D IP = 2.2.2.2

Rušenje povezave s spletnim strežnikom

Požarni zid pobriše tabelo

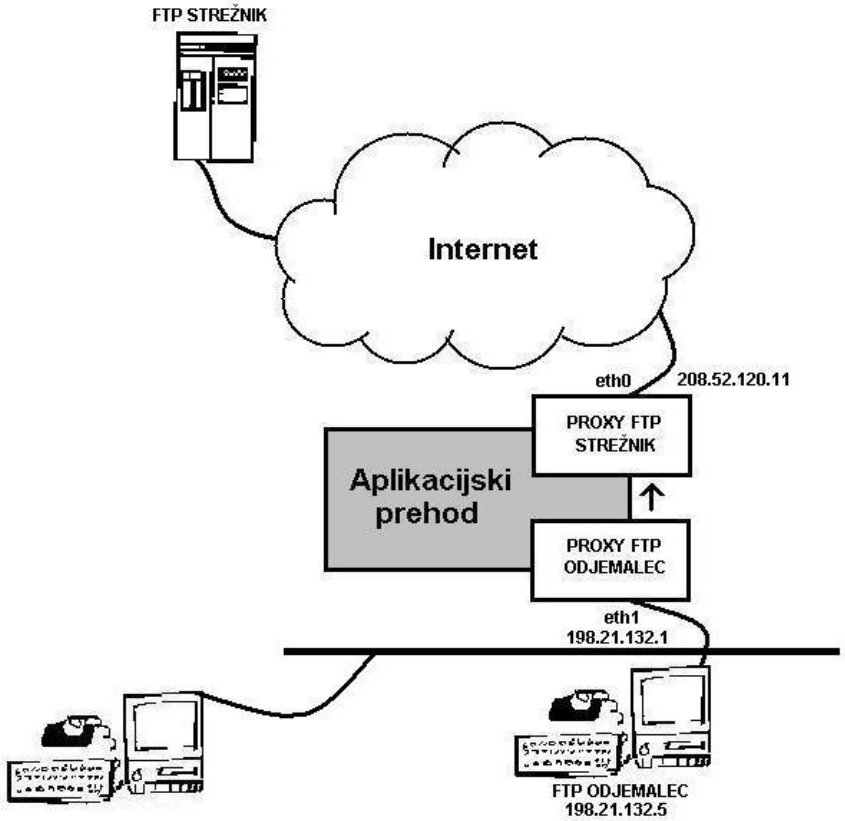
Blokiraj vse ostale zahteve z interneta

Spletni strežnik vzpostavlja sejo

S IP = 2.2.2.2 D IP = 1.1.1.1	S TCP = 80 D TCP = 2000	SYN = 1

Aplikacijski prehod - PROXY

- PROXY sistem = PROXY strežnik + PROXY odjemalec
- Vmesni element med strežniško in odjemalčevo aplikacijo
- Ni direktne komunikacije med entitetama



Demilitarized Zone - DMZ

- Omrežje DMZ v IT svetu – nevtralna cona med omrežjema
  - Trusted
  - Untrustred
- V DMZ območje se postavi javne stežnike (mail, splet ...)
- Pravila
  - DOVOLI PROMET IZ:
    - untrusted > DMZ
    - trusted > DMZ
    - trusted > untrusted
  - BLOKIRAJ PROMET IZ:
    - untrusted > trusted
    - DMZ > trusted