NII – pitanja za ispit

1. Grupe tokova saobraćaja.

- grupa korisničkog saobraćaja (nastaje/namenjen je za krajnje aplikacije; tranzitni)
  - računarske mreže postoje zbog ove grupe
  - sa tačke gledišta komunikacionih uređaja u pitanju je tranzitni saobraćaj
  - saobraćaj nastaje ili je namenjen korisničkim aplikacijama na krajnjim rubovima mreže
- grupa kontrolnog saobraćaja (konfiguracija kom. uređaja; protokoli dinamičkog rutiranja)
  - saobraćaj na osnovu kog se automatski podešava konfiguracija komunikacionih uređaja, odnosno same mreže
  - protokoli za dinamičko rutiranje su tipičan primer iz ove grupe
- grupa upravljačkog saobraćaja (administratori; nadgledanje komunikacionih uređaja)
  - saobračaj iz ove grupe posledica je procesa pristupa, nadgledanja i upravljanja komunikacionim uređajima od strane administratora i specijalizovanih softvera za administraciju mreža
- grupa servisnog saobraćaja (različite karakteristike, kriptovanje, zaglavlja, svaki deo servisa, tretman u tranzitne)
  - trenutna upotreba mreža podrazumeva postojanje velikog broja servisa koji se zasnivaju na IP saobraćaju sa različitim zahtevanim karakteristikama (različit tretman u tranzitu, kriptovanje, dodatna zaglavlja…)
  - u osnovi je u pitanju korisnički saobraćaj sa potrebom za posebnim tretmanom na komunikacionim uređajima (IPSec zahteva upotrebu modula za enkripciju, QoS zahteva dodatnu obradu zaglavlja i utiče na tretman ostalih grupa saobraćaja…)
  - postojanje ove grupe saobraćaja utiče i na kompleksnost grupa kontrolnog saobraćaja i upravljačkog saobraćaja

- kontrolni i upravljački – direktno utiču na funkcionalnost mreže
- svi – direktno utiču na funkcionalnost pojedinog servisa

- zašto upravljamo tokovima saobraćaja?
  - podizanje nivoa bezbednosti mreže
  - podizanje nivoa bezbednosti servisa
  - definisanje logičkih grupa: po servisima, po korisnicima, po organizacionoj strukturi
  - definisanje toka saobraćaja radi ostvarivanja specijalnog tretmana, fino definisanje tokova iz servisne grupe tokova saobraćaja
  -

- alati i mehanizmi za upravljanje tokovima saobraćaja [prenosni, mrežni, transportni, aplikativni]:
  1. filtriranje (mrežni, transportni i aplikativni nivo)
  2. prevođenje IP adresa = NAT-ovanje (mrežni nivo)
  3. SOCKS servis (transportni i aplikativni nivo)
  4. HTTP Proxy servis (aplikativni nivo)
  5. tuneliranje (prenosni, mrežni, transportni i aplikativni nivo)
  6. QoS = Quality of Service (prenosni i mrežni nivo)

2. Osobine kontrolnog saobraćaja.

- vidi pitanje 1

3. Ideja filtriranja saobraćaja.

- filtriranje je alat za upravljanje tokovima saobraćaja. Osnovna ideja je da se opiše tok saobraćaja (ili skup tokova saobraćaja) i da se definiše akcija koja se primenjuje na paketu koji

pripada nekom toku ili skupu tokova saobraćaja. Može se vršiti na svim uređajima koji se povezuju u računarske mreže – na korisničkim i na komunikacionim uređajima.

4. Objasniti metodu filtriranja uz pomoć refleksivnih ACL-a.

- refleksivne ACL = stateful filtriranje. Uvodi se dinamika, privremeno filtriranje se aktivira u slučaju iniciranja sesije (TCP ili UDP) sa branjene mreže. Privremeno filtriranje omogućava da se doda privremeno pravilo u postojeću listu nad nekim interfejsom. Na ovaj način se u ulaznom smeru ka branjenoj mreži dopušta samo saobraćaj koji pripada iniciranoj sesiji. Privremeno pravilo se briše iz liste po završetku sesije. Ograničenje je to što nema podršku za aplikacije koje u toku sesije barataju sa tokovima čiji se portovi menjaju (sesija je skup koji ima više od dva elementa).

5. Funkcija NAT posrednika je?

- NAT posrednik vrši preslikavanje između skupova IP adresa. Na spoju mreže sa okruženjem može da menja adresna polja IP paketa i da zapamti kakve su izmene izvršene.

6. Kako se formira tabela preslikavanja (bira adresa) u slučaju dinamičnog NAT-a?

- skup IP adresa sa unutrašnje mreže preslikava se na skup adresa sa spoljašnje mreže. Postoje dva načina: preslikavanje 1 na 1 i preslikavanje „NA“ (nastaje radom – dinamički).
- koraci:
  1. definiše se interfejs preko koga je povezana unutrašnja mreža
  2. definiše se interfejs preko koga je povezana spoljašnja mreža
  3. definiše se skup spoljašnjih IP adresa na koje će se preslikavati unutrašnje (IP nat pool)
  4. definišu se unutrašnje IP adrese za koje će se vršiti preslikavanje (preko access-list)
  5. unutrašnja IP adresa se preslikava na prvu slobodnu IP adresu iz nat pool-a

7. Nacrtati jedan primer tabele preslikavanja u slučaju dinamičnog NAT-a.

- 1 na 1 → tabela preslikavanja formira se dinamički i sadrži osnovni zapis:

IP adresa unutrašnje mreže	*Polazni port (TCP/UDP)*	*Dodeljena IP adresa spoljašnje mreže*	*Dodeljeni polazni (TCP/UDP) port*
1.1.1.1		2.2.2.1	
1.1.1.2		2.2.2.2	

- NA → tabela preslikavanja formira se dinamički i sadrži prošireni zapis:

IP adresa unutrašnje mreže	*Polazni port (TCP/UDP)*	*Dodeljena IP adresa spoljašnje mreže*	*Dodeljeni polazni (TCP/UDP) port*
1.1.1.1	24569 (TCP)	2.2.2.2	2000 (TCP)
1.1.1.2	34567 (TCP)	2.2.2.2	2001 (TCP)

8. Koja su poboljšanja uvedena SOCKS verzijom 5 u odnosu na verziju 4?

- SOCKS servis omogućava upravljanje tokovima saobraćaja. Upravljanje se vrši između transportnog i aplikativnog nivoa. SOCKS servis podrazumeva postojanje SOCKS servera i SOCKS klijenta. Kod verzije 4 je podržan samo TCP i loši su mehanizmi za pouzdano slanje lozinke. Verzija 5 pruža podršku za rad sa UDP i ima znatno poboljšane mehanizme za autentifikaciju. Podrška za rad: IPv4, IPv6; TCP, UDP; metode autentifikacije; enkripcija – DES, 3DES, IPSec; tuneliranje – PPTP, L2TP; razmena ključeva – SKIP, ISAKMP.

9. Šta se dobija upotrebom HTTP proxy servisa?

- u početku - dominantna upotreba *cache* funkcionalnosti koja je omogućavala:
  - podizanje kvaliteta HTTP servisa za krajnjeg korisnika
  - smanjenje troškova za *bandwidth* korisnika i ISP-a
- dodatno, ali ne manje bitno:
  - filtriranje (III, IV, V nivo)
  - autentifikacija i autorizacija
  - logovanje aktivnosti
  - shaping
  - odličan alat, koji zajedno sa drugim načinima upravljanja omogućava definisanje i primenu kompleksne politike upravljanja tokovima saobraćaja

10. Koje su mane transparentnog proksiranja?

- transparentno proksiranje je preusmeravanje HTTP konekcije od klijenta ka serveru ka HTTP proxy serveru bez klijentovog znanja. Prednosti su to što nema dodatne konfiguracije kod klijenta i to što ima više prostora za reakciju u slučaju da HTTP proxy ne radi.
- mane transparentnog proksiranja:
  - zahteva NAT (konfiguracija složenija, samim tim i verovatnoća za grešku u konfiguraciji cele mreže raste)
  - mogući problemi sa *Path MTU Dicovery* mehanizmom
  - problem u radu sa starijim verzijama HTTP klijenata
  - gubimo funkcionalnost autentifikacije i autorizacije na Proxy serveru
  - podrška samo za HTTP (SSL, FTP i drugi protokoli nemaju podršku)

11. Arhitektura tuneliranja.

- u slučaju kada se osnovna jedinica prenosa nekog protokola enkapsulira u osnovnu jedinicu prenosa protokola koji je prvi niži po referentnom modelu komunikacije, govorimo o klasičnoj (regularnoj) enkapsulaciji. “Spoljašnji” protokol je prvi niži u odnosu na “unutrašnji” protokol. Drugačije kombinacije “spoljašnjeg” i “unutrašnjeg” protokola u zavisnosti od njihove pozicije u referentnom modelu možemo nazvati tuneliranje.
- arhitektura tuneliranja:
  - transportni protokol – protokol transportne mreže
  - protokol tunela – definiše, kreira, raskida, upravlja tunelom
  - tunelirani protokol – originalne jedinice prenosa koje se prenose kroz tunel

12. Problemi koji mogu nastati unutar tuneliranja.

- tuneliranje za posledicu ima povećanje veličine osnovne jedinice prenosa:
  - što može dovesti do fragmentacije koja je loša po pitanju end-to-end performansi
  - krajnje tačke, koje učestvuju u komunikaciji, nisu upoznate sa činjenicom da tunel snižava MTU
- tuneliranje zahteva dodatne aktivnosti u procesiranju osnovnih jedinica prenosa
- može dovesti do problema u radu između različitih implementacija

13. Navesti arhitekturu PPTP tunela *(primer PPTP paketa i šta je to PPTP)*.

- GRE (Generic Routing Encapsulation) – pokušaj da se napravi generalno rešenje koje neće zavisiti od specifičnosti tuneliranog protokola i transportnog protokola
- PPP omogućava prenos različitih protokola III nivoa kroz *point-to-point* veze
- PPTP (Point to Point Tunneling Protocol) – ekstenzija PPP. Omogućava prenos PPP frejmova preko IP mreže:
  - tunelirani protokol – PPP
  - protokol tunela – GRE

    - transportni protokol – IP
- PPTP ima mogućnost tuneliranja više PPP sesija kroz jedan tunel. PPTP sesija je skup više od dva toka saobraćaja: upravljački kanal (kreiranje, upravljanje i raskidanje tunela) i kanal za prenos podataka (tunel). Kanal za prenos podataka (tunel):
    - PPP frejm se enkapsulira u GREv1 jedinicu prenosa
    - GREv1 se enkapsulira u IP

Ethernet	*IP*	*GRE*	*PPP*	*IP*	*TCP*	*HTTP*

14. Navesti arhitekturu L2TP tunela *(primer L2TP paketa i šta je to L2TP)*.

- L2TP (Layer Two Tunneling Protocol) – omogućava prenos PPP frejmova preko IP, Frame Relay, ATM i drugih mreža
    - tunelirani protokol – PPP
    - protokol tunela - L2TP
    - transportni protokol – UDP/IP
- ima mogućnost kreiranja više tunela sa više PPP sesija krz jedan logički tunel

Ethernet	*IP*	*UDP*	*L2TP*	*PPP*	*IP*	*TCP*	*HTTP*

- L2TP tunel je sesija sa dva toka saobraćaja, ne postoje odvojeni upravljački kanal i kanal tunela. Razlikuju se tipovi poruka: kontrolne poruke i poruke za prenos podataka.

15. Navesti tipove VPN-a i tehnologije za njihovu realizaciju.

- VPN (Virtual Private Network) - privatna mreža za prenos podataka koja se realizuje preko javne infrastrukture upotrebom tuneliranja i drugih mehanizama zaštite podataka i služi za njihov prenos.
- tipovi:
    - trusted VPN – ekskluzivnost, garancija karakteristika (QoS). Realizuju se putem unapred određenih putanja sa definisanim karakteristikama kroz mrežu jednog ili više ugovorom vezanih provajdera. Provajderi garantuju putanje i njihove karakteristike. Servis koji se pruža od strane provajdera i potpuno je transparentan u odnosu na korisnika.
    - secure VPN – koristi se kriptozaštita da bi se ostvarila: autentifikacija, integritet, poverljivost, neporecivost. Nema zavisnosti od provajdera. Omogućava se pristup klasifikovanih korisnika – klasifikovanim privatnim servisima sa bilo koje tačke Interneta.
    - hybrid VPN – omogućava se paralelno korišćenje oba tipa VPN, u potpunosti ili delimično.
- tehnologije:
    - trusted VPN: ATM, Frame Relay, L2 MPLS, L3 MPLS/BGP
    - secure VPN: Ipsec, Ipsec/GRE, Ipsec/L2TP, SSL/TLS
    - hybrid VPN: bilo koja kombinacija gore navedenih