Lab 1 – Network sniffing i zaštita pomoću IPSec tunela

Topologija

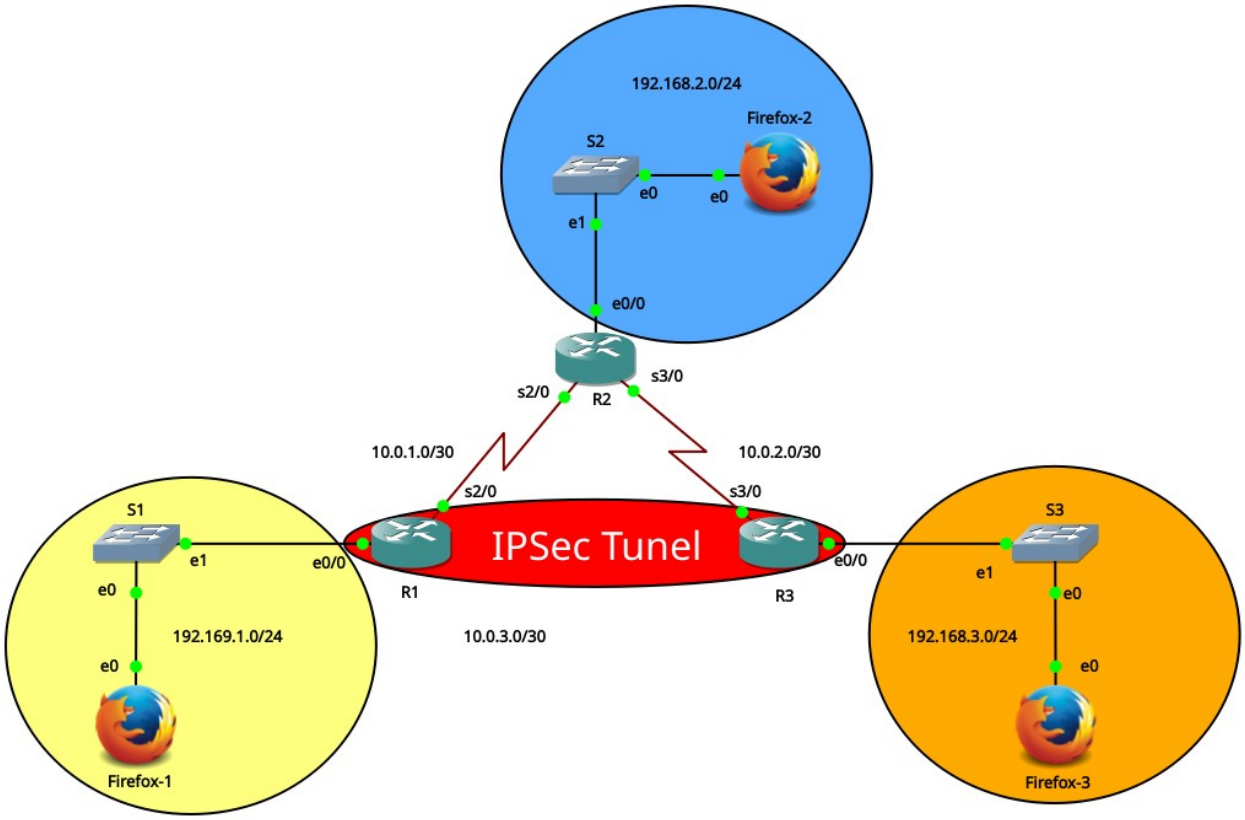


Tabela adresa

Uređaj	Interfejs	IP adresa	Mrežna maska	Default Gateway
R1	F0/0	192.168.1.1	255.255.255.0	N/A
	S1/0	10.0.1.1	255.255.255.252	N/A
R2	F0/0	192.168.2.1	255.255.255.0	N/A
	S1/0	10.0.1.2	255.255.255.252	N/A
	S1/1	10.0.2.2	255.255.255.252	N/A
R3	F0/0	192.168.3.1	255.255.255.0	N/A
	S1/1	10.0.2.1	255.255.255.252	N/A
PC-1	NIC	192.168.1.10	255.255.255.0	192.168.1.1
PC-2	NIC	192.168.2.10	255.255.255.0	192.168.2.1
PC-3	NIC	192.168.3.10	255.255.255.0	192.168.3.1

Ciljevi

1. Postaviti topologiju
2. Konfigurisati uređaje i proveriti međusobne konekcije
3. Konfigurisati i testirati IPSec VPN tunel
4. Iskoristiti Wireshark za prikupljanje poverljivih informacija

Opis vežbe

Network sniffing se u nekim situacijama ne smatra pravim sajber napadom (ali se svakako smatra pretnjom), jer se ne nanose nikakve promene niti šteta na računarski sistem i njegovu mrežu. Network sniffing podrazumeva „osluškivanje“ mreže ili njeno nadgledanje, radi prikupljanja određenih informacija (podataka). Ovo može podrazumevati i njihovo prikupljanje radi utvrđivanja problema u mreži i njenog testiranja, a može se i zloupotrebiti radi krađe podataka i poverljivih informacija. U ovoj konkretnoj vežbi se demonstrira primer kako se Wireshark može iskoristiti da se nadgledaju paketi koji prolaze kroz nezaštićenu mrežu (mrežu bez enkripcije) kao i da se „uhvate“ poverljivi podaci kao što su korisničko ime i lozinka za pristup nekom veb serveru, a zatim se demonstriraju mogućnosti IPSec protokola i IPSec VPN tunela za sprečavanje prikupljanja tih podataka tako što se svi podaci između konifigurisanih uređaja šalju enkriptovano.

Zahtevi

1) 3 Cisco IOU L3 rutera
2) 3 Ethernet sviča
3) 3 Firefox-a

1. Osnovna podešavanja

1.1. Postavka uređaja i kreiranje topologije

Postavite sve uređaje i pravilno ih povežite, kao što je i prikazano na slici.

1.2 Vraćanje rutera na početnu konfiguraciju

Obrišite prethodnu konfiguraciju ukoliko postoji, a zatim restartujte ruter.

```
R1(config)# erase startup-config
R1(config)# reload
```

1.3. Osnovna konfiguracija

Konfigurišite osnovne parametre na svim ruterima i Firefox uređajima, date u tabeli iznad (korisnička imena, IP adrese...).

1.4. Onemogućavanje DNS Lookup-a

Onemogućite DNS lookup kako ruter ne bi pokušavao da prevodi pogrešno ukucane komande.

```
R1(config)# no ip domain-lookup
```

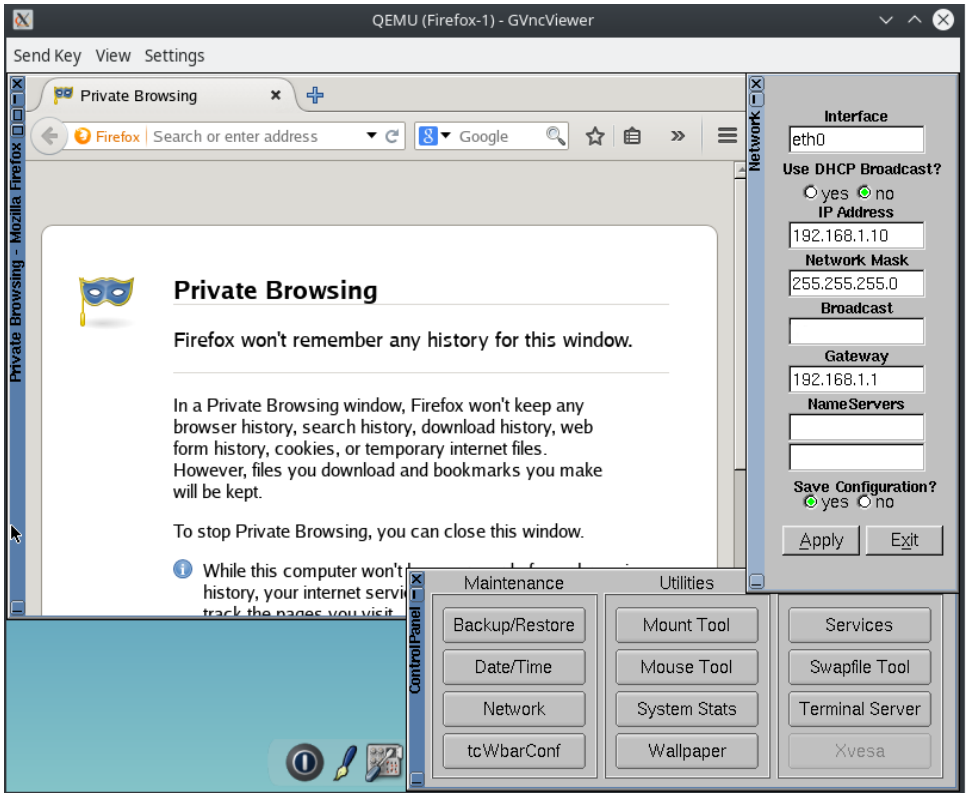
1.5. Konfiguracija ruting protokola

Konfigurišite OSPF protokole na ruterima R1, R2 i R3 kako bi mogli međusobno komunicirati.

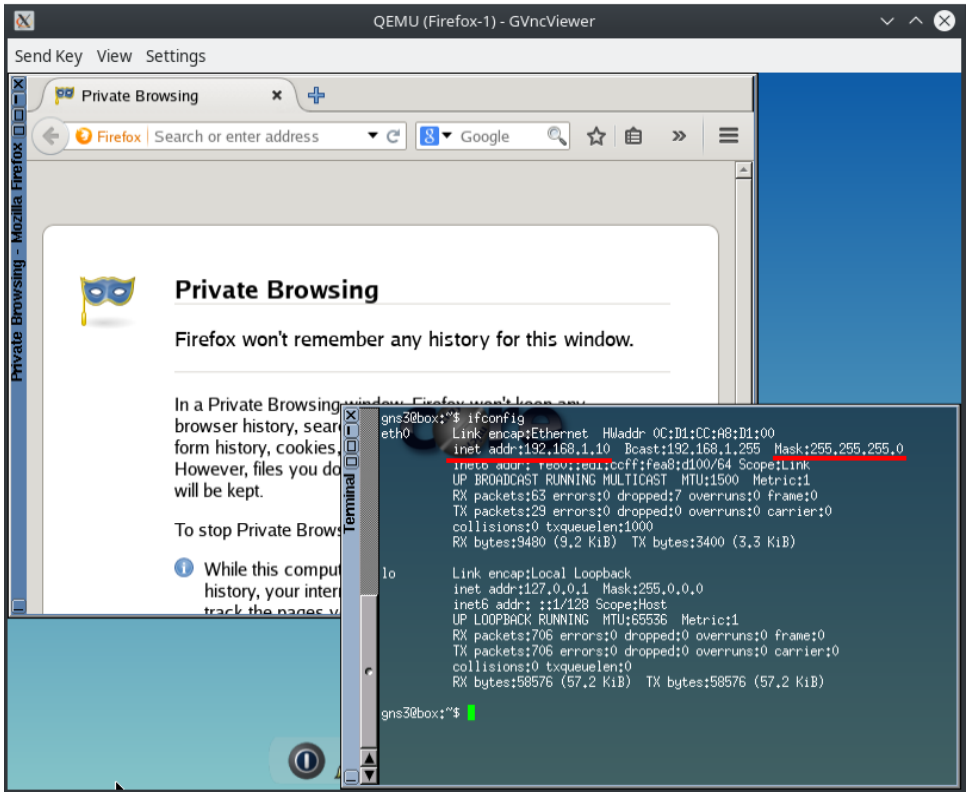
```
R1(config)# router ospf 1
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
R1(config-router)# network 10.0.1.0 0.0.0.3 area 0

R2(config)# router ospf 1
R2(config-router)# network 192.168.2.0 0.0.0.255 area 0
R2(config-router)# network 10.0.1.0 0.0.0.3 area 0
R2(config-router)# network 10.0.2.0 0.0.0.3 area 0

R3config)# router ospf 1
R3(config-router)# network 192.168.3.0 0.0.0.255 area 0
R3(config-router)# network 10.0.2.0 0.0.0.3 area 0
```

1.6. Firefox konfiguracija

Konfigurišite IP parametre za sve Firefox uređaje pokretanjem konzole Firefox-a u *Control Panel* > *Network*. Popunite parametre kao na slici u skladu sa podacima iz tabele date na početku vežbe.



Da biste proverili da li vam je Firefox prihvatio IP adresu, otvorite terminal iz donjeg menija i unesite komandu **ifconfig**. Trebalo bi da dobijete nešto slično onome na slici ispod, a crvenom linijom su označeni ispravna IP adresa i njena maska.



1.7. Testiranje konekcije

Testirajte konekcije međusobnim pingovanjem uređaja. U koliko neki uređaj ne može pingovati drugi, proverite da li ste dobro uneli mreže za oglašavanje protokola, kao i da li ste dobro podesili IP adrese i da li su ih uređaji prihvatili.

2. Konfiguracija pristupa ruteru i osnovna zaštita

2.1. Kreiranje lozinki za pristup ruterima R1, R2 i R3

Postavite lozinke za pristup privilegovanom modu, konzoli i za udaljeni pristup (virtuelne linije), na sva 3 rutera, omogućite logovanje, podesite da se linija prekine ako nema nikakvih aktivnosti u periodu od 5 minuta i unesite komandu da sprečite da vam konzolne poruke prekidaju kucanje.

```
R1(config)# enable secret ciscopa55
R1(config) line console 0
R1(config-line)# password ciscoconpa55
R1(config-line)# login
R1(config-line)# exec-timeout 5 0
R1(config-line)# loggin synchronous
R1(config-line)# exit
R1(config) line vty 0 4
R1(config-line)# password ciscovtypa55
R1(config-line)# login
R1(config-line)# exec-timeout 5 0
R1(config-line)# loggin synchronous
R1(config-line)# exit
```

2.2. Enkriptovanje lozinki

Dodatno zaštite lozinke enkripcijom.

```
R1(config)#service password-encryption
```

2.3. Postavljanje poruke upozorenja

Postavite poruku koja će se prikazivati prilikom pristupanja ruteru.

```
R1(config)# banner motd # UPOZORENJE! Pristup ruteru je zabranjen
neautorizovanim licima! #
```

2.4. Konfigurisanje SSH servera na ruterima R1 i R3

Prvo je potrebno konfigurisati ime domena.

```
R1(config)# ip domain name bezbednost.com
```

Zatim kreirajte lokalni nalog za administrativni pristup sa najvećim nivoom privilegija i enkriptovanom lozinkom.

```
R1(config)# username ciscoadmin privilege 15 secret ciscoadmin12345
```

Nakon što je lokalni nalog kreiran, potrebno je na virtuelnim linijama podesiti privilegovani nivo 15 kako bi korisnik direktno pristupio privilegovanom EXEC modu, umesto korisničkom. Takođe je potrebno i podesiti da se pri pristupanju virtelnim linijama, zahteva korisničko ime i lozinka prethodno kreiranog privilegovanog naloga.

```
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# exit
```

Da bi veza putem virtuelnih linija bila uspostavljena pomoću SSH protokola (koji je bezbedniji od Telnet-a), potrebno je konfigurisati SSH na virtuelnim linijama. Takođe podesite i da se koristi SSH verzija 2.

```
R1(config)# line vty 0 4
R1(config)# ip ssh version 2
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Sledeći korak je generisanje RSA ključeva koji služe za autentifikaciju i enkripciju podataka koji se prenose putem SSH konekcije.

```
R1(config)# crypto key generate rsa general-keys modulus 1024
```

I na kraju je potrebno podesiti vremenski period nakon kojeg će se SSH konekcija prekinuti ukoliko bude neaktivna, kao i ograničavanje broja pokušaja SSH autentifikacije.

```
R1(config)# ip ssh time-out 90
R1(config)# ip ssh authentication-retries 2
```

Testirajte SSH konekciju tako što ćete pokušati da se poveže sa rutera R1 na R3 i obrnuto.

```
R1# ssh -l ciscoadmin 10.0.2.2
```

3. Podizanje HTTP servera

Jedna od mogućnosti Cisco rutera jeste da radi kao HTTP server. HTTP server na Cisco ruterima se podiže sledećom komandom:

```
R1(config)# ip http server

R3(config)# ip http server
```

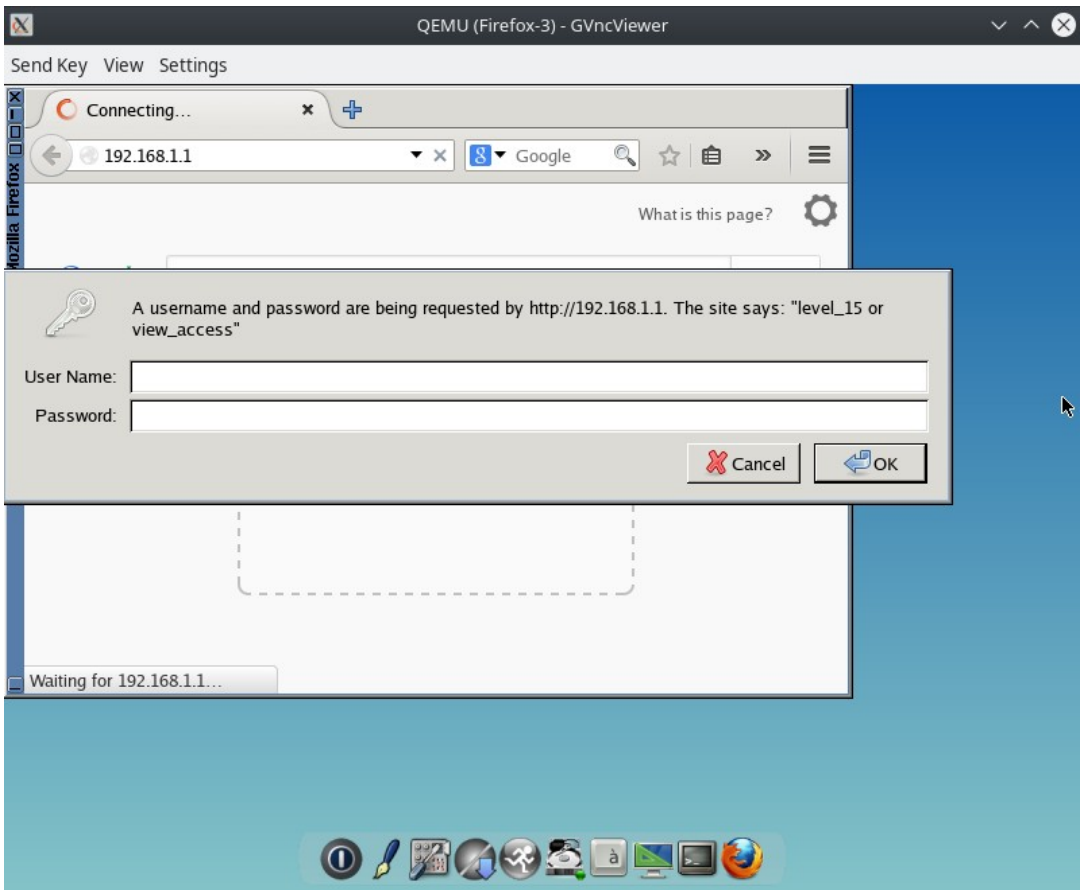
Da bismo bili sigurniji da niko ne može pristupiti ovom serveru bez dodatne zaštite, omogućićemo zahtevanje korisničkog imena i lozinke za pristup. Za to se koristi komanda **ip http authenticatio**n. Izlistajte sve moguće metode autentifikacije komandom:

```
R1(config)# ip http authentication ?
    aaa       Use AAA access control methods
    enable  Use enable passwords
    local    Use local username and passwords
```

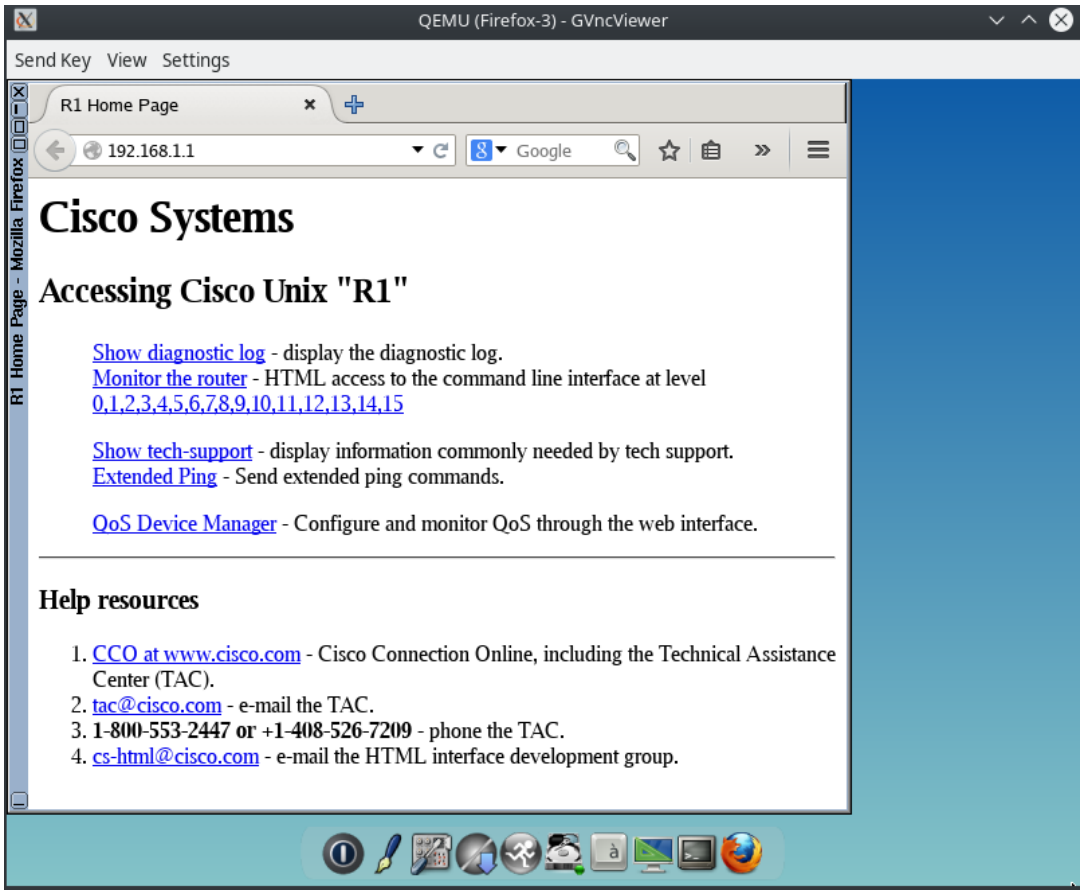
Mi ćemo koristiti opciju **local** što bi značilo da je za pristupanje našem HTTP serveru potreban lokalni nalog koji smo ranije kreirali.

```
R1(config)# ip http authentication local
```

Kada sa uređaja Firefox-3 pokušate otvoriti R1 server (http://192.168.1.1), od vas će se zahtevati da uneste korisničko ime i lozinku, kao što je prikazano na slici ispod.



Kada uneste podatke i pristupite serveru, dobićete stranicu kao na slici ispod, koja znači da ste uspešno pristupili HTTP serveru.



Glavni problem koji se sada javlja jeste što mreža i komunikacija koja se obavlja između uređaja nije enkriptovana i što se pristupni podaci kao što su korisničko ime i lozinka, lako mogu "presesti" pomoću Wireshark-a, što ćemo i videti u nastavku vežbe.

4. Prikupljanje paketa i informacija uz Wireshark

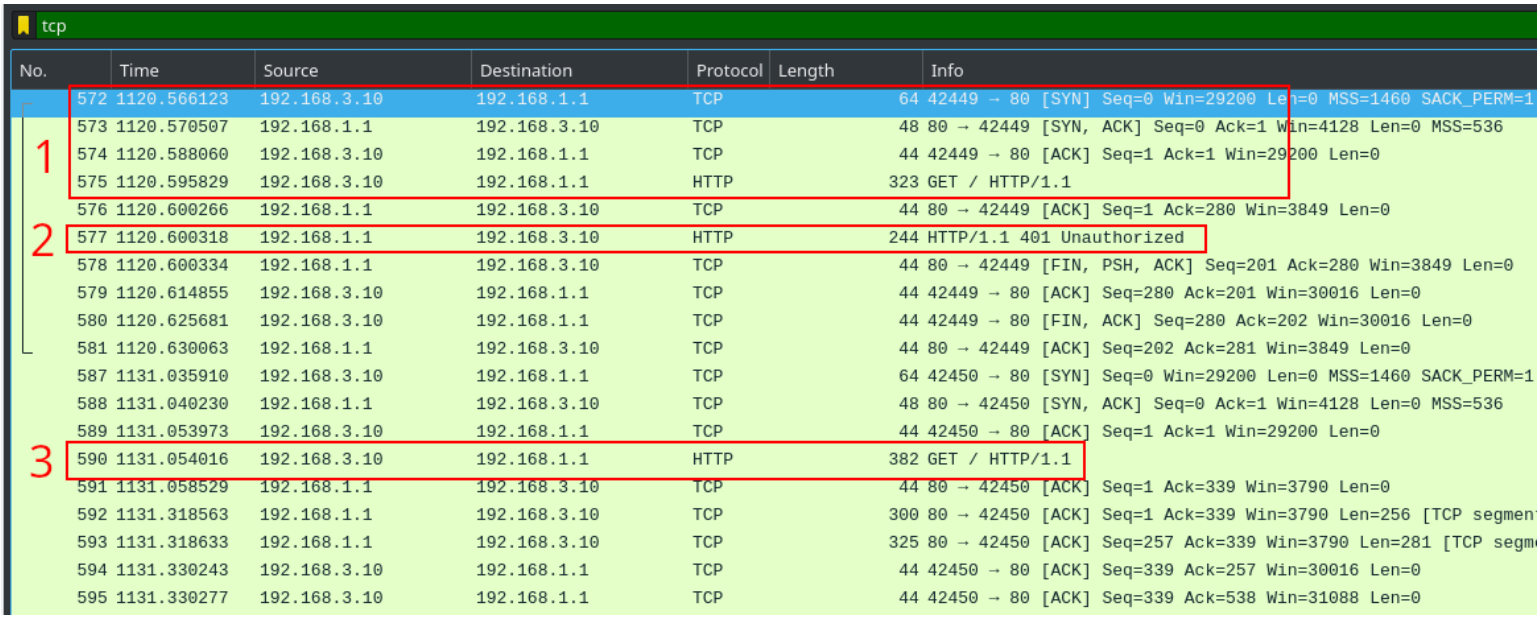
U GNS3 programu, Wireshark se pokreće desnim klikom na link između dva uređaja, zatim se klikne na *Start capture*, onda se pojavljuje prozor u kome možete postaviti ime fajla i potvrditi sa *OK*. Nakon toga će se otvoriti Wireshark i započeti beleženje paketa na linku između ta dva uređaja.

Kada pokrenete Wireshark, primetićete dosta OSPF Hello paketa kao i CDP - Device ID pakete koji sadrže informacije o određenom uređaju kao što su ime rutera, adrese, model uređaja i verzija Cisco IOS-a, i sl.

4.1. Beleženje TCP i HTTP paketa

Pokrenite Wireshark na serijskoj vezi između rutera R1 i R2, a zatim sa Firefox-3 uređaja pristupite R1 veb serveru. Wireshark će zabeležiti vaš pokušaj pristupa kao i podatke za pristup koje ste uneli.

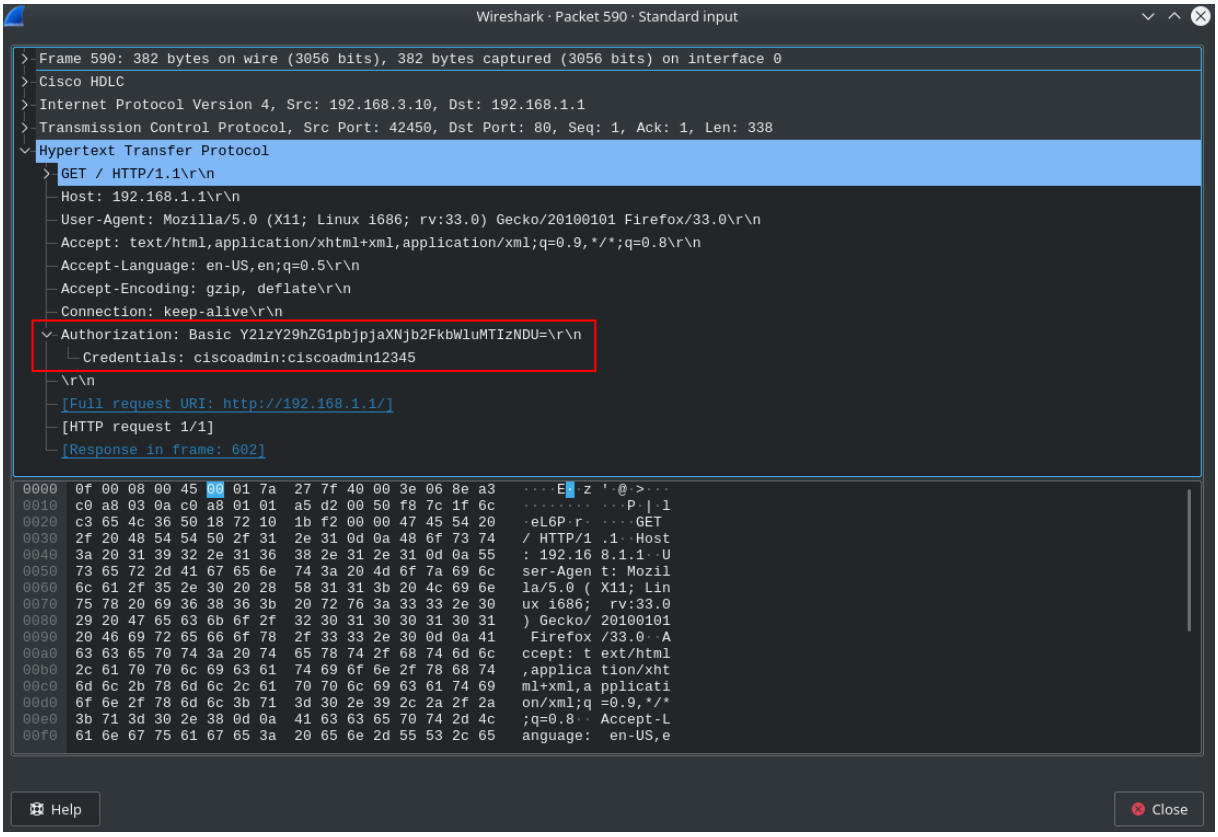
U Wireshark polju za filtere, unesite **tcp** i pritisnite enter, kako bi vam se samo TCP paketi prikazivali. Preko Firefox-3 uređaja otvorite http://192.168.1.1, zatim unesite podatke za pristup. Kada otvorite Wireshark trebalo bi nešto slično slici ispod da dobijete.



Na slici uočavamo nekih par bitnih paketa. Prva označeno polje predstavlja tzv. *Three-Way Handshake*, metoda za uspostavljanje TCP konekcija u računarskim mrežama. Uređaj sa adresom 192.168.3.10 (Firefox-3) je poslao SYN paket uređaju sa adresom 192.168.1.1 (R1). Zatim je R1 poslao SYN i ACK pakete nazad ka Firefox-3 uređaju i na kraju je Firefox-3 odgovorio ruteru R1 sa ACK paketom. Poslednji paket (575) predstavlja uspešno uspostavljenu komunikaciju.

S obzirom da je naš HTTP server podešen tako da je potrebno uneti korisničko ime i lozinku da bi mu se pristupilo, u slučaju da unesete pogrešne podatke, dobićete HTTP kod 401 Unauthorized, kao što je i prikazano na slici (označeno polje broj 2).

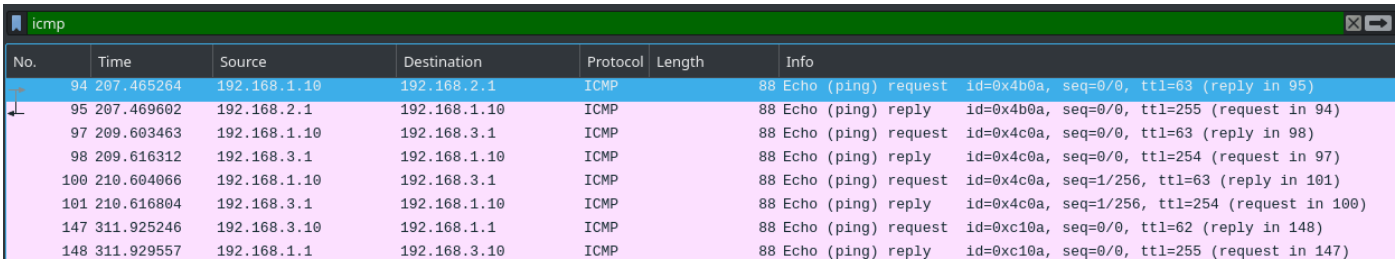
Poslednje polje je polje koje označava supešno logovanje na server. Zapravo ovaj pakekt izgleda isto kao i paket 575 s tim što je paket 590 malo veći od 575. To je zato što sada ovaj paket sadrži i još dodatne informacije od kojih su neke i pristupni podaci, korisničko ime i lozinka. Dvoklikom otvorite paket i u protokolu *Hypertext Transfer Protocol*, proširite polje *Authorization* kako biste videli kredencijale za pristup HTTP serveru.



Wireshark takođe može zabeležiti i koje ste stranice otvorili, tako da ako otvorite na primer *Show diagnostic log* stranicu, u Wiresharku bi trebalo da vam se pojavi među paketima, paket sa opisom *HTTP/1.1 200 OK (text/html)*. Pronađite takav paket i otvorite ga, a zatim ćete u delu *Line-based text data* videti otvorenu stranicu u HTML kodu.

4.3. Beleženje ICMP paketa

Isto tako i ako biste pingovali neki od rutera, Wireshark bi takođe to mogao zabeležiti, što je i prikazano na slici ispod, gde su prikazani samo ICMP paketi.



Ovim zaključujemo da ovakve stvari nisu prihvatljive u praksi i da se kokmunikacija ka osetljivim informacijama i resursima mreže (u ovom slučaju našim HTTP serverima), mora zaštiti, što će biti sledeći korak.

Dodatak: Istražite koje još pakete je Wireshark zabeležio (bez obzira na tip protokola) i koje informacije možete dobiti iz njih.

5. Konfiguracija IPSec VPN tunela

Konfigurisanje IPSec VPN tunela se sastoji iz dva dela:

1. Implementacijie Internet Key Exchange (IKE) parametara
2. Implementaciji IPSec parametara

U ovom delu vežbe se konfigurišu ti parametri potrebni za kreiranje IPSec VPN tunela između R1 i R3, kroz koji će se podaci prenositi bezbedno i enkriptovano.

5.1. Testiranje konekcije iz LAN mreže R1 ka LAN mreži R3

Kako bi mogli uspešno konfigurisati i testirati IPSec VPN tunel, potrebno je utvrditi da je veza između LAN mreže R1 i LAN mreže R3 moguća.

Pingujte Firefox-3 sa uređaja Firefox-1

```
gns3@box:~$ ping 192.168.3.10
```

Ako je ping neuspešan, proverite dobro da li su vam svuda dobro podešene IP adrese, kao i ruting protokoli i mreže koje oglašavaju.

5.2. IKE implementacija

IKE se sastoji iz dve faze:

1. IKE faza 1 - Definište metodu razmene ključeva koji se koriste za verifikaciju i propuštanje IKE polisa između uređaje
2. IKE faza 2 - U ovoj fazi uređaji razmenjuju i poklapaju IPSec polise za autentifikaciju i enkripciju podataka.

Kako bi IPSec VPN tunel mogao funkcionisati, IKE mora prethodno biti omogućen na ruteru. IKE je inače podrazumevano omogućen, ali za slučaj da nije, može se oogućiti sledećom komandom:

```
R1(config)# crypto isakmp enable

R3(config)# crypto isakmp enable
```

Da bi razmena ključeva bila moguća, potrebno je kreirati ISAKMP polisu koja definiše algoritme za enkripciju i autentifikaciju, kao i heš koji se koristi za slanje podataka u VPN tunelu.

Na ruterima R1 i R3, kreirajte ISAKMP polisu sa prioritetom 10. Podesite SHA heš algoritam i AES-256 algoritam za enkripciju, Diffie-Hellman grupu 14 za razmenu ključeva, a kao tip autentifikacije, podesite *pre-shared* ključeve. Takođe podesite i vremenski period od 3600 sekundi.

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# group 14
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# lifetime 3600
```

Potvrdite IKE polisu komandom **show crypto isakmp policy**:

```
R1# show crypto isakmp policy

Global IKE policy
Protection suite of priority 10
       encryption algorithm:    AES - Advanced Encryption Standard (256 bit
keys).
       hash algorithm:              Secure Hash Standard
       authentication method:  Pre-Shared Key
```

```
       Diffie-Hellman group:   #14 (2048 bit)
       lifetime:                       3600 seconds, no volume limit
```

Sledeće što je potrebno konfigurisati jesu *pre-shared* ključevi koji se koriste za autentifikaciju IKE polise i oni moraju biti konfigurisani na svim ruterima koji upućuju na drugi kraj VPN tunela. Konfigurišite *pre-shared* ključ cisco123 na oba rutera R1 i R3.

```
R1(config)# crypto isakmp key cisco123 address 10.0.2.2

R3(config)# crypto isakmp key cisco123 address 10.0.1.1
```

Sledeći korak je podesiti set za transformaciju koji se takođe razmenjuje između VPN tačaka kako bi se formirala bezbedna konekcija.

Kreirajte set za transformaciju sa oznakom 50, koji koristi ESP transformaciju sa AES 256 čiperom sa ESP i SHA hešom.

```
R1(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R1(cfg-crypto-trans)# exit

R3(config)# crypto ipsec transform-set 50 esp-aes 256 esp-sha-hmac
R3(cfg-crypto-trans)# exit
```

Kako bi enkripcija VPN tunela moga raditi, potrebno je definisati proširene pristupne liste kako bi ruter znao koji saobraćaj, tj. pakete da enkriptuje. Paket kojem je prolaz dozvoljen od strane pristupne liste (koja definiše IPSec saobraćaj) se šalje enkriptovano, dok paketi kojima nije dozvoljen prolaz, se ne odbacuju već šalju neenkriptovano.

U ovom slučaju, saobraćaj koji dolazi iz LAN mreže R1 je potrebno enkriptovati kada ide ka LAN mreži R3 i obrnuto. Ove liste se postavljaju na *outbound* interfejsima, tj. krajnjim tačkama VPN tunela.

```
R1(config)# access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255

R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.1.0
0.0.0.255
```

Na kraju je potrebno kreirati kripto mapu koja će povezivati saobraćaj koji odgovara pristupnoj listi sa susednim uređajima i različitim IKE i IPSec podešavanjima. Kripto mapa se može primeniti na više interfejsa, ali to bi uvek trebalo biti interfejsi koji "gledaju" ka drugom kraju IPSec tunela, tj. VPN kranjoj tački.

Kreirajte kripto mapu sa imenom CMAP i rednim brojem 10 na ruteru R1.

```
R1(config)# crypto map CMAP 10 ipsec-isakmp
```

Naznačite koja pristupna lista definiše koji će se saobraćaj enkriptovati

```
R1(config-crypto-map)# match address 101
```

Podesite krajnju tačku VPN tunela putem IP adrese.

```
R1(config-crypto-map)# set peer 10.0.2.2
```

Podesite dodatne parametre kao što su set za transformaciju (da budete sigurni da će ga ovaj uređaj koristiti), bezbedan tip prosleđivanja i podrazumevani vremenski period trajanja IPSec Security Association (SA).

```
R1(config-crypto-map)# set pfs group14
R1(config-crypto-map)# set transform-set 50
R1(config-crypto-map)# set security-association lifetime seconds 900
R1(config-crypto-map)# exit
```

Takođe iste parametre (sem IP adrese krajnje tačke) podesite na ruteru R3.

```
R3(config)# crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)# match address 101
R3(config-crypto-map)# set peer 10.0.1.1
R3(config-crypto-map)# set pfs group14
R3(config-crypto-map)# set transform-set 50
R3(config-crypto-map)# set security-association lifetime seconds 900
R3(config-crypto-map)# exit
```

Primenite kripto mape na odgovarajuće interfejse:

```
R1(config)# interface s2/0
R1(config-if)# crypto map CMAP
R1(config-if)# exit

R3(config)# interface s3/0
R3(config-if)# crypto map CMAP
R3(config-if)# exit
```

5.3. Verifikacija IPSec konfiguracije

Komanda **show crypto ipsec transform-set** prikazuje konfigurisane IPSec polise u formi seta za transformaciju.

```
R1# show crypto ipsec transform-set
Transform set default: { esp-aes esp-sha-hmac  }
  will negotiate = { Transport,  }

Transform set 50: { esp-256-aes esp-sha-hmac
  will negotiate = { Tunnel,  },
```

Komanda **show crypto map** prikazuje kripto mapu koja će biti primenjena na ruter.

```
R1# show crypto map
Crypto Map IPv4 "CMAP" 10 ipsec-isakmp
       Peer = 10.0.2.2
       Extended IP access list 101
           access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
       Current peer: 10.0.2.2
       Security association lifetime: 4608000 kilobytes/900 seconds
       Responder-Only (Y/N): N
       PFS (Y/N): Y
       DH group:  group14
       Mixed-mode : Disabled
       Transform sets={
               50:  { esp-256-aes esp-sha-hmac  } ,
       }
       Interfaces using crypto map CMAP:
               Serial2/0

       Interfaces using crypto map NiStTeSt1:
```

5.4. Verifikacija funkcionalnosti IPSec tunela

Komandom **show crypto isakmp** se proverava da li postoje IKE SA. Ako bi sada izvršili komadnu primetili bismo da nikakve rezultate ne dobijamo. To je zato što još uvek nismo generisali određeni saobraćaj koji smo definisali pristupnim listama.

Takođe komandom **show crypto ipsec sa** možemo proveriti koliko se paketa poslalo između kranjih VPN tačaka (nula trenutno) kao i neke dodatne informacije kao što su MTU *plaintext* paketa, IP adrese krajnjih VPN tačaka, koliko je paketa kompresovano, poslato sa greškom, itd.

5.5. Generisanje neinteresantnog saobraćaja

Pingujte sa rutera R1 IP adresu interfejsa s3/0 rutera R3. Ping bi trebalo da bude uspešan.
Pingujte sa rutera R1 IP adresu interfejsa e0/0 rutera R3. Ping bi trebalo da bude uspešan.

Komandom **show crypto isakmp sa** možemo utvrditi da je broj prenetih enkriptovanih paketa i dalje nula. To je zato što je ruter R1 pingovao ruter R3 njemu najbližom IP adresom, tj. ping je usledio sa interfejsa s2/0, mreža u kojoj se nalazi ta adresa ne spada u interesantni saobraćaj.

Interesantan saobraćaj je onaj saobraćaj koji smo definisali da se enkriptuje, tj. ako paketi dolaze iz LAN mreže rutera R1 ka LAN mreži rutera R3 i obrnuto, taj saobraćaj će se smatrati interesasntnim. Sav ostali saobraćaj, koji ne dolazi iz navedenih LAN mreža a namenjen je njima, ili ide ka njima a dolazi iz drugih LAN mreža, će se smatrati neinteresantnim saobraćajem.

5.6. Generisanje interesantnog saobraćaja

Pingujte IP adresu rutera R3, 192.168.3.1 sa rutera R1 ali sa izvornom adresom 192.168.1.1. Ping bi trebalo da bude uspešan.

Ako sada ponovo unesemo komandu **show crypto isakmp** sa primetićemo da se SA kreirao.

```
R1# show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
10.0.2.2        10.0.1.1        QM_IDLE           1001 ACTIVE

IPv6 Crypto ISAKMP SA
```

Ako ponovo izvršimo komandu **show crypto ipsec sa** primetićemo da da je situacija malo drugačija nego ranije i da se poslao određen broj enkriptovanih i transformisanih paketa.

```
R1# show crypto ipsec sa

interface: Serial2/0
   Crypto map tag: CMAP, local addr 10.0.1.1

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer 10.0.2.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

    local crypto endpt.: 10.0.1.1, remote crypto endpt.: 10.0.2.2
    plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Serial2/0
    current outbound spi: 0x8BED14C5(2347570373)
    PFS (Y/N): Y, DH group: group14

    inbound esp sas:
     spi: 0x26855F65(646274917)
       transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 1, flow_id: SW:1, sibling_flags 80004040, crypto map: CMAP
       sa timing: remaining key lifetime (k/sec): (4152458/862)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)
```

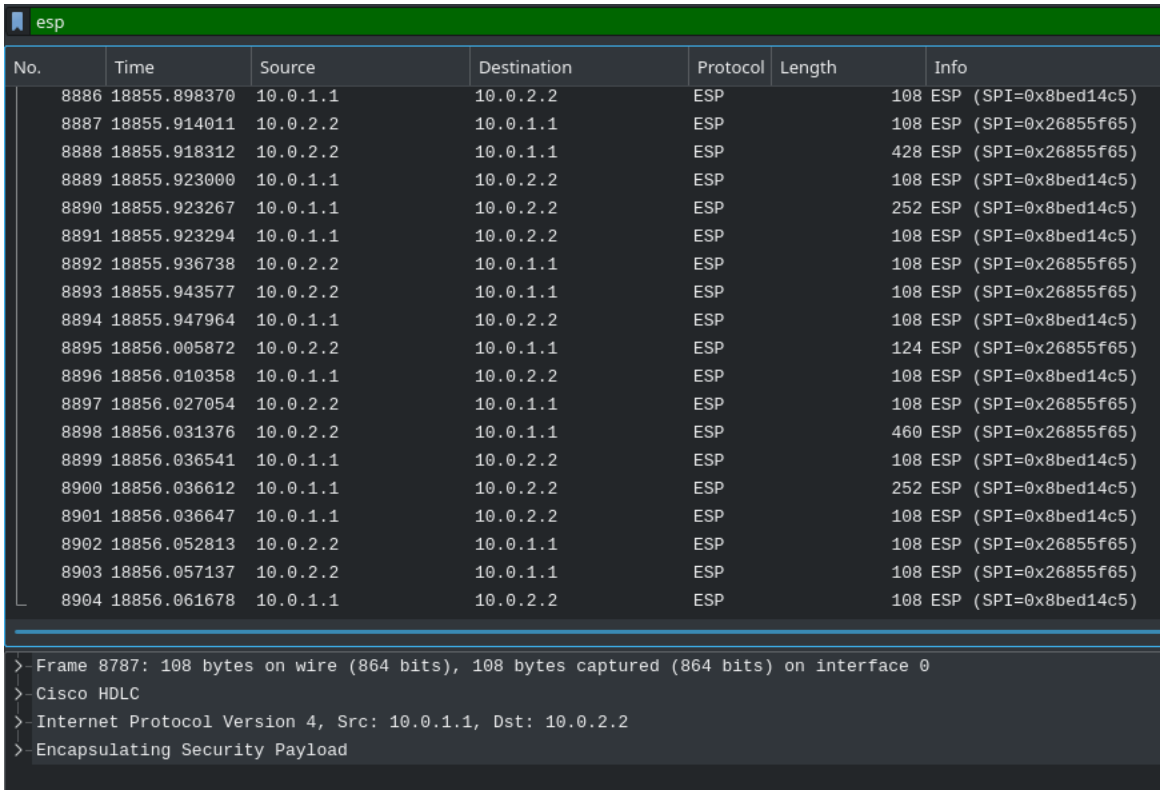
```
inbound ah sas:

inbound pcp sas:

outbound esp sas:
 spi: 0x8BED14C5(2347570373)
   transform: esp-256-aes esp-sha-hmac ,
   in use settings ={Tunnel, }
   conn id: 2, flow_id: SW:2, sibling_flags 80004040, crypto map: CMAP
   sa timing: remaining key lifetime (k/sec): (4152458/862)
   IV size: 16 bytes
   replay detection support: Y
   Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Pokušajte otvoriti HTTP server rutera R3 sa Firefox-1 uređaja i rutera R1 sa Firefox-3 uređaja. Da li se i taj saobraćaj preneo putem IPSec tunela?

5.7. Beleženje IPSec saobraćaja u Wireshark-u

Pre postavljanja IPSec VPN tunela, imali smo prilike da vidimo da Wireshark lako može zabeležiti svaki saobraćaj u mreži koji je namenjen LAN mreži R1 a koji dolazi iz ostalih LAN mreža (i obrnuto). Sada je situacija drugačija. Wireshark će zabeležiti aktivnosti na mreži ali neće moći videti koje su to aktivnosti.

Na slici ispod je prikazan zabeležen saobraćaj, tj. paketi koji su se preneli dok smo pingovali uređaje i pristupali HTTP serverima, nakon konfiguracije IPSec tunela. Primetićete da su svi paketi enkapsulirani u **Encapsulating Security Payload (ESP)** pakete a iz kojih se ne može ništa izvući sem izvornih i odredišnih adresa (krajnjih tačaka tunela).



6. Regulisanje pristupa HTTP serverima

Poslednji problem jeste da ako neko iz LAN mreže R2 pristupa nekim od HTTP servera R1 i R3, taj saobraćaj neće biti enkriptovan, i napadač će pomoću Wireshark-a moći ukrasti poverljive podatke. Postoji par stvari koje se mogu uraditi u ovakvoj situaciji.

1. Podesiti SSL sertifikat i konfigurisati HTTPS server na ruteru
2. Dozvoliti pristup HTTP serveru isključivo određenim pojedincima ili LAN mreži.

S obzirom da smo u ovoj vežbi kreirali VPN tunel između LAN mreža R1 i R3, na neki način je logično i da određenim informacijama i resursima samo i tim mrežama dozvolimo pristup, tj. ograničiti pristup HTTP serveru. To možemo učiniti pomoću proširene pristupne liste.

Na ruterima R1 i R3 kreirajte proširenu pristupnu listu koja će blokirati pristup njihovim HTTP serverima uređajima iz LAN mreže R2, ali će dozvoliti ostali vid saobraćaja.

```
R1(config)#$ access-list 105 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.1 eq
80
R1(config)# access-list 105 permit ip any any

R3(config)#$ access-list 105 deny tcp 192.168.2.0 0.0.0.255 host 192.168.1.1 eq
80
R3(config)# access-list 105 permit ip any any
```

Primenite pristupne liste na odgovarajuće interfejse.

```
R1(config)# int s2/0
R1(config-if)# ip access-group 105 in
R1(config-if)# exit

R3(config)# int s3/0
R3(config-if)# ip access-group 105 in
R3(config-if)# exit
```

Sada ako pokušate da pristupite nekom od HTTP servera iz LAN mreže R2, biće vam blokiran pristup, a Wireshark će i to zabeležit kao što je i prikazano na slici ispod.

No.	Time	Source	Destination	Protocol	Length	Info
10366	21747.569644	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2208, returned sequence 2208
10367	21750.001281	10.0.1.1	224.0.0.5	OSPF	84	Hello Packet
10368	21753.477779	10.0.1.2	224.0.0.5	OSPF	84	Hello Packet
10369	21755.189339	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2209, returned sequence 2208
10370	21757.573520	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2209, returned sequence 2209
10371	21759.623564	10.0.1.1	224.0.0.5	OSPF	84	Hello Packet
10372	21763.385650	10.0.1.2	224.0.0.5	OSPF	84	Hello Packet
10373	21765.193209	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2210, returned sequence 2209
10374	21767.573581	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2210, returned sequence 2210
10375	21768.676851	10.0.1.1	224.0.0.5	OSPF	84	Hello Packet
10376	21770.956529	192.168.2.10	192.168.1.1	TCP	64	55777 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=6532709 TSecr=0 WS=3
10377	21770.960837	10.0.1.1	192.168.2.10	ICMP	60	Destination unreachable (Communication administratively filtered)
10378	21772.720517	10.0.1.2	224.0.0.5	OSPF	84	Hello Packet
10379	21773.531847	N/A	N/A	CDP	358	Device ID: R1.bezbednost.com Port ID: Serial2/0
10380	21774.795912	N/A	N/A	CDP	343	Device ID: R2 Port ID: Serial2/0
10381	21775.193034	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2211, returned sequence 2210
10382	21777.577796	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 2211, returned sequence 2211
10383	21778.448081	10.0.1.1	224.0.0.5	OSPF	84	Hello Packet
10384	21782.636832	10.0.1.2	224.0.0.5	OSPF	84	Hello Packet