Udaljeni pristup računalu te pristup Internetu s prilagodljivim sigurnosnim vatroštitom

Kordić, Petar

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Petar Kordić

Udaljeni pristup računalu te pristup Internetu s prilagodljivim sigurnosnim vatroštitom

ZAVRŠNI RAD

Varaždin, 2024.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Petar Kordić

Matični broj: 0016143797

Studij: Informacijski sustavi

Udaljeni pristup računalu te pristup Internetu s prilagodljivim sigurnosnim vatroštitom

ZAVRŠNI RAD

Mentor:

Izv. prof. dr. sc. Nikola Ivković

Varaždin, rujan 2024.

Petar Kordić

Izjava o izvornosti

Izjavljujem da je moj završni/diplomski rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor/Autorica potvrdio/potvrdila prihvaćanjem odredbi u sustavu FOI-radovi

Sažetak

Cilj ovog rada je prikazati implementaciju mrežnog vatroštita u računalnoj mreži korporacije u cilju ostvarenja dvije osnovne funkcionalnosti: udaljeni pristup putem Interneta računalu unutar lokalne mreže korporacije i pristup Internetu s računala u korporativnoj mreži.

Implementacija je prikazana uz pomoć laboratorijskog okruženja koje se sastojalo od hardverskog vatroštita proizvođača Cisco te nekoliko računala u ulozi poslužitelja i klijenata. Prikazani su koraci konfiguriranja vatroštita, testiranje funkcionalnosti te na kraju je prikazana konfiguracija vatroštita uz objašnjena važnijih parametara.

Ključne riječi: komunikacija, lokalna mreža, Internet, vatroštit, računalo, server.

Sadržaj

1. Uvod

Komunikacija putem interneta je odavno postala svakodnevnica u svim segmentima života, od osobnog do poslovnog. Kako bi se osigurala sigurna komunikacija koju treća strana ne može pratiti ili zloupotrijebiti, tijekom zadnjih tridesetak godina stručnjaci za informacijske i komunikacijske tehnologije su razvijali razne vrste vatroštita.

Vatroštiti (eng. *Firewall*) su mrežni uređaji koji nadziru dolazni i odlazni promet te temeljem određenih pravila i kriterija odlučuju hoće li propustiti ili blokirati mrežni promet koji prolazi kroz vatroštit[1]. Jedna od glavnih funkcionalnosti vatroštita je povezivanje sigurnih i nesigurnih mreža. Pod sigurnom mrežom se smatra npr. lokalna mreža određene korporacije, a pod nesigurnom Internet ili lokalna mreža neke druge korporacije.

Vatroštit može biti hardverski ili sofverski, a u ovom radu se koristio hardverski vatroštit Cisco ASA 5585. Predmetni vatroštit spada u tzv. *stateful* vatroštite koji na ISO 4 razini provjerava pakete koji prolaze kroz njega te temeljem svoje *stateful* tablice zaključuje je li određeni paket dio nove ili postojeće veze. Temeljem te informacije te temeljem provjere pristupnih listi, vatroštit dozvoljava ili blokira mrežni promet koji prolazi kroz njega.

Stateful vatroštitima su prethodili tzv. *packet filter* vatroštiti koji ne vode računa o statusu veza nego dozvoljavaju ili blokiraju mrežni promet samo na osnovu pristupnih listi[2]. Primjeri takvog vatroštita su *iptables* mehanizni na Linux računalima ili Windows vatroštit. Vatroštiti koji provjeravaju promet na ISO 7 razini spadaju u tzv. Next generation vatroštite koji, povrh provjere pristupnih listi i *stateful* inspekcije, vrše inspekciju mrežnog prometa sve do razine aplikacije.

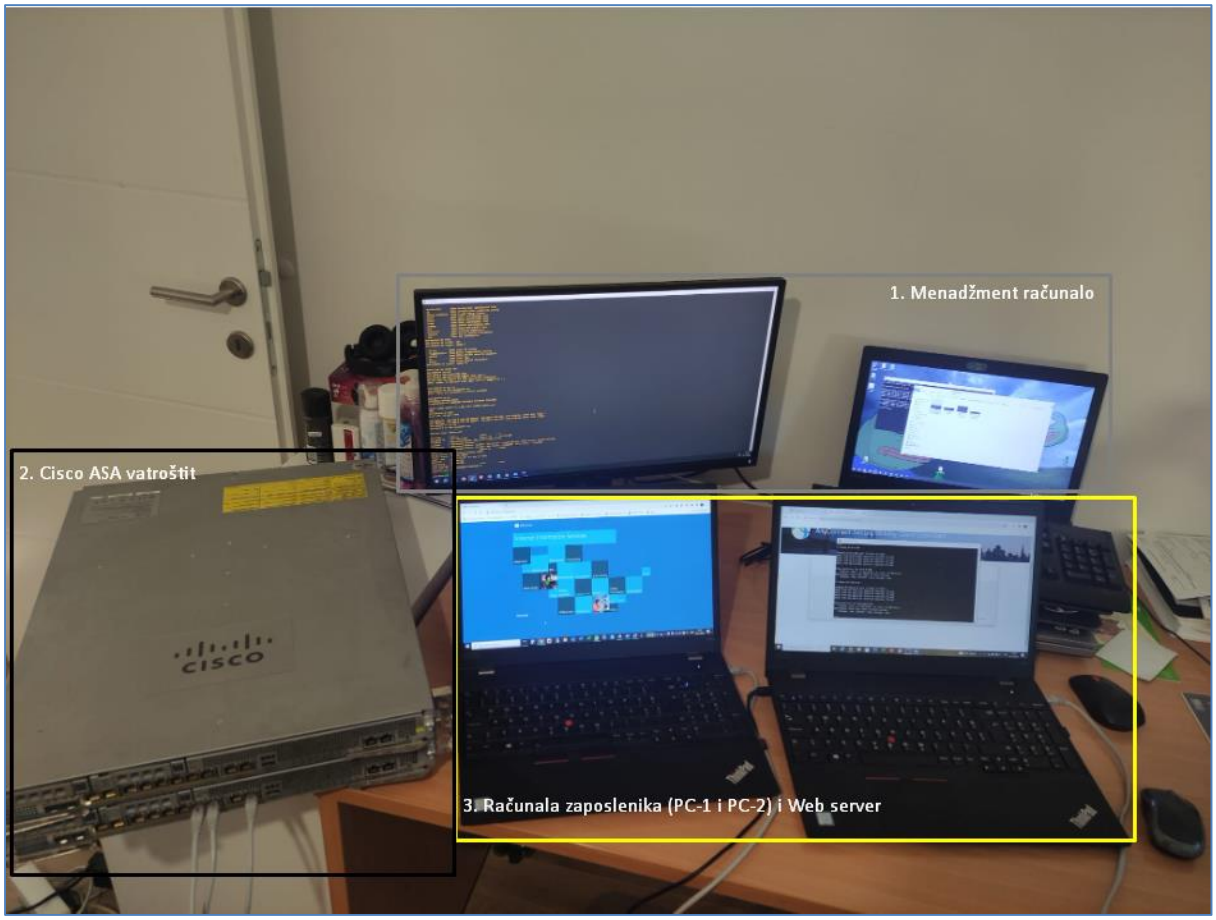
Ovaj rad obrađuje dva scenarija koji se vrlo često susreću u stvarnim situacijama: udaljeni pristup putem Interneta računalu unutar lokalne mreže korporacije i pristup Internetu s računala na korporativnoj mreži. Scenariji su simulirani u laboratorijskoj okolini, a rad prikazuje korake konfiguriranja vatroštita, testiranje uspostavljenih veza te objašnjenje važnijih dijelova konfiguracije vatroštita.

Na kraju rada u prilogu se nalazi ispis važnijih dijelova konfiguracije vatroštita s objašnjenjima.

2. Oprema u laboratoriju

Oprema korištena u laboratoriju za testiranje scenarija ovog rada sastoji se od nekoliko hardverskih i softverskih komponenti. Od hardverskih komponenti su korištena 3 računala, 1 monitor i 1 Cisco ASA vatroštit. Korišteni su i UTP kablovi za međusobno povezivanje svih komponenti.

Od softverskih komponenti korišteni su Cisco ASA softver koji se nalazi na samom Cisco ASA hardverskom vatroštitu, Cisco ASDM softver (Cisco Adaptive Security Device Manager), Cisco AnyConnect softver i aplikacija PuTTY. Svaka komponenta je obrađena nadalje u ovom radu, a slika 1. prikazuje kako oprema izgleda uživo u improviziranom laboratatoriju u radnoj sobi.



Slika 1: Fizički izgled opreme

2.1. Hardver

2.1.1. Vatroštit Cisco ASA

Seriju ASA vatroštita je razvila američka tvrtka Cisco. ASA je skraćenica od *Adaptive Security Appliance*, ili na hrvatskom prilagodljivi sigurnosni uređaj. Razvijan je od 2005. godine na temelju Cisco PIX uređaja i još uvijek se koristi po cijelom svijetu[3].

2.1.2. Računala

Na slici 1. računala su označena sivim i žutim pravokutnikom. Sva tri računala pripadaju Lenevo Ideapad ili Thinkpad seriji. U sivom pravokutniku se nalazi menadžment računalo koje služi za konfiguriranje vatroštita. Na njemu se koristi više aplikacija za konfiguriranje vatroštita pa je spojen na dodatni monitor zbog lakšeg pregleda.

U žutom pravokutniku se nalaze računala koja imaju uloge računala zaposlenika i uloge servera. Što se tiče servera, u prvom scenariju gdje se simulira udaljeni pristup s Interneta računalu unutar lokalne mreže korporacije, korišten je Windows datotečni server. U drugom scenariju gdje se simulira pristup Internetu s računala na korporativnoj mreži, korišten je Windows Web Server (*IIS*).

2.2. Softver

2.2.1. ASA i ASDM

Cisco ASA softver je operativni sustav koji se nalazi na Cisco ASA vatroštitima. Instalacijske datoteke ASA softvera su smještene u tzv. Flash memoriji vatroštita, a operativni sustav se izvodi u radnoj memoriji vatroštita.

Cisco Adaptive Security Device Manager, u daljnjem tekstu ASDM, je Ciscov softver za upravljanje vatroštitima putem grafičkog sučelja[4]. Instalira se na menadžment računalu. U okviru prvog scenarija, ASDM je korišten za konfiguriranje VPN-a kojeg zaposlenici koriste putem Cisco AnyConnect aplikacije.

2.2.2. PuTTY

PuTTY je besplatni softver otvorenog koda koji služi kao emulator terminala. U okviru oba scenarija PuTTY je korišten za upravljanje ASA-om putem menadžment računala.

2.2.3. Cisco AnyConnect

Cisco AnyConnect je softver koji omogućuje zaposlenicima sigurno spajanje na korporacijsku mrežu putem VPN-a. U okviru prvog scenarija, ovaj softver se preuzima s vatroštita te se instalira na korisničko računalo.

3. Scenariji

Prvi scenarij simulira udaljeni pristup s Interneta računalu unutar lokalne mreže korporacije. Prikazat će se cijeli postupak, od konfiguriranja VPN postavki na vatroštitu putem ASDM softvera, preko korisničkog spajanja na vatroštit, preuzimanja i instaliranja Cisco AnyConnect softvera na korisničko računalo do povezivanja korisnika na datotečni server smješten na korporacijskoj mreži.

Drugi scenarij simulira pristup Internetu s računala na korporativnoj mreži. Korisnik će s računala (u daljnjem tekstu PC-1) unutar korporacijske mreže pristupiti web serveru (u daljnjem tekstu Web server-1) koji se nalazi na Internetu. Prilikom spomenutog pristupa, privatna IP adresa računala PC-1 će biti, putem NAT pravila na vatroštitu, translatirana u javnu IP adresu. Dodatno, pristup će biti ograničen putem pristupnih listi (eng. *Access lists*) na vatroštitu. Mrežni resursi korišteni za potrebe laboratorija ovog rada su bili ograničeni u smislu korištenja javnog IPv4 prostora. Kako laboratorij nije raspolagao s javnim IPv4 adresama, umjesto javnih IPv4 adresa su korištene privatne IPv4 adrese iz raspona 10.0.0.0/8. To ograničenje nije utjecalo na cilj i rezultate ovog rada.

Glavne karakteristike oba scenarija su opisane u sljedećoj tablici.

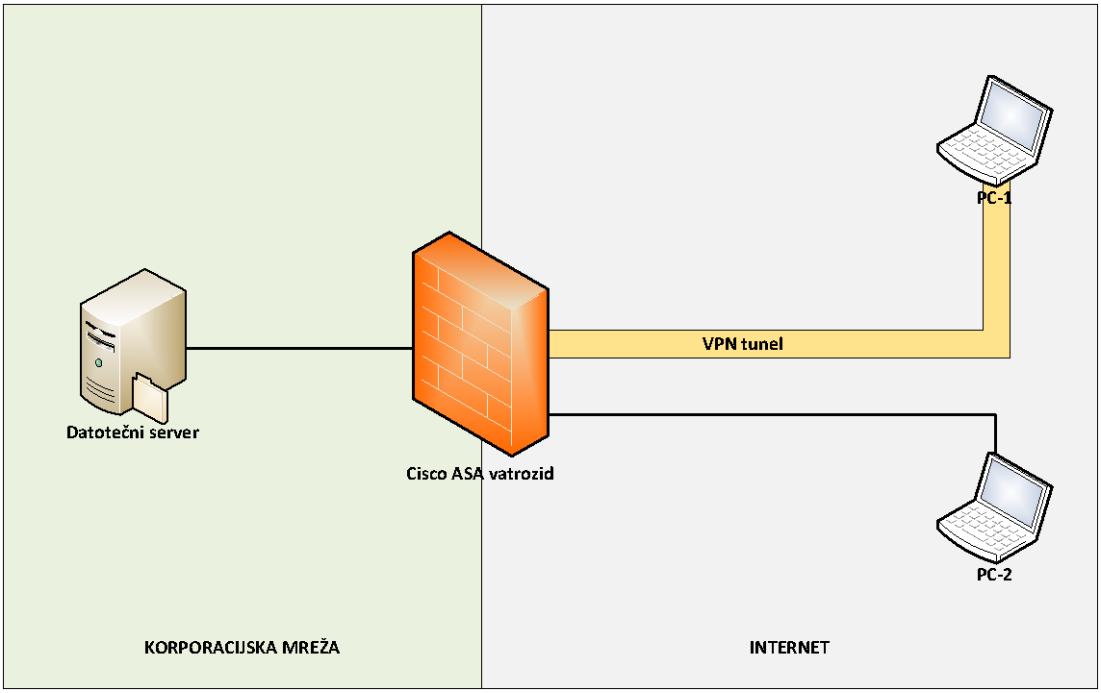
Tablica 1: Prikaz karakteristika scenarija

Scenarij / Karakteristika scenarija	Scenarij 1: Udaljeni pristup s Interneta računalu unutar lokalne mreže korporacije	Scenarij 2: Pristup Internetu s računala na korporativnoj mreži
Smjer pristupa	Nesigurna mreža → Sigurna mreža	Sigurna mreža → Nesigurna mreža
Resurs kojemu se pristupa	Datotečni server na korporacijskoj mreži	Web server na Internetu
Odredišni port resursa kojemu se pristupa	TCP/445 (MS Server Message Block v2)	TCP/80 (HTTP)
Aktivan VPN	DA	NE
Autentifikacija korisnika na vatroštitu	DA	NE
Korišten NAT	NE	DA
Korišten DHCP pool na vatroštitu	DA	NE

3.1. Udaljeni pristup s Interneta računalu unutar lokalne mreže korporacije

Unutar ovog scenarija, korisnik koji nije trenutačno na radnom mjestu želi pristupiti datotečnom serveru unutar korporacije kako bi preuzeo neke podatke. Mrežni administrator treba konfigurirati VPN postavke na vatroštitu, a korisnik treba preuzeti Cisco AnyConnect, instalirati ga na svoje računalo, povezati se na lokalnu mrežu i pristupiti na datotečni server.

Slika broj 2. prikazuje shemu ovog scenarija. Kao što prikazuje shema, na Internetu su 2 računala (PC-1 i PC-2) od kojih će PC-1 biti povezan na vatroštit putem VPN tunela. S unutarnje strane vatroštita, na korporacijskoj mreži, nalazi se datotečni server kojem pristupiti PC-1 kroz uspostavljeni VPN tunel.

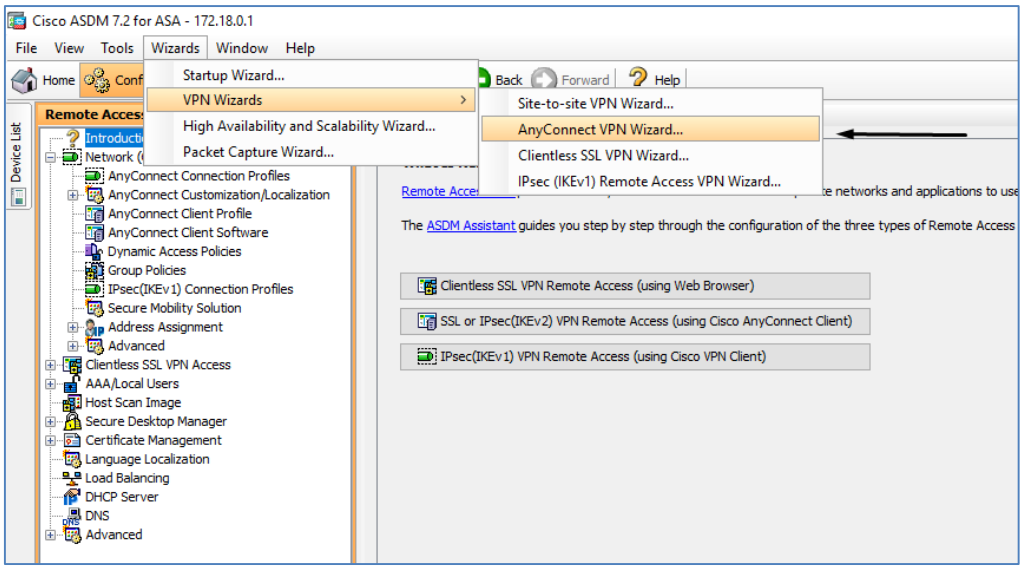


Slika 2: Shema scenarija 1

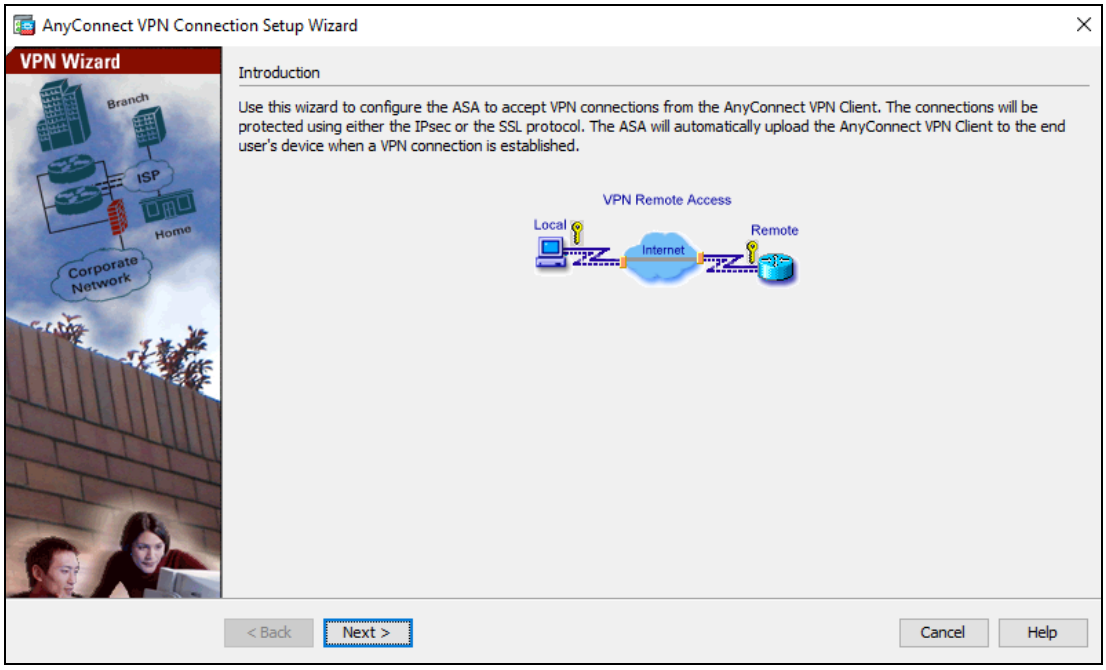
3.1.1. Konfiguriranje VPN-ovih postavki na vatroštitu

Korak 1: Odabir vrste VPN tunela

Mrežni administrator putem opcije „Wizards - VPN Wizards – AnyConnect VPN Wizard“ na Cisco ASDM-u odabire vrstu VPN tunela. Odabire se „SSL or IPSec (IKEv2) VPN Remote access (using Cisco AnyConnect Client)“.



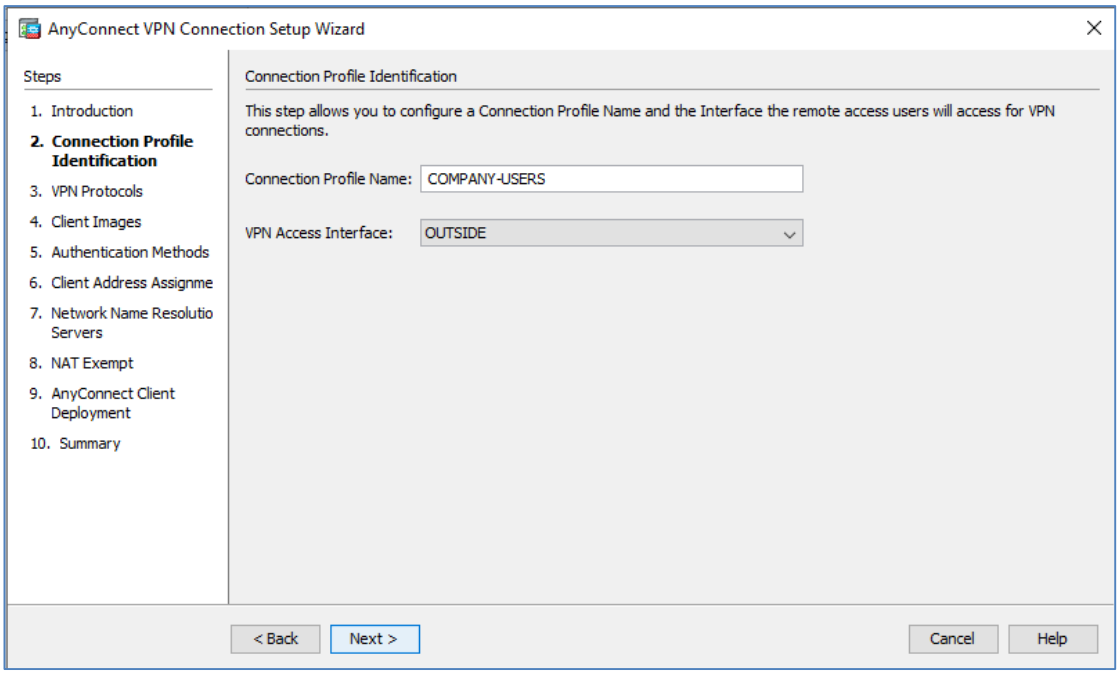
Slika 3: Odabir vrste VPN tunela



Slika 4: Objašnjenje Remote Access VPN tunela

Korak 2: Odabir imena VPN profila i vanjskog sučelja

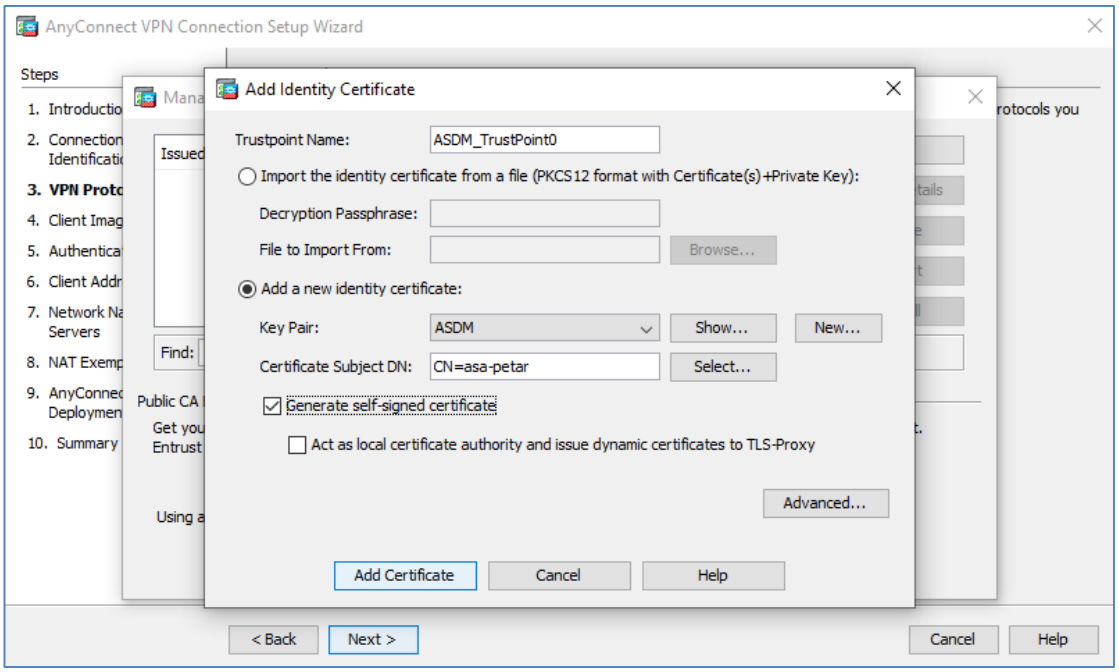
Ime VPN profila označava grupu korisnika koji će imati ista prava prilikom spajanja na korporacijsku mrežu putem VPN tunela. VPN tunel će se terminirati na odabranom sučelju „OUTSIDE“.



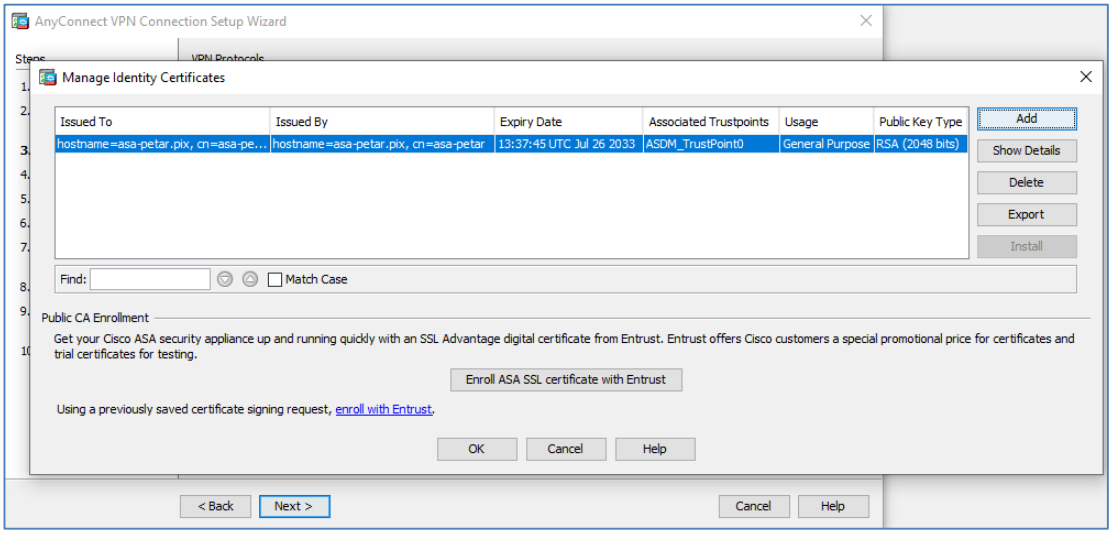
Slika 5: Odabir imena VPN profila i vanjskog sučelja

Korak 3: Odabir certifikata i VPN protokola

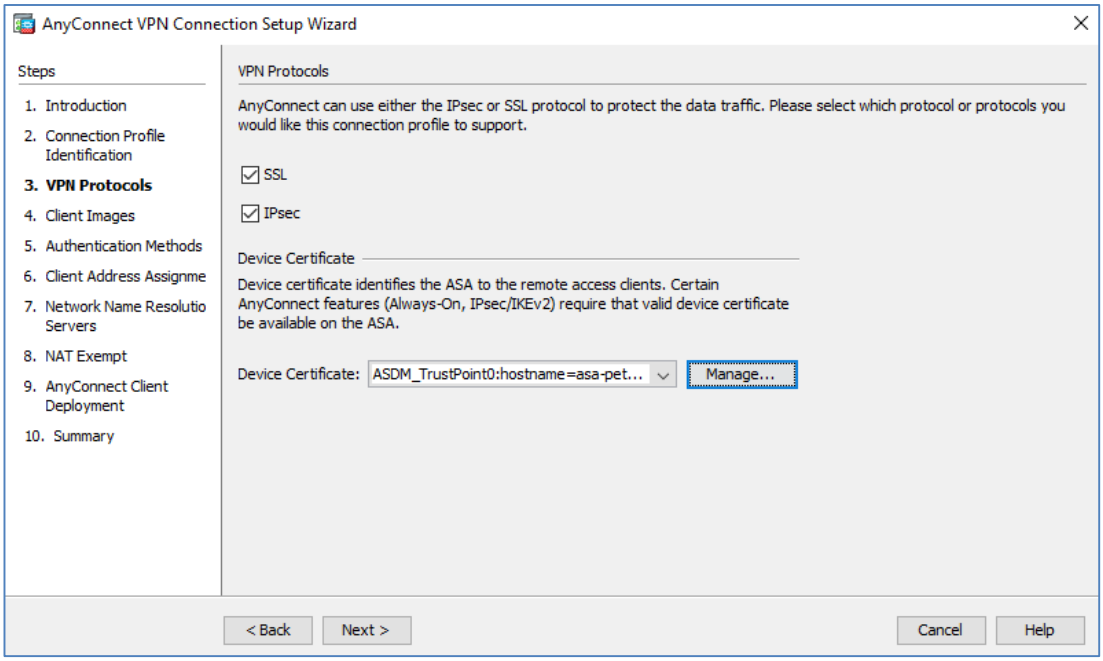
Kako bi se vatroštit identificirao korisnicima koji će se povezivati putem VPN tunela, u tu svrhu treba generirati digitalni certifikat na samom vatroštitu. Kako će vatroštit sam sebi generirati certifikat, ova vrsta certifikata je „self-signed“ certifikat.



Slika 6: Odabir certifikata (self-signed certifikat)



Slika 7: Odabir certifikata (ostali parametri)

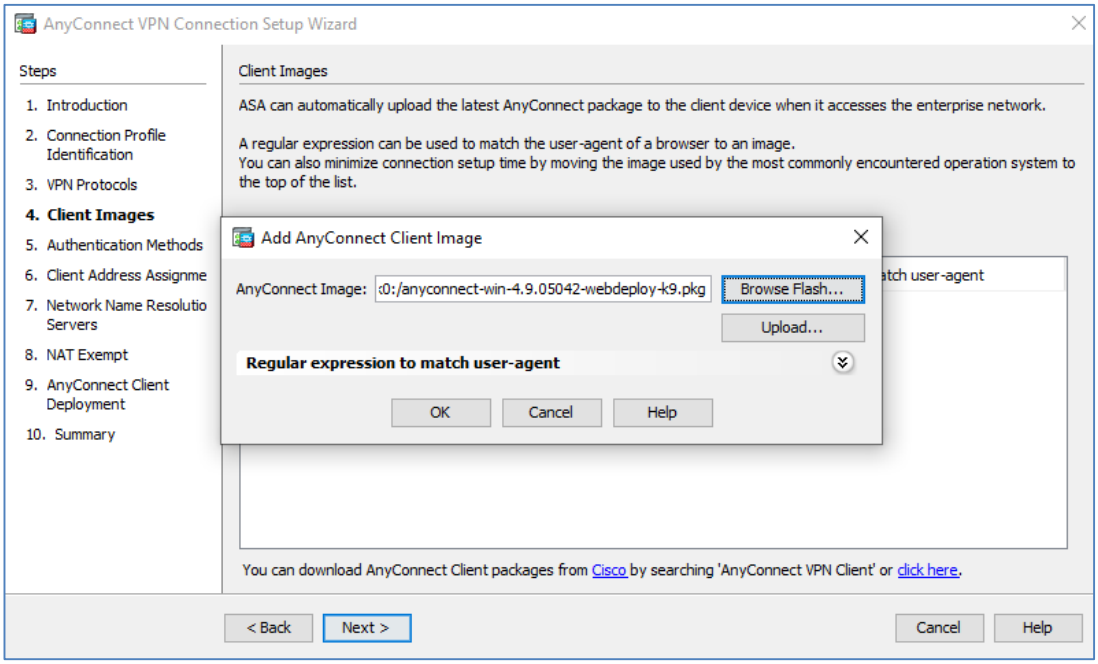


Slika 8: Odabir VPN protokola (SSL i IPsec)

Korak 4: Odabir načina instalacije Cisco AnyConnect softvera

Cisco AnyConnect softver se može instalirati na korisničko računalo na dva načina. Prvi način je da korisnik sam osigura instalacijske datoteke (npr. putem USB diska). Drugi način je da korisnik, nakon autentifikacije na vatroštitu, preuzme instalacijske datoteke sa web sučelja vatroštita. Da bi korisnici mogli preuzeti instalacijske datoteke, te datoteke se prvo moraju instalirati na vatroštit. Na slici 9 je

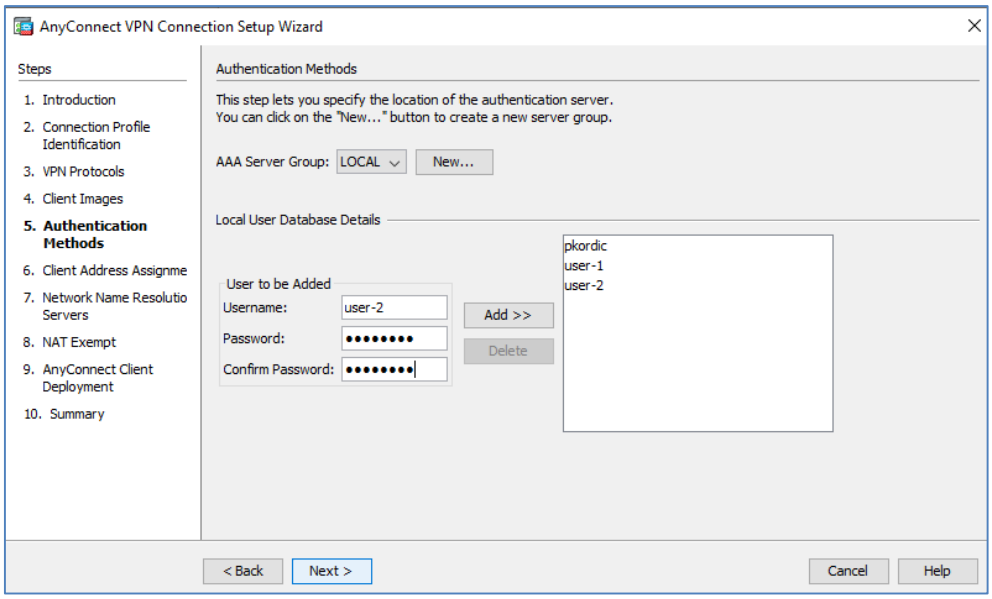
prikazan odabir već instaliranih instalacijskih datoteka koje će preuzeti korisnici nakon autentifikacije na vatroštitu.



Slika 9: Odabir načina instalacije Cisco AnyConnect softvera

Korak 5: Odabir metode autentifikacije i kreiranje korisnika

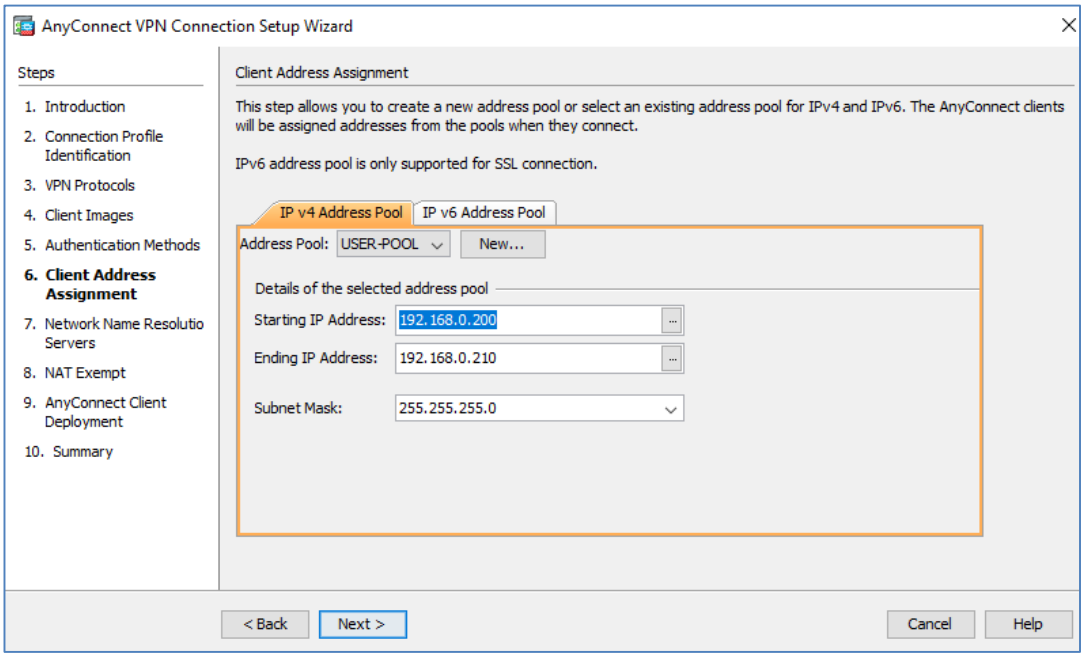
Kako u ovom scenariju nemamo eksterni server za autentifikaciju, odabiremo da će korisnici biti kreirano lokalno na vatroštitu. Za ovaj scenarij dodana su 2 korisnika, “user-1“ i “user-2“ i “pkordic“ kao administrator.



Slika 10: Odabir metode autentifikacije i kreiranje korisnika

Korak 6: Kreiranje raspona IP adresa

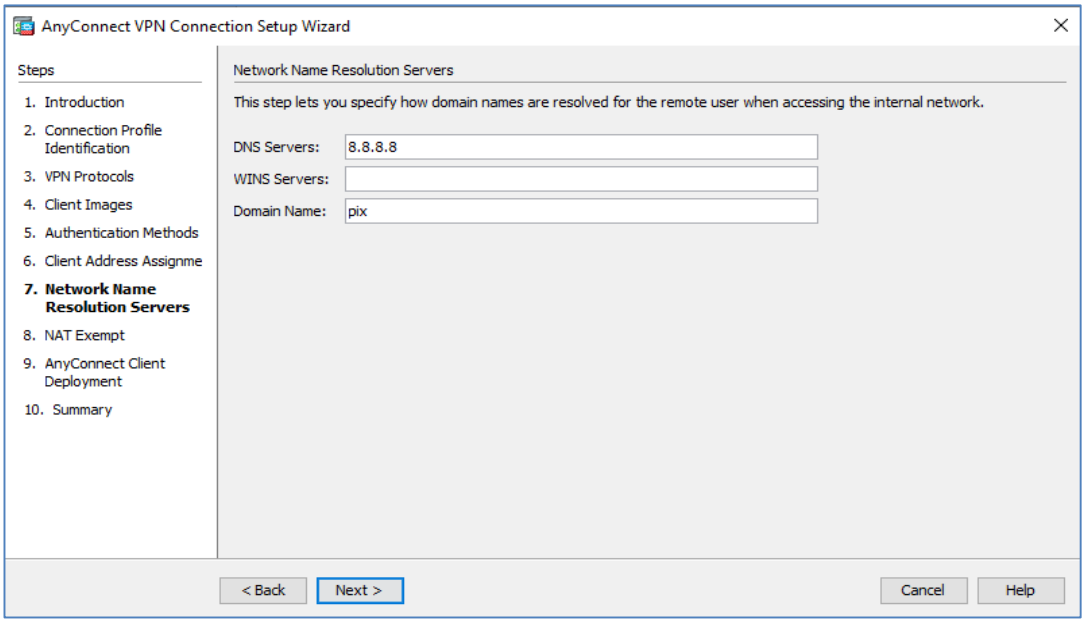
Potrebno je kreirati raspon privatnih IP adresa koje će biti automatski dodijeljene korisničkim računalima prilikom uspostave VPN tunela.



Slika 11: Kreiranje raspona IP adresa

Korak 7: Odabir DNS servera

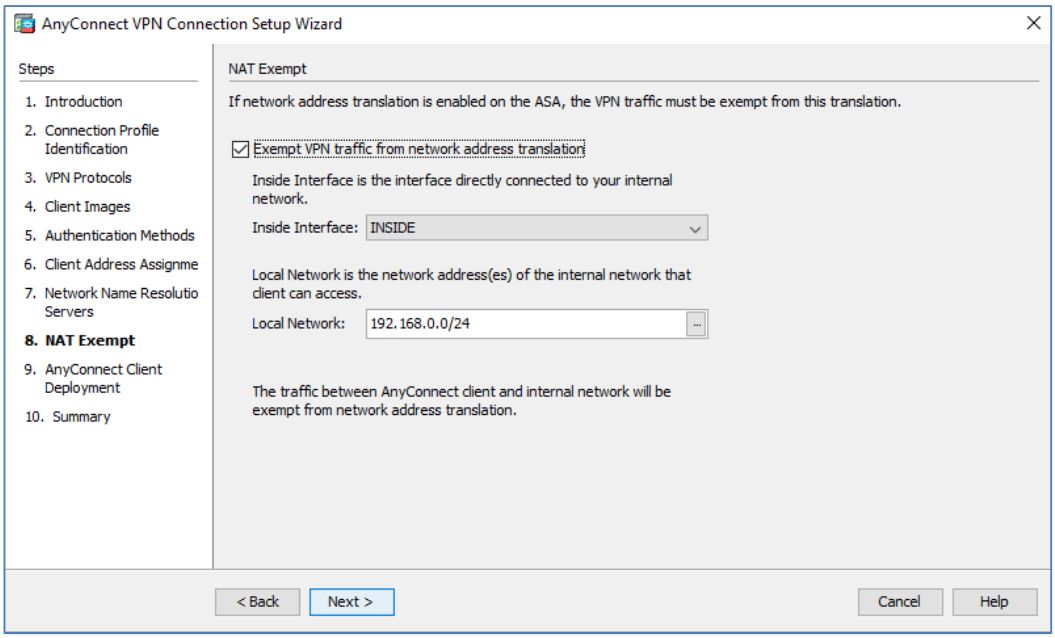
Potrebno je konfigurirati informacije o DNS serveru kojeg će koristiti korisnik nakon povezivanja na VPN. Radi jednostavnosti odabran je Google-ov DNS server s IPv4 adresom 8.8.8.8.



Slika 12. Odabir DNS servera

Korak 8: Izuzeće od translacije IP adresa

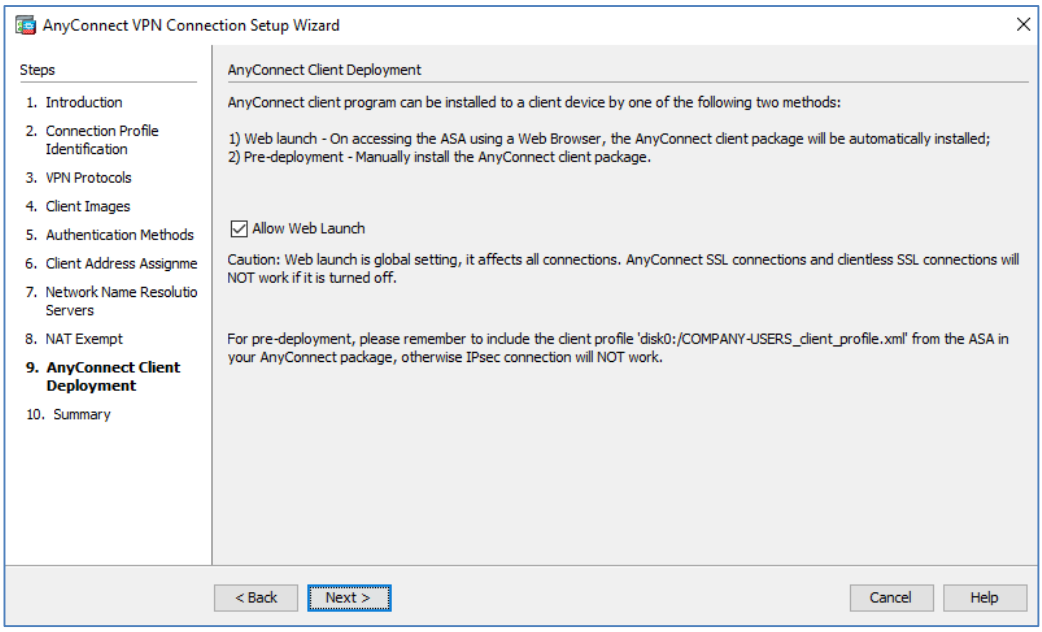
U ovom korak je konfigurirano da se ne translatiraju korisničke IP adrese dobivene putem DHCP protokola opisanog u 6. koraku. Nadalje, konfiguriran je mrežni raspon kojem mogu pristupiti korisnici putem VPN tunela.



Slika 13. Izuzeće od translacije IP adresa i mrežni raspon kojemu mogu pristupiti korisnici

Korak 9: Dopuštenje za preuzimanje instalacijskih datoteka za Cisco AnyConnect

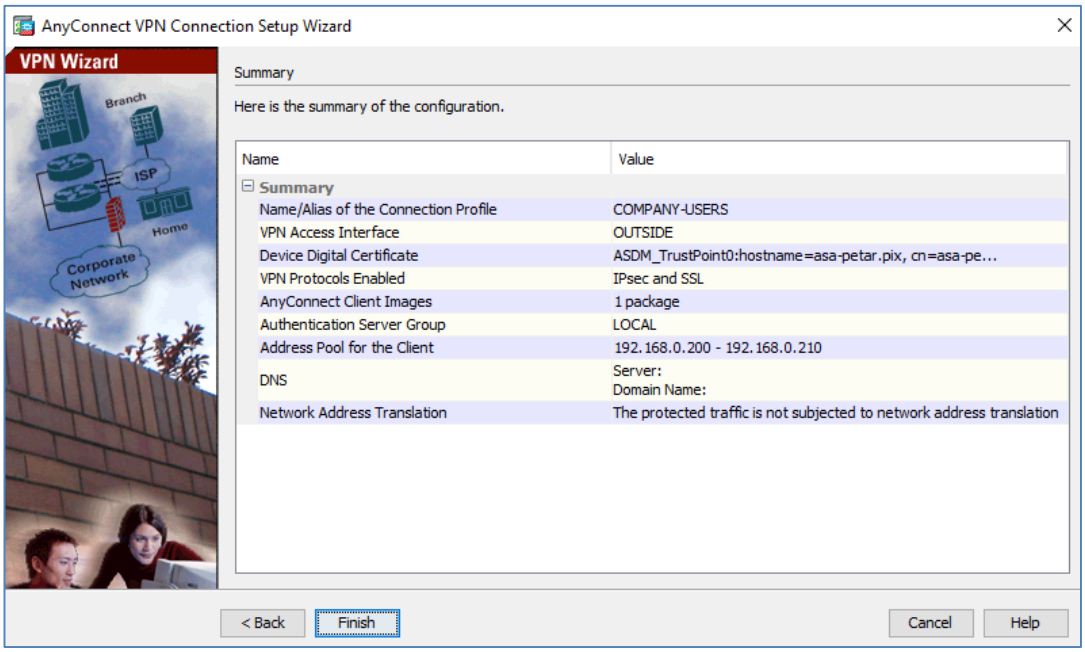
Postavkom „Allow Web Launch“ je omogućeno korisnicima da preuzmu instalacijske datoteke za Cisco AnyConnect program.



Slika 14. Dopuštenje za preuzimanje instalacijskih datoteka za Cisco AnyConnect

Korak 10: Sažetak VPN postavki

Na kraju je prikazan sažetak VPN postavki prema kojima će biti konfiguriran VPN tunel za korisnike u grupi „COMPANY-USERS“.

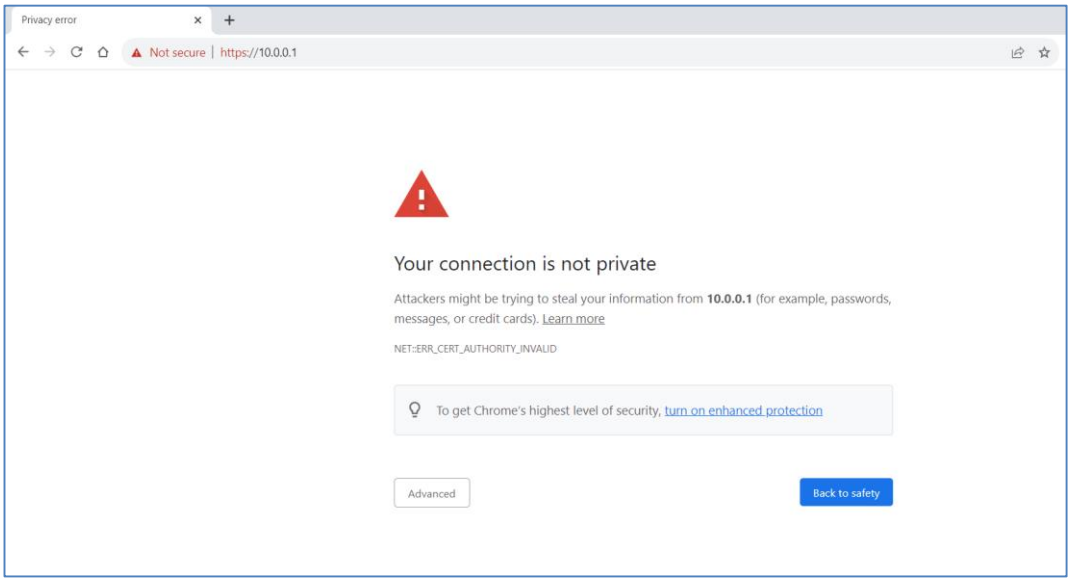


Slika 15. Sažetak VPN postavki

3.1.2. Pristup korisnika putem VPN tunela

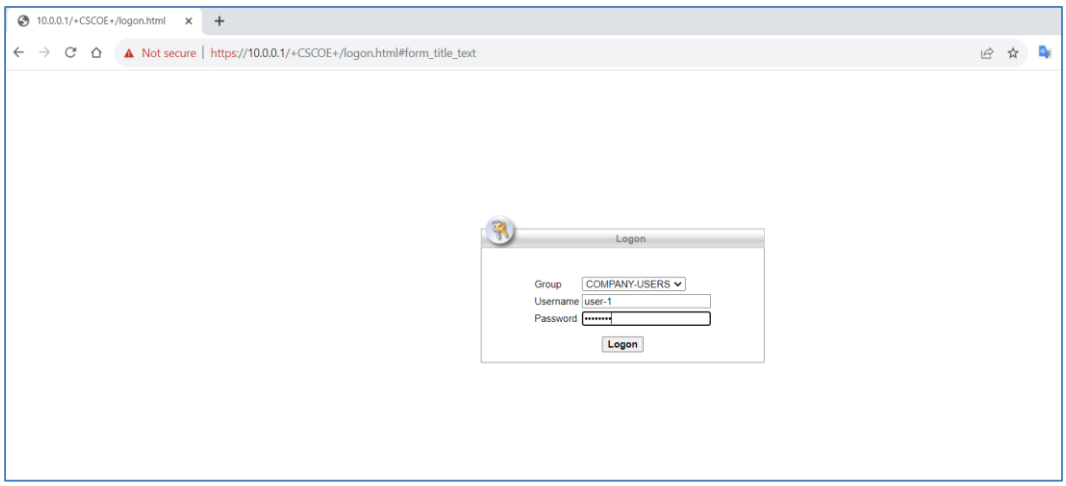
Korak 1: Inicijalno povezivanje na vatroštit

Korisnik se https protokolom spaja na vatroštit, upisujući u internetski preglednik IP adresu vanjskog sučelja vatroštita. Kako korisnikov internetski preglednik ne prepoznaje certifikat kojeg vatroštit koristi za https promet, javlja se upozorenje.



Slika 16: Inicijalno povezivanje na vatroštit

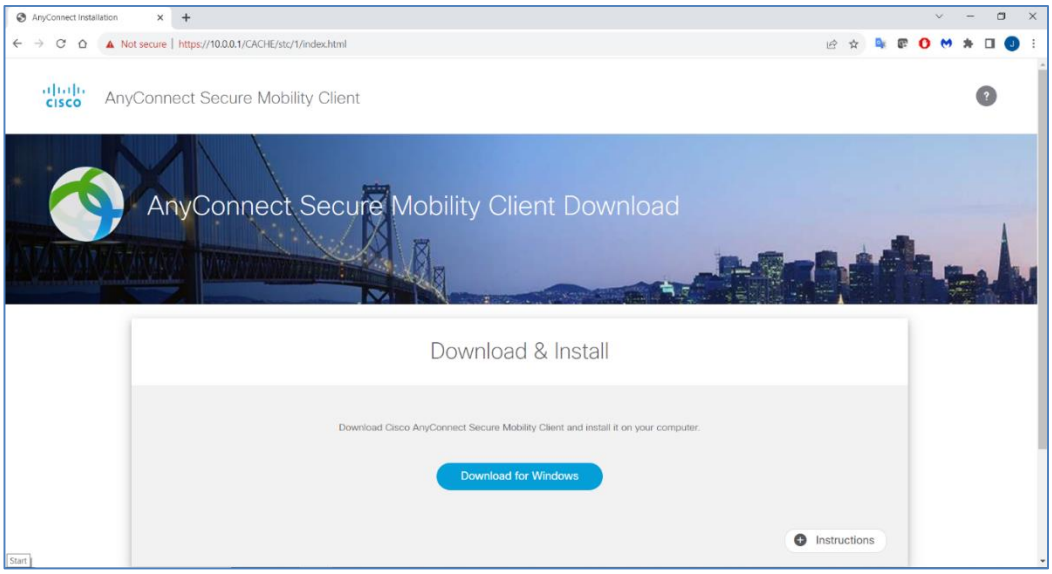
Opcija “Advanced“ preusmjerava korisnika na stranicu za prijavljivanje na vatroštit gdje može preuzeti Cisco AnyConnect instalacijske datoteke. Korisnik pripada grupi „COMPANY-USERS“ i prijavljuje se s prethodno definiranim podacima na vatroštitu, Username: user-1 i Password: 99887766.



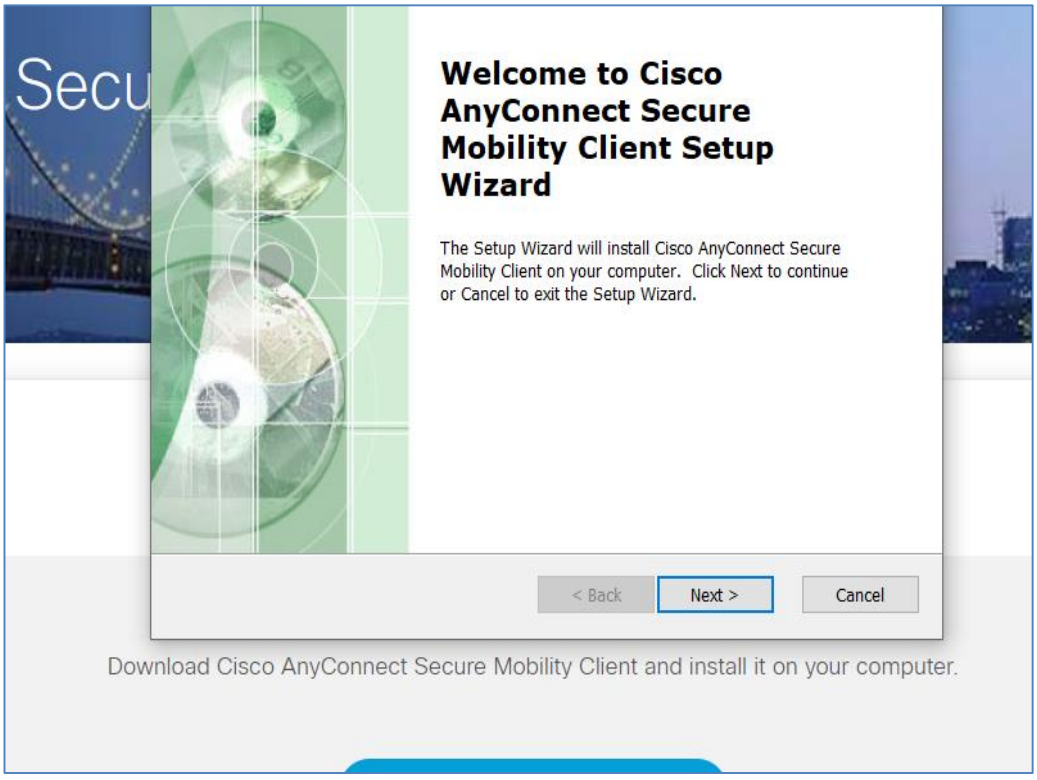
Slika 17: Korisnički podaci za prijavu na vatroštit

Korak 2: Preuzimanje instalacijskih datoteka i instaliranje Cisco AnyConnect

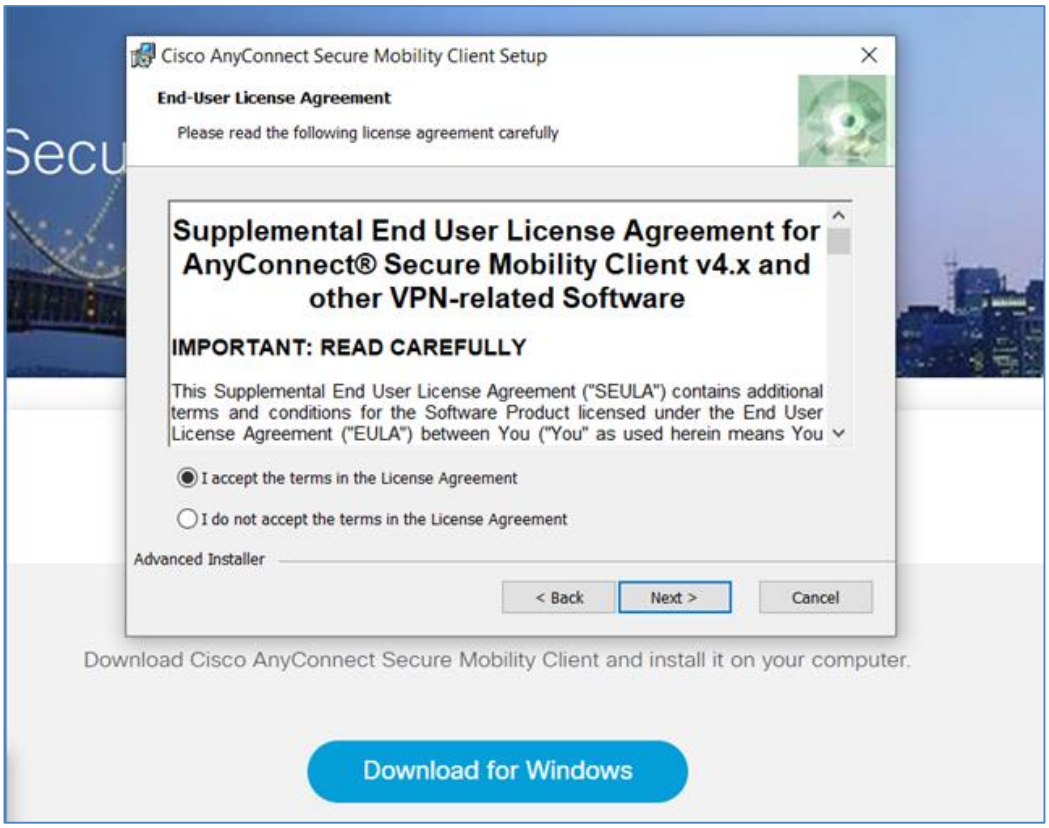
Nakon uspješne prijave, korisniku je prikazana stranica za preuzimanje instalacijskih datoteka za Cisco AnyConnect.



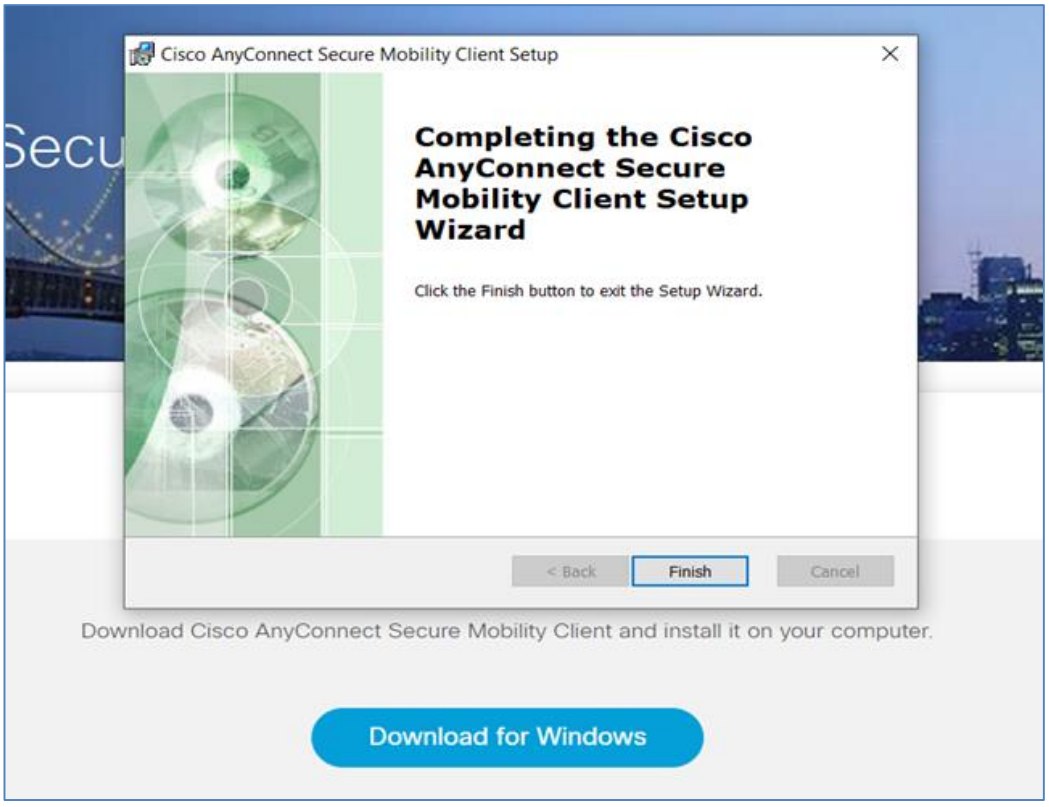
Slika 18: Preuzimanje instalacijskih datoteka za Cisco AnyConnect



Slika 19. Instaliranje Cisco AnyConnect: Prva stranica



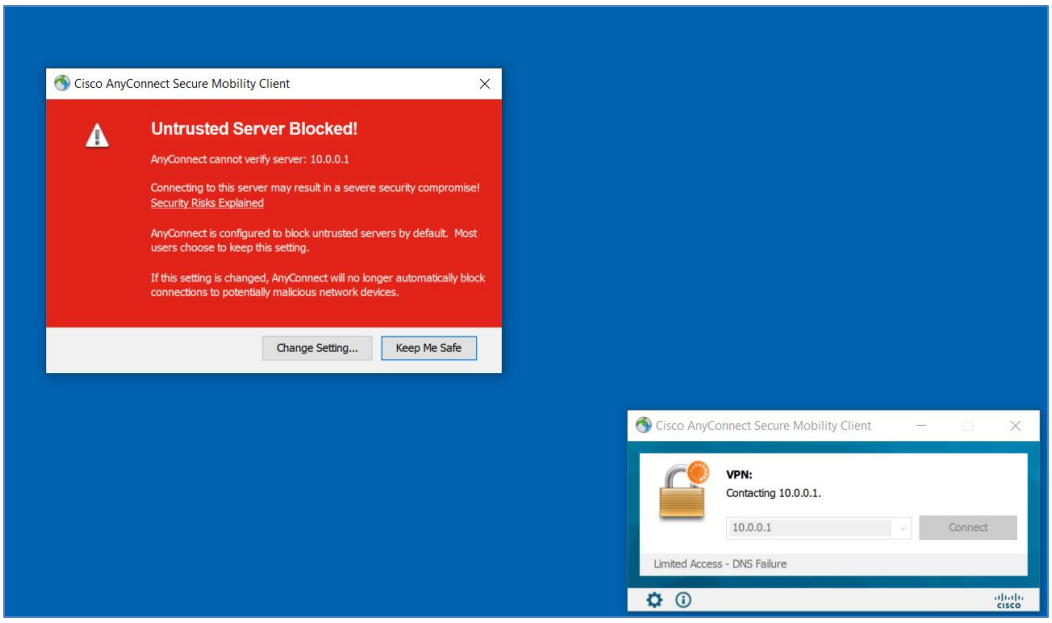
Slika 20. Instaliranje Cisco AnyConnect: Uvjeti korištenja



Slika 21. Instaliranje Cisco AnyConnect: Završetak

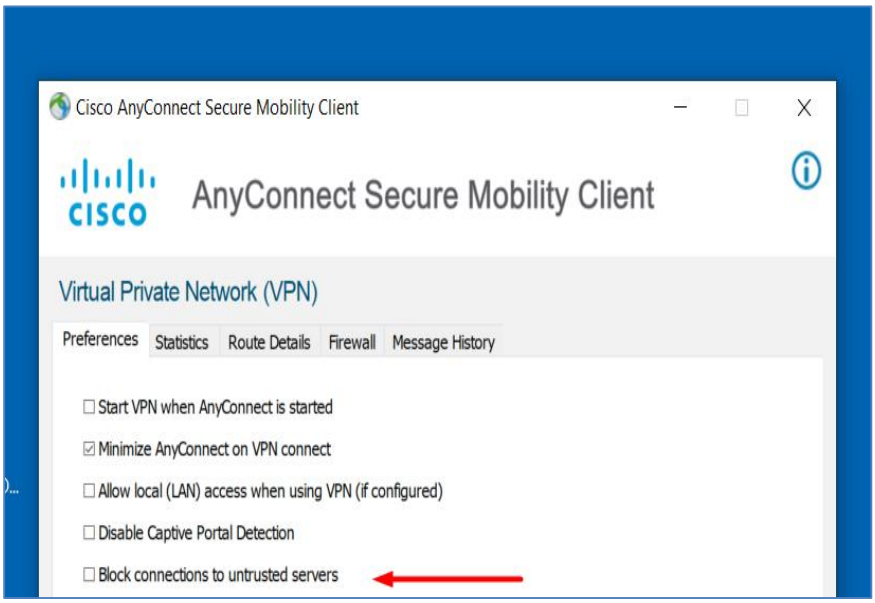
Korak 3: Inicijalno povezivanje putem Cisco AnyConnect

Kod inicijalnog povezivanja Cisco AnyConnect će javiti upozorenje da je blokirano povezivanje na nepovjerljiv VPN server. Razlog tome je isti kao i kod upozorenja koje javlja preglednik, samo ovaj put upozorenje javlja AnyConnect.



Slika 22. Cisco AnyConnect: upozorenje da je blokirano povezivanje na nepovjerljiv VPN server

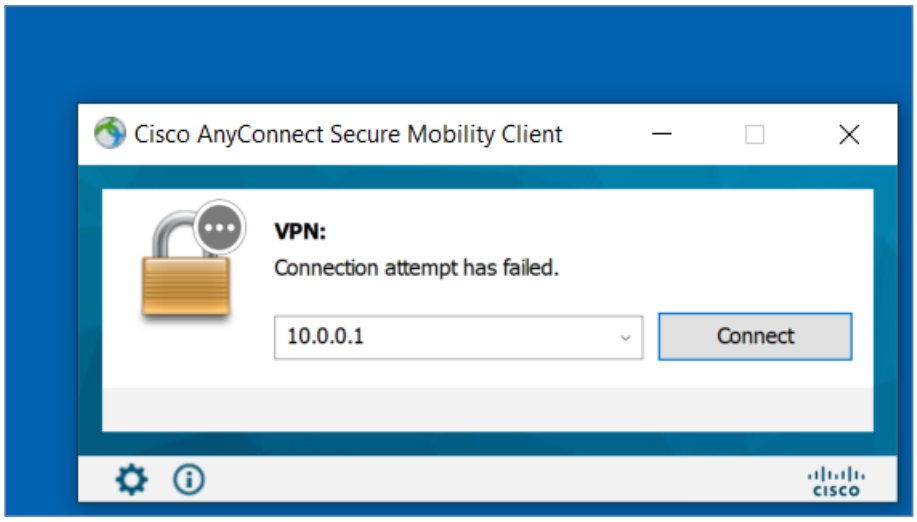
Ovaj problem se rješava tako da u postavkama Cisco AnyConnect programa odznačimo blokiranje nepovjerljivih VPN servera.



Slika 23. Cisco AnyConnect: Odznačavanje blokiranja nepovjerljivih VPN servera

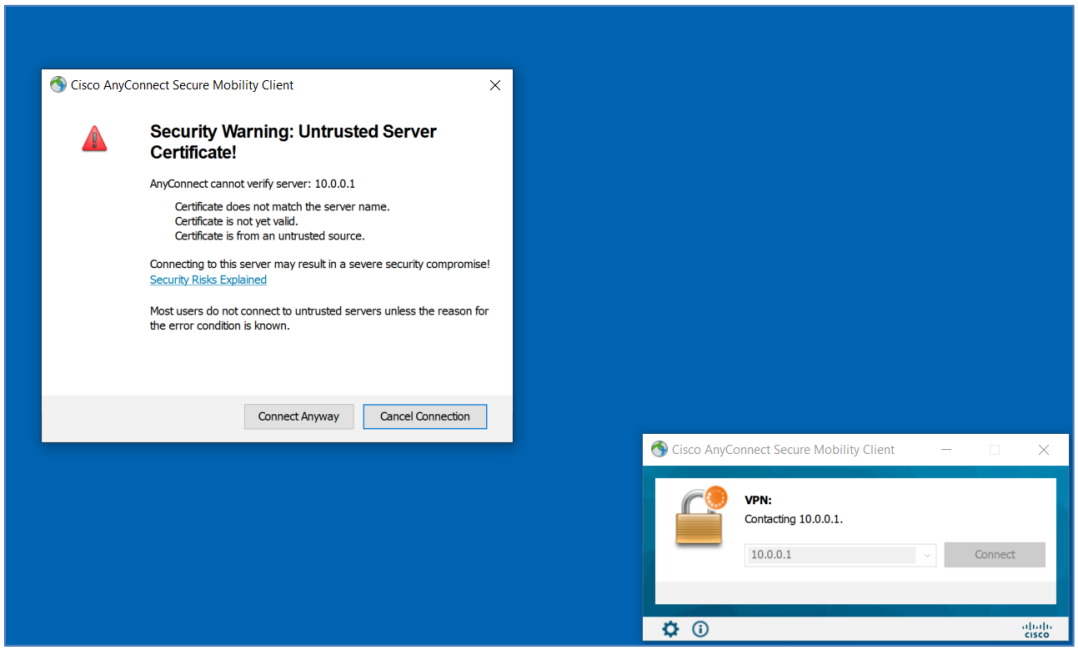
Korak 4: Ponovno spajanje i prijava na lokalnu mrežu

Nakon odznačavanja blokiranja nepovjerljivih VPN servera, korisnik mora opet pokrenuti povezivanje na vatroštit putem Cisco AnyConnect.

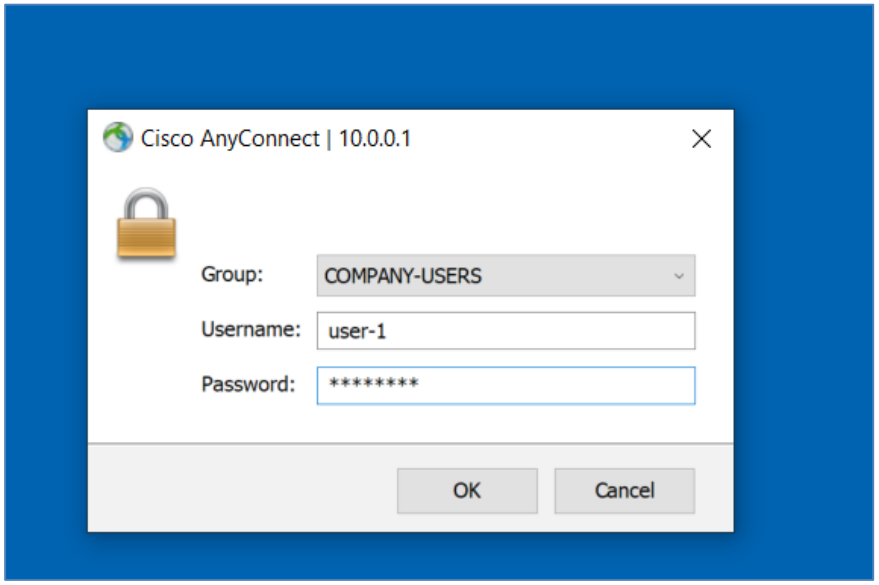


Slika 24. Cisco AnyConnect: ponovno pokretanje povezivanja na vatroštit

Cisco AnyConnect opet javlja upozorenje radi nepoznatog certifikata. Korisnik može odabrati opciju “Connect anyway“ zato što zna da je VPN server na kojeg se povezuje siguran.

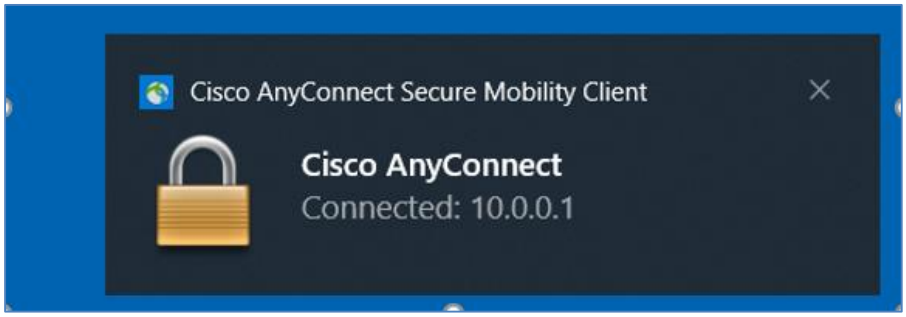


Slika 25. Cisco AnyConnect: ponovno pokretanje povezivanja na vatroštit

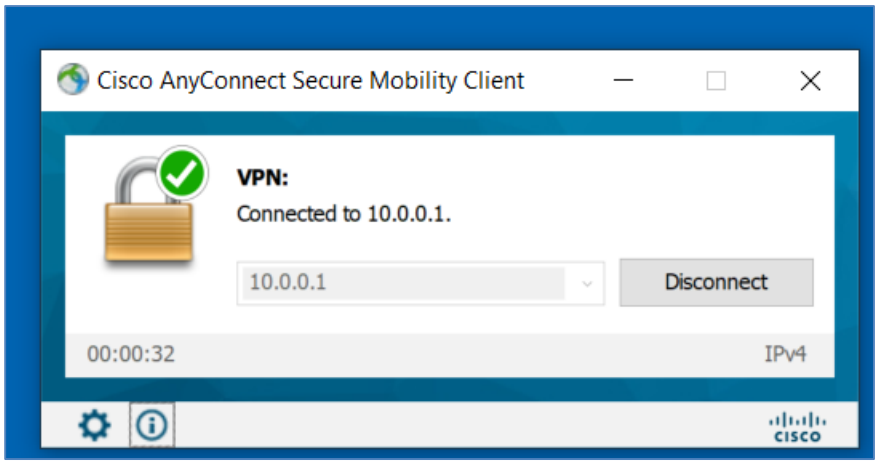


Slika 26. Cisco AnyConnect: Prijava na VPN server

Ako je korisnik unio ispravne podatke, u donjem desnom kutu doći će mu ova obavijest i ovako će mu sada izgledati Cisco AnyConnect.



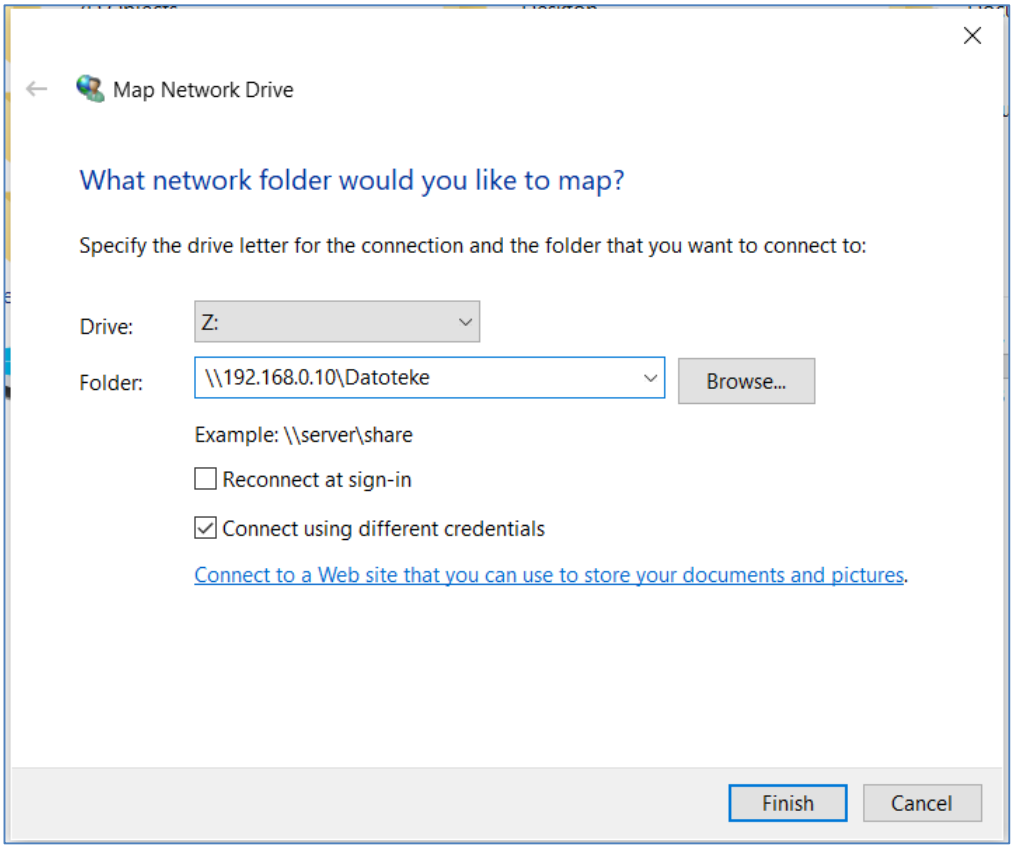
Slika 27. Cisco AnyConnect: Obavijest o uspješnoj prijavi



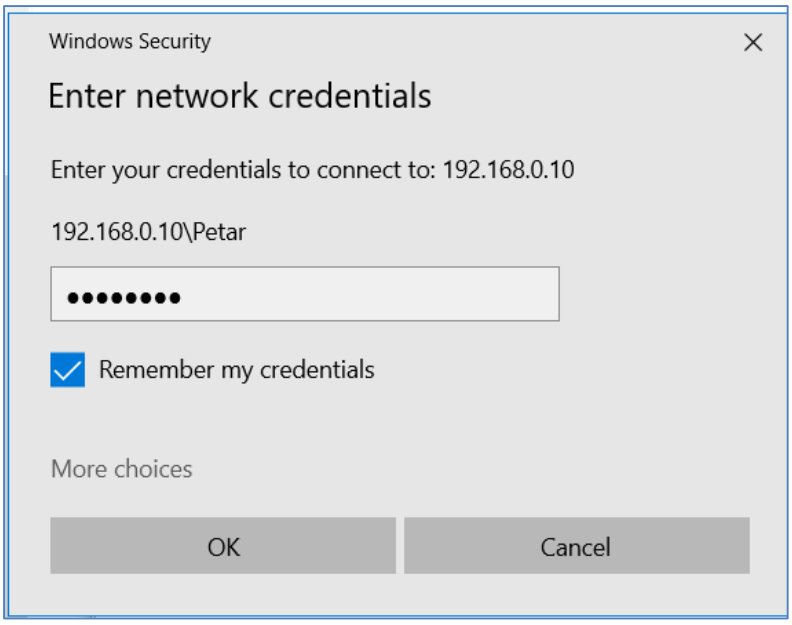
Slika 28. Cisco AnyConnect: Cisco AnyConnect nakon uspješne prijave

Korak 5: Prijava na datotečni server

Nakon što se korisnik uspješno povezao na vatroštit putem Cisco AnyConnect-a, može pokrenuti prijavu na datotečni server.



Slika 29. Pristup mapi na datotečnom serveru

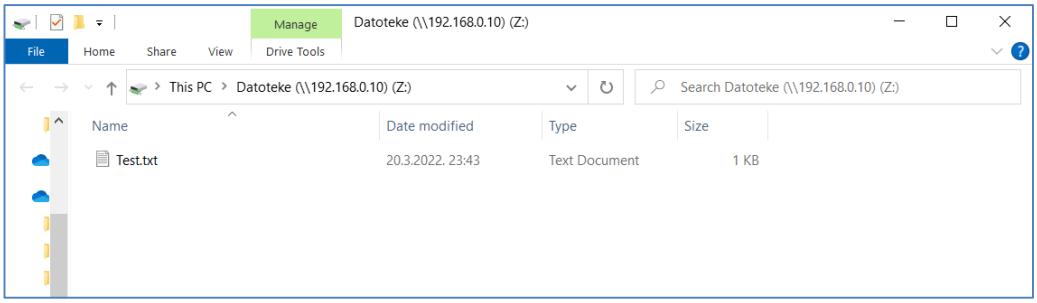


Slika 30. Pristup mapi na datotečnom serveru – nastavak

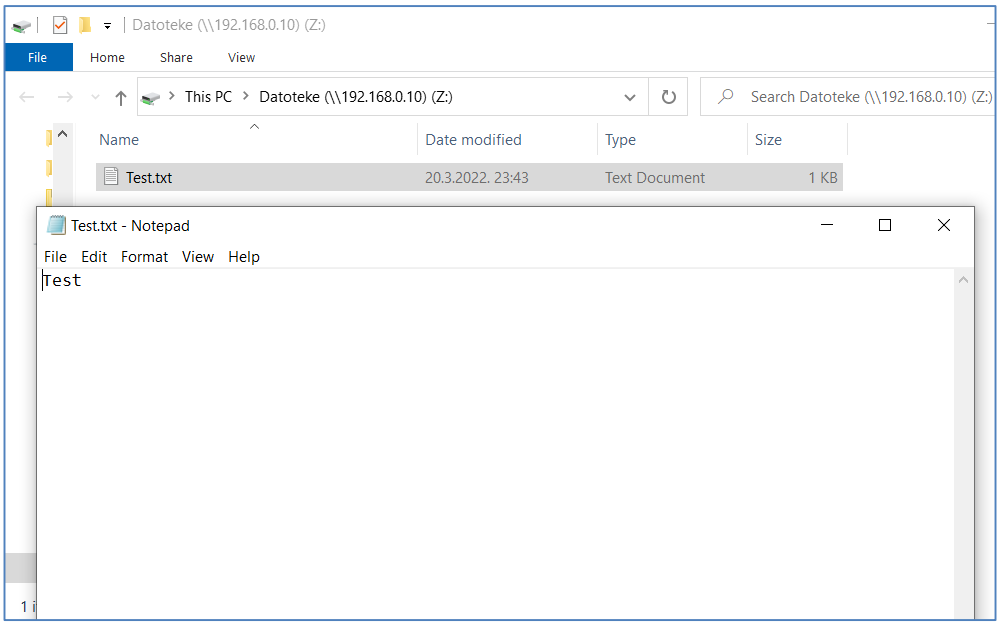
IP adresa datotečnog servera na korporacijskoj mreži je 192.168.0.10. Windows korisnik Petar je definiran na datotečnom serveru. Lozinka za korisnika Petar je 99887766.

Korak 6: Pristup datoteci na datotečnom serveru

Korisnik Petar se uspješno prijavio na datotečni server gdje mu je prikazana datoteka „Test.txt“.



Slika 31. Pristup datoteci na datotečnom serveru



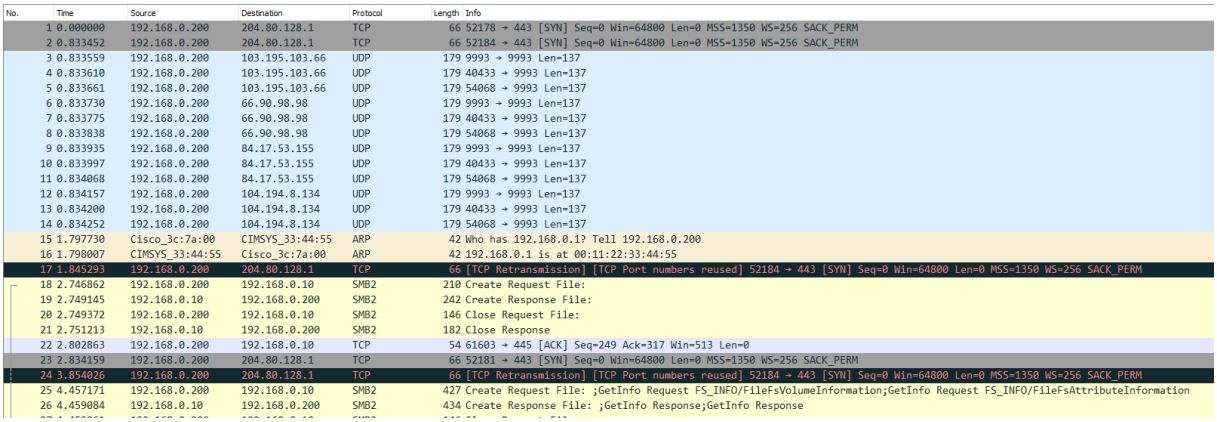
Slika 32. Otvaranje datoteke na datotečnom serveru

Korisnik Petar je uspješno otvorio datoteku na datotečnom serveru „Test.txt“.

3.1.3. Analiza mrežnog prometa u Wiresharku

Pomoću Wireshark aplikacije sniman je promet na računalu PC-1 u dva koraka.

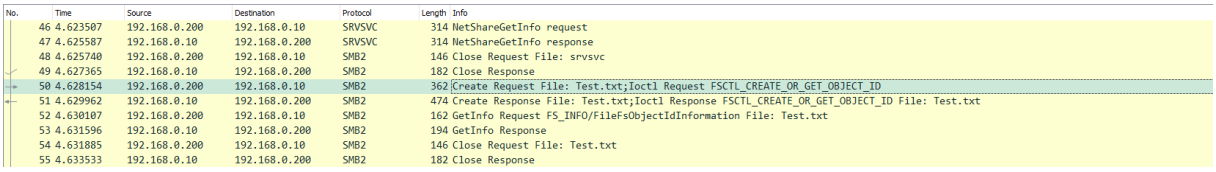
U prvom koraku se vidi nešifrirani promet između računala PC-1 i datotečnog servera, zato što je promet sniman na Cisco AnyConnect virtualnom sučelju (IP adresa 192.168.0.200). Spomenuto virtualno sučelje postaje aktivno na računalu PC-1 nakon što se aktivira Cisco AnyConnect VPN tunel. Od 18. retka se vidi da računalo PC-1 putem SMB2 protokola pokušava dohvatiti datoteku s datotečnog servera (IP adresa 192.168.0.10).



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.200	204.80.128.1	TCP	66	52178 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM
2	0.833452	192.168.0.200	204.80.128.1	TCP	66	52184 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM
3	0.833559	192.168.0.200	103.195.103.66	UDP	179	9993 → 9993 Len=137
4	0.833610	192.168.0.200	103.195.103.66	UDP	179	40433 → 9993 Len=137
5	0.833661	192.168.0.200	103.195.103.66	UDP	179	54068 → 9993 Len=137
6	0.833730	192.168.0.200	66.90.98.98	UDP	179	9993 → 9993 Len=137
7	0.833775	192.168.0.200	66.90.98.98	UDP	179	40433 → 9993 Len=137
8	0.833838	192.168.0.200	66.90.98.98	UDP	179	54068 → 9993 Len=137
9	0.833935	192.168.0.200	84.17.53.155	UDP	179	9993 → 9993 Len=137
10	0.833997	192.168.0.200	84.17.53.155	UDP	179	40433 → 9993 Len=137
11	0.834068	192.168.0.200	84.17.53.155	UDP	179	54068 → 9993 Len=137
12	0.834157	192.168.0.200	104.194.8.134	UDP	179	9993 → 9993 Len=137
13	0.834200	192.168.0.200	104.194.8.134	UDP	179	40433 → 9993 Len=137
14	0.834252	192.168.0.200	104.194.8.134	UDP	179	54068 → 9993 Len=137
15	1.797730	Cisco_3c:7a:00	CIMSYS_33:44:55	ARP	42	Who has 192.168.0.1? Tell 192.168.0.200
16	1.798007	CIMSYS_33:44:55	Cisco_3c:7a:00	ARP	42	192.168.0.1 is at 00:11:22:33:44:55
17	1.845293	192.168.0.200	204.80.128.1	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 52184 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM
18	2.746862	192.168.0.200	192.168.0.10	SMB2	210	Create Request File:
19	2.749145	192.168.0.10	192.168.0.200	SMB2	242	Create Response File:
20	2.749372	192.168.0.200	192.168.0.10	SMB2	146	Close Request File:
21	2.751213	192.168.0.10	192.168.0.200	SMB2	182	Close Response
22	2.802863	192.168.0.200	192.168.0.10	TCP	54	61603 → 445 [ACK] Seq=249 Ack=317 Win=513 Len=0
23	2.834159	192.168.0.200	204.80.128.1	TCP	66	52181 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM
24	3.854026	192.168.0.200	204.80.128.1	TCP	66	[TCP Retransmission] [TCP Port numbers reused] 52184 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1350 WS=256 SACK_PERM
25	4.457171	192.168.0.200	192.168.0.10	SMB2	427	Create Request File: ;GetInfo Request FS_INFO/FileFsVolumeInformation;GetInfo Request FS_INFO/FileFsAttributeInformation
26	4.459084	192.168.0.10	192.168.0.200	SMB2	434	Create Response File: ;GetInfo Response;GetInfo Response

Slika 33. Wireshark – inicijalna komunikacija na vitrualnom sučelju

Slika 34. prikazuje ime datoteke koja je tražena. U opisu retka 50. i 51. vidi se ime tražene datoteke „Text.txt“.



No.	Time	Source	Destination	Protocol	Length	Info
46	4.623507	192.168.0.200	192.168.0.10	SRVSVC	314	NetShareGetInfo request
47	4.625587	192.168.0.10	192.168.0.200	SRVSVC	314	NetShareGetInfo response
48	4.625740	192.168.0.200	192.168.0.10	SMB2	146	Close Request File: srvsvc
49	4.627365	192.168.0.10	192.168.0.200	SMB2	182	Close Response
50	4.628154	192.168.0.200	192.168.0.10	SMB2	362	Create Request File: Test.txt;Ioctl Request FSCTL_CREATE_OR_GET_OBJECT_ID
51	4.629962	192.168.0.10	192.168.0.200	SMB2	474	Create Response File: Test.txt;Ioctl Response FSCTL_CREATE_OR_GET_OBJECT_ID File: Test.txt
52	4.630107	192.168.0.200	192.168.0.10	SMB2	162	GetInfo Request FS_INFO/FileFsObjectIdInformation File: Test.txt
53	4.631596	192.168.0.10	192.168.0.200	SMB2	194	GetInfo Response
54	4.631885	192.168.0.200	192.168.0.10	SMB2	146	Close Request File: Test.txt
55	4.633533	192.168.0.10	192.168.0.200	SMB2	182	Close Response

Slika 34. Wireshark – detalji o komunikaciji na virtualnom sučelju

U drugom koraku se vidi samo šifrirani promet zato što je sniman na fizičkom Ethernet sučelju računala PC-1 (IP adresa 10.0.0.100), a u toj točci je promet već šifriran.

No.	Time	Source	Destination	Protocol	Length	Info
8	4.567021	10.0.0.100	10.0.0.1	TCP	66	56096 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
9	4.567722	10.0.0.1	10.0.0.100	TCP	60	443 → 56096 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
10	4.567840	10.0.0.100	10.0.0.1	TCP	54	56096 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11	4.594984	10.0.0.100	10.0.0.1	TLSv1.2	571	Client Hello
12	4.595653	10.0.0.1	10.0.0.100	TCP	60	443 → 56096 [ACK] Seq=1 Ack=518 Win=32768 Len=0
13	4.601150	10.0.0.1	10.0.0.100	TLSv1.2	1245	Server Hello, Certificate, Server Key Exchange, Server Hello Done
14	4.655721	10.0.0.100	10.0.0.1	TCP	54	56096 → 443 [ACK] Seq=518 Ack=1192 Win=63049 Len=0
15	9.829371	10.0.0.100	10.0.0.1	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
16	9.830902	10.0.0.1	10.0.0.100	TCP	60	443 → 56096 [ACK] Seq=1192 Ack=644 Win=32768 Len=0
17	9.830902	10.0.0.1	10.0.0.100	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
18	9.832024	10.0.0.100	10.0.0.1	TLSv1.2	1253	Application Data
19	9.832819	10.0.0.1	10.0.0.100	TCP	60	443 → 56096 [ACK] Seq=1243 Ack=1843 Win=32768 Len=0
20	9.834538	10.0.0.1	10.0.0.100	TLSv1.2	552	Application Data
21	9.834538	10.0.0.1	10.0.0.100	TLSv1.2	764	Application Data
22	9.834538	10.0.0.1	10.0.0.100	TLSv1.2	90	Application Data
23	9.834631	10.0.0.100	10.0.0.1	TCP	54	56096 → 443 [ACK] Seq=1843 Ack=2487 Win=64240 Len=0

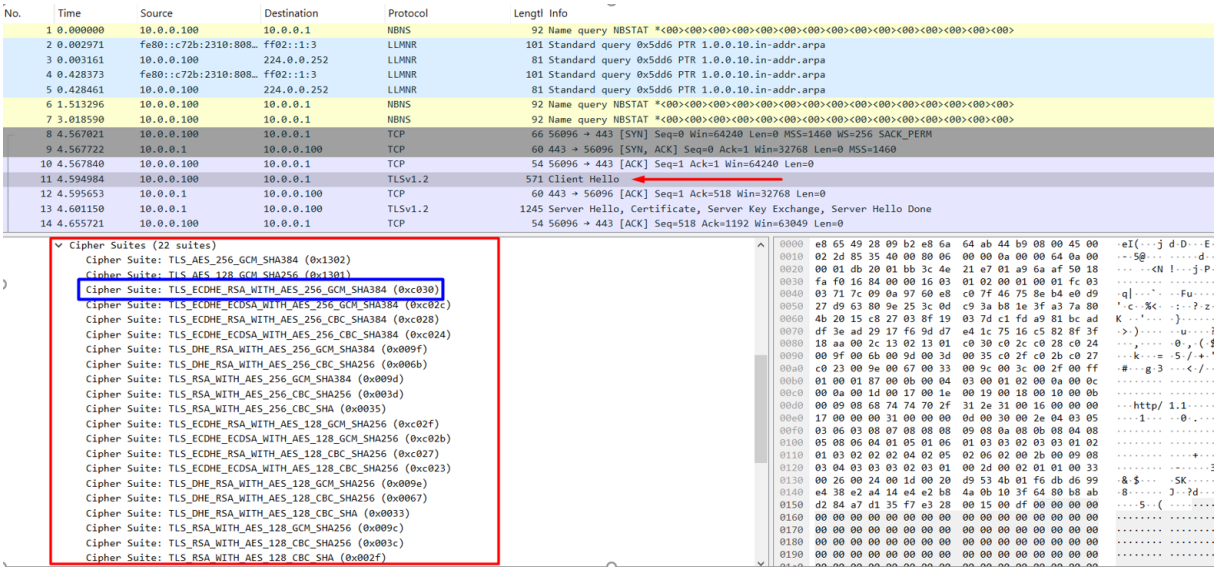
Slika 35. Wireshark snimka – inicijalna komunikacija: uspostava VPN tunela

Korisnik pokreće Cisco AnyConnect i kreira se VPN tunel između računala PC-1 i vanjskog sučelja vatroštita. Komunikacija unutar VPN tunela je šifrirana i Wireshark ne može pročitati tu komunikaciju. Za šifriranje se koristi DTLSv1.2 protokol koji je baziran na TLS-u.

No.	Time	Source	Destination	Protocol	Length	Info
145	21.725970	10.0.0.100	10.0.0.1	DTLSv1.2	176	Application Data
146	21.726059	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
147	21.726118	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
148	21.726162	10.0.0.100	10.0.0.1	DTLSv1.2	136	Application Data
149	21.726199	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
150	21.726235	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
151	21.726274	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
152	21.726309	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
153	21.726345	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
154	21.726384	10.0.0.100	10.0.0.1	DTLSv1.2	141	Application Data
155	21.726424	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
156	21.726461	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
157	21.726632	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
158	21.726681	10.0.0.100	10.0.0.1	DTLSv1.2	120	Application Data
159	21.726725	10.0.0.100	10.0.0.1	DTLSv1.2	139	Application Data
160	21.726761	10.0.0.100	10.0.0.1	DTLSv1.2	365	Application Data

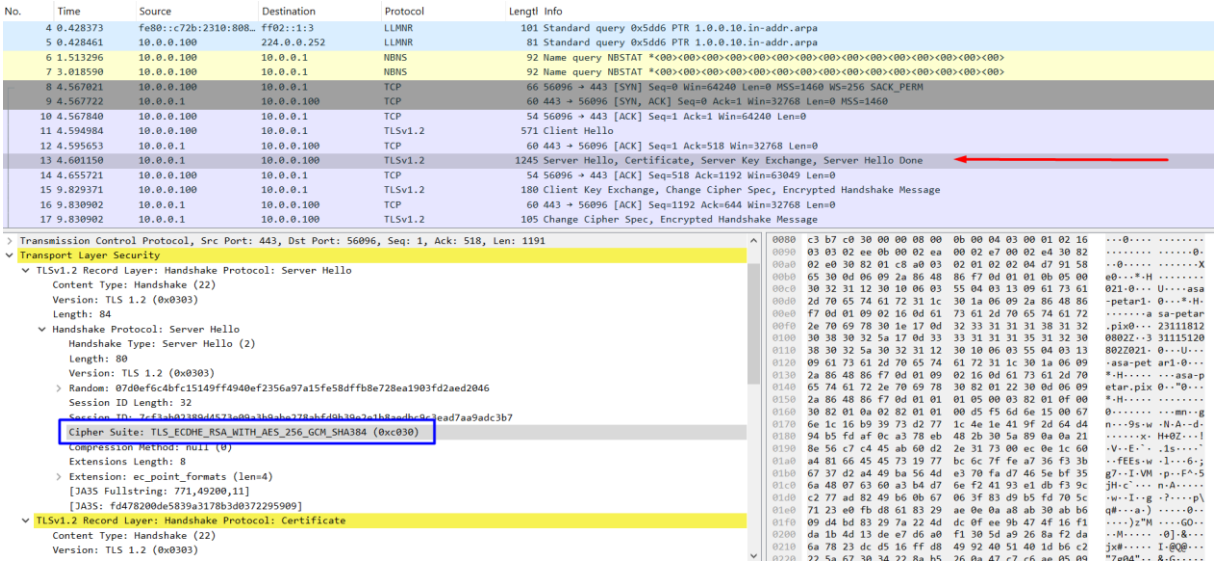
Slika 36. Wireshark snimka – šifrirana komunikacija putem VPN tunela

Slika 37. prikazuje sadržaj paketa 11 u Wireshark snimci. U tom paketu nalazi se upit PC-1 prema vatroštitu s popisom kriptografskih skupova koji će se mogu koristiti za sigurnu komunikaciju. Crvenim pravokutnikom je označen popis skupova koje PC-1 može koristiti. Plavim pravokutnikom je označen kriptografski skup kojeg će vatroštit odabrati.



Slika 37. Wireshark snimka - Client Hello (paket 11)

Slika 38. prikazuje odgovor od strane vatroštita u paketu 13. U sadržaju paketa 13 vidi se odabrani kriptografski skup „Cipher Suite: TLS_ECHE_RSA_WITH_AES_256_GCM_SHA384 (0x030)“. Na slici je označen s plavim pravokutnikom kao i na prethodnoj slici.

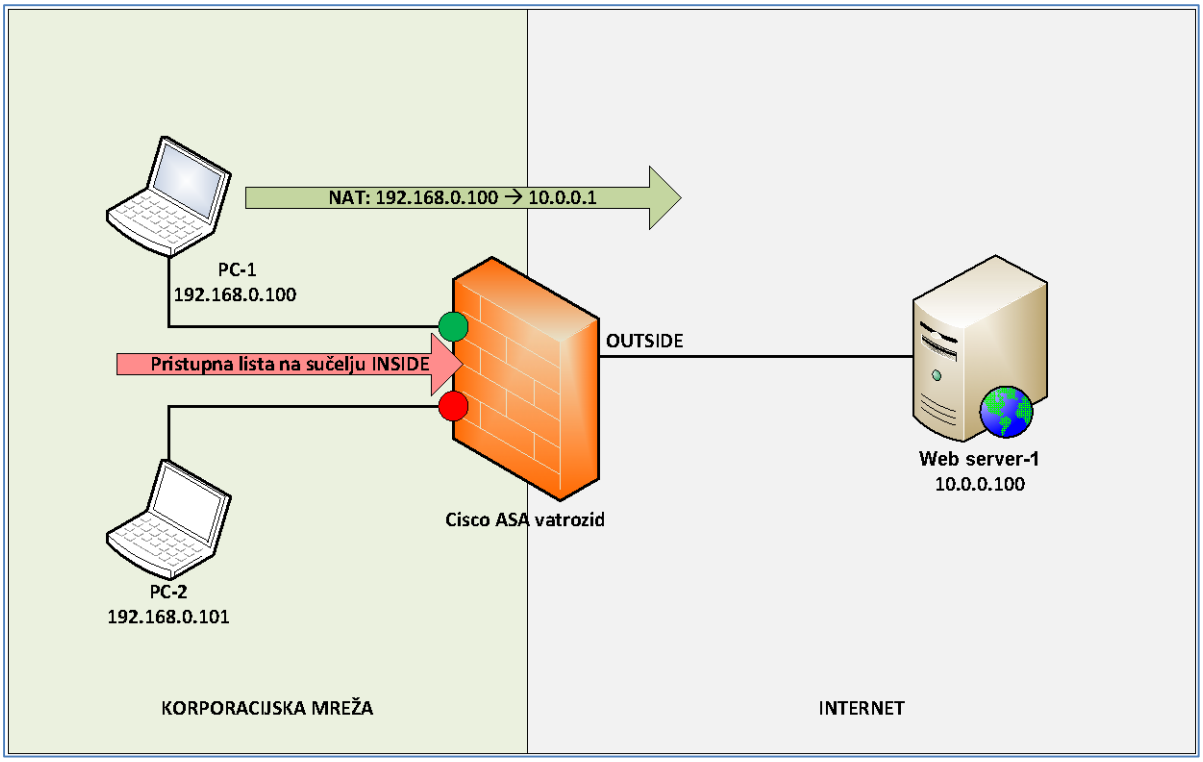


Slika 38. Wireshark snimka - Sever Hello (paket 13)

3.2. Pristup Internetu s računala na korporativnoj mreži

Kako bi računalo na korporativnoj mreži moglo pristupiti Internetu na vatroštitu je potrebno konfigurirati pristupnu listu i translaciju IP adresa (eng. *Network Address Translation - NAT*). Pristupne liste definiraju može li računalo ili skupina računala povezana na jedno sučelje vatroštita pristupiti drugom računalu ili skupini računala povezanim na drugim sučeljima vatroštita.

U ovom scenariju bit će definirana pristupna lista koja dopušta računalu PC-1 s korporacijske mreže pristup Web serveru Web server-1 na Internetu. Kako u laboratorijskom okruženju nema javnih IP adresa, javne IP adrese su simulirane uz pomoć privatnih IP adresa iz raspona 10.0.0.0/24. Razlog tomu je taj što korištenje javnih IP adresa nije besplatno.



Slika 39. Shema scenarija 2

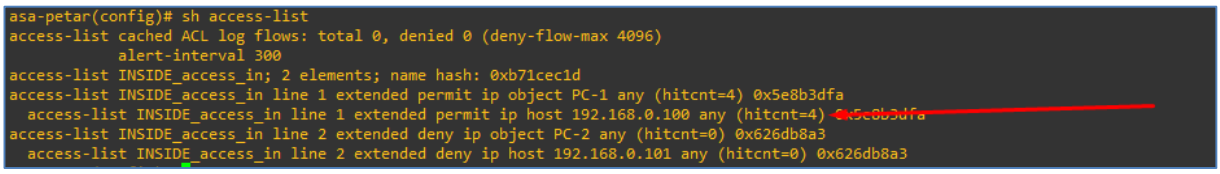
3.2.1. Pristupna lista

Na INSIDE sučelju vatroštita primijenjena je pristupna lista koja definira:

1. PC-1 može pristupiti na Web server-1.

2. PC-1 ne može pristupiti na Web server-1.

Radi jednostavnosti pristupne liste korišten je parametar „any“ umjesto IP adrese Web server-1.



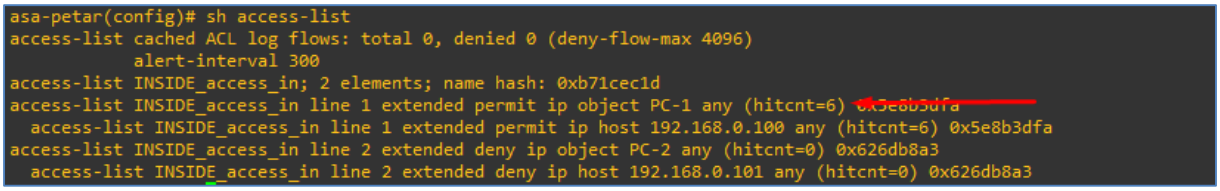
Slika 40. Pristupna lista

Za rad s pristupnim listama korištena je aplikacija PuTTY. Naredba za prikaz pristupnih listi je „sh access-list“. U 3. retku na slici 40 vidljivo je da ova pristupna lista ima naziv „INSIDE_access_in“ i unutar nje su 2 linije.

Linija 1 definira da računalo PC-1 može pristupiti vanjskim serverima na Internetu jer linija sadrži parametre „permit“ i „any“ koji omogućuju računalu PC-1 pristup bilo kojoj destinacijskoj IP adresi. Vidljiva je i druga verzija linije 1 u kojoj umjesto imena objekata pišu njihove IP adrese.

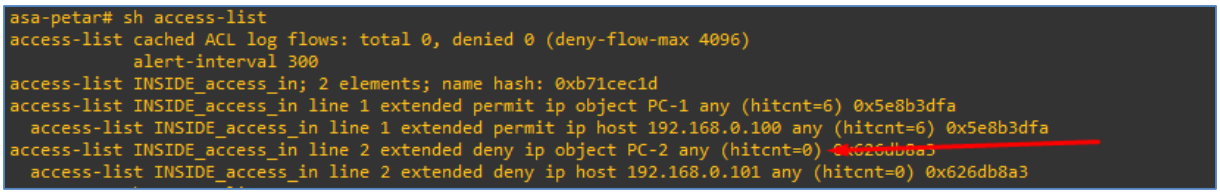
Linija 2 definira da računalo PC-2 ne može pristupiti vanjskim serverima na Internetu jer linija sadrži parametre „deny“ i „any“ koji zabranjuju računalu PC-2 pristup bilo kojoj destinacijskoj IP adresi.

Korisnu informaciju o prometu daje parametar „hitcnt“ koji prikazuje koliko puta je korištena određena linija u pristupnoj listi.

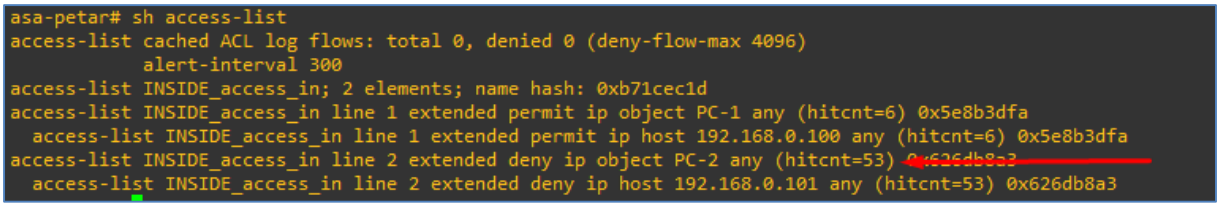


Slika 41. Prikaz „hitcnt“

Sljedeće dvije slike prikazuju parametar „hitcnt“ prije i nakon pokušaja pristupa računala PC-2 na Web server-1.



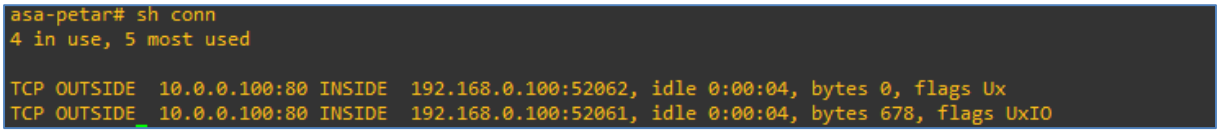
Slika 42. Prikaz parametra „hitcnt“ prije korištenja linije u pristupnoj listi



Slika 43. Prikaz parametra „hitcnt“ nakon korištenja linije u pristupnoj listi

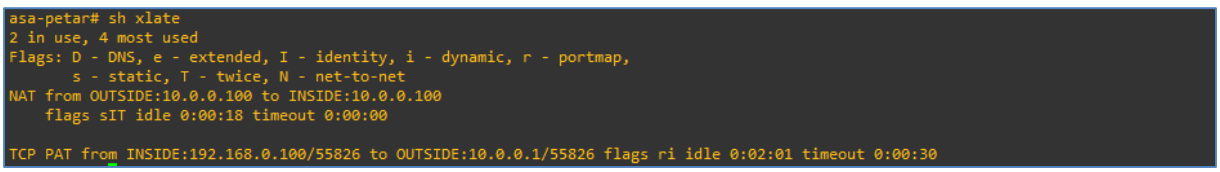
3.2.2. Prikaz veza i prevođenje

Naredbom „sh conn“ moguće je vidjeti TCP i UDP veze u tablici vatroštita. Vidljivo je da je računalo PC-1 otvorilo 2 TCP veze prema Web server-1. Obje veze su bez prometa zadnje 4 sekunde. Po prvoj vezi je preneseno 0 bajtova, a po drugoj 678 bajtova.



Slika 44. Prikaz veza

Naredbom "show xlate" moguće je vidjeti translaciju izvorišne IP adrese računala PC-1 prilikom pristupa Web serveru Web server-1. IP adresa računala PC-1 na lokalnoj mreži je 192.168.0.100 i ta IP adresa se na vatroštitu translatira u javnu IP adresu s kojom se može pristupiti Web serveru. Tako će Web server-1 vidjeti da mu se pristupa s IP adrese 10.0.0.1, a ne s IP adrese 192.168.0.100.



Slika 45. Naredba „show xlate“

Naredbom "sh run nat" moguće je vidjeti konfigurirano pravilo za translaciju IP adresa prilikom pristupa računala PC-1 Web serveru Web server-1. Pravilo definira da se IP adresa računala PC-1 translatira na vatroštitu u IP adresu koja je dodijeljena vanjskom sučelju vatroštita (10.0.0.1). Nadalje, pravilo definira da se ne koristi prevođenje IP adrese Web servera.

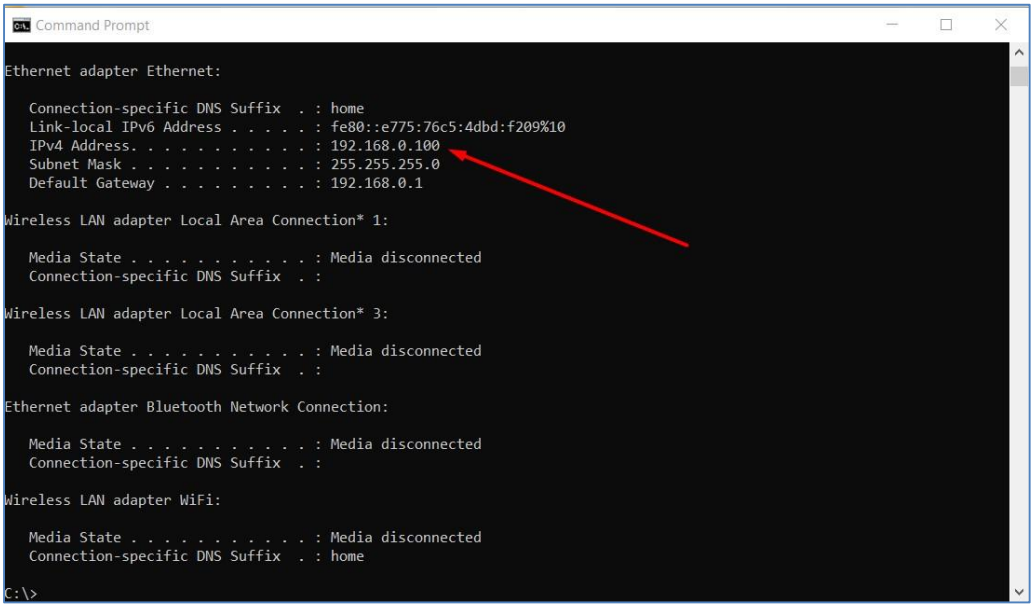
```
asa-petar# sh run nat
nat (INSIDE,OUTSIDE) source dynamic PC-1 interface destination static WEB-SERVER-1 WEB-SERVER-1
```

Slika 46. Naredba „sh run nat“

3.2.3. Uspješan pristup web serveru

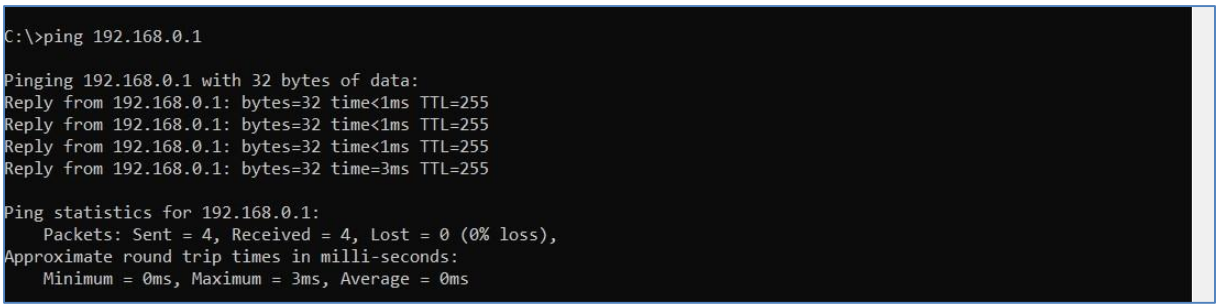
Slijedi prikaz uspješnog pristupa računala PC-1 serveru Web server-1

Naredbom „ipconfig“ izdanom na računalu PC-1 moguće je vidjeti njegovu IP adresu. Vidljivo je da je IP adresa računala PC-1 ista kao i IP adresa računala PC-1 u pristupnoj listi.



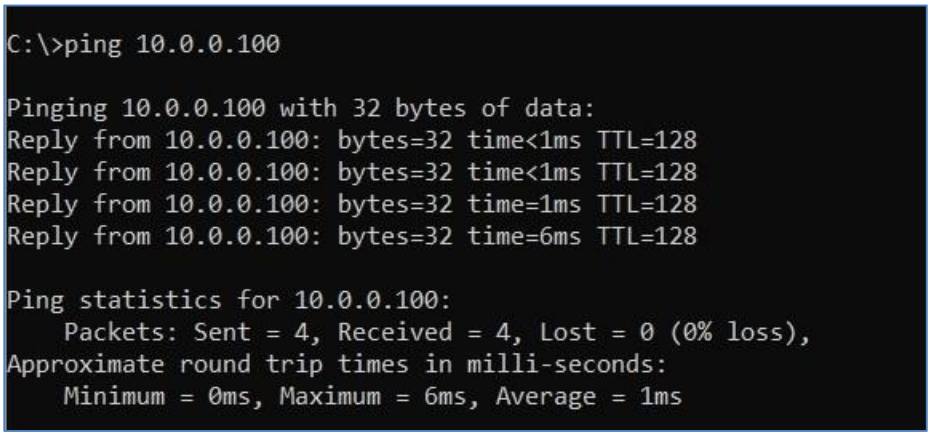
Slika 47. Prikaz IP adrese računala PC-1

Slika 48. prikazuje naredbu „ping“ na računalu PC-1 kojom se prikazuje dostupnost INSIDE sučelja vatroštita koje je ujedno i default gateway za računalo PC-1.



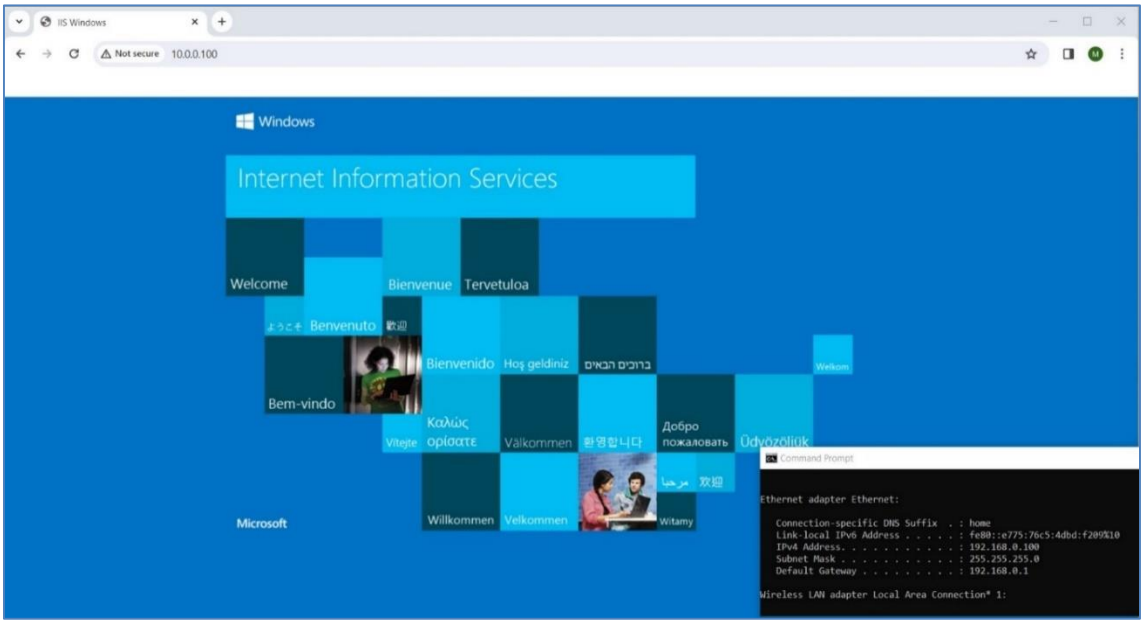
Slika 48. Naredba „ping“ s računala PC-1 prema default gatewayu

Slika 49. prikazuje naredbu „ping“ na računalu PC-1 kojom se prikazuje dostupnost servera Web server-1.



Slika 49. Naredba „ping“ s računala PC-1 prema server Web server-1

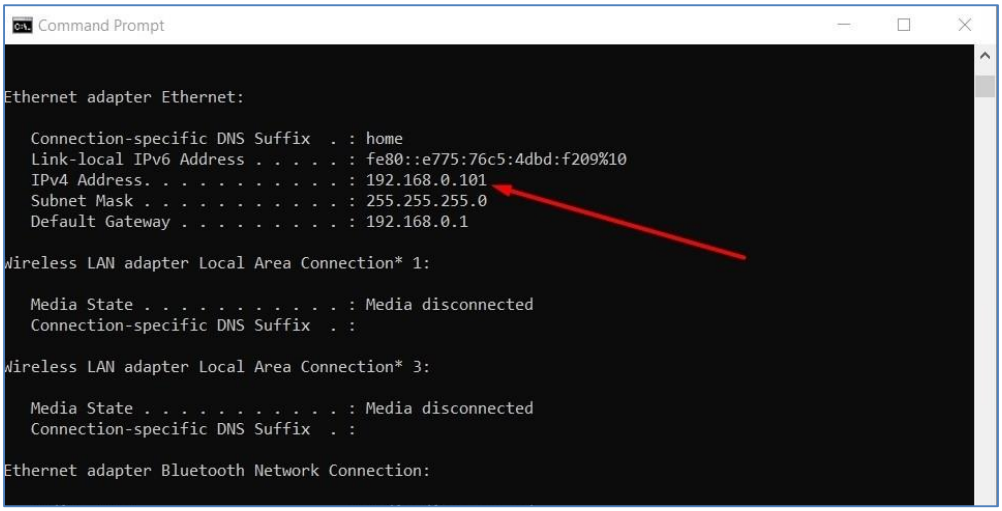
Slika 50. prikazuje uspješan dohvat Web stranice na serveru Web server-1. U donjem desnom kutu nalazi se naredbeni redak s naredbom “ipconfig“ gdje se vidi da je dohvat web stranice izvršen s računala PC-1.



Slika 50. Uspješan dohvat web stranice servera Web server-1 s računala PC-1

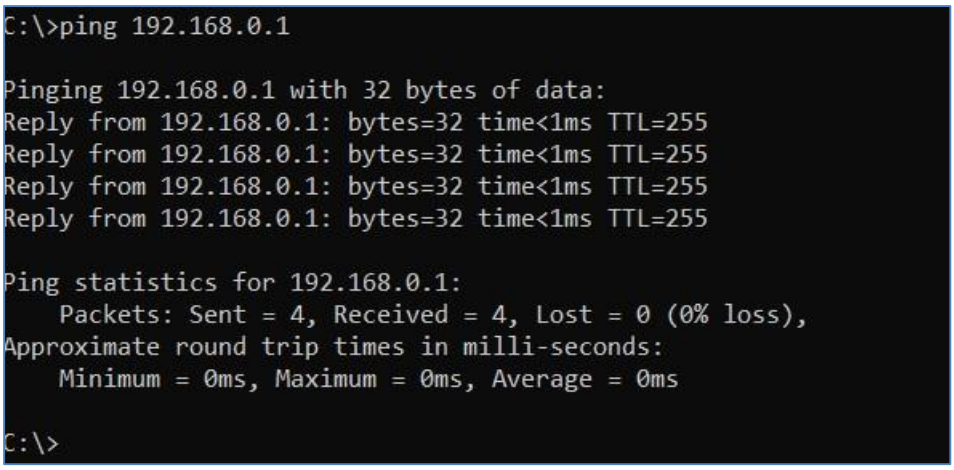
3.2.4. Neuspješan pristup web serveru

Slijedi prikaz neuspješnog pristupa računala PC-2 serveru Web server-1. Naredbom „ipconfig“ izdanom na računalu PC-2 moguće je vidjeti njegovu IP adresu. Vidljivo je da je IP adresa računala PC-2 ista kao i IP adresa računala PC-2 u pristupnoj listi.



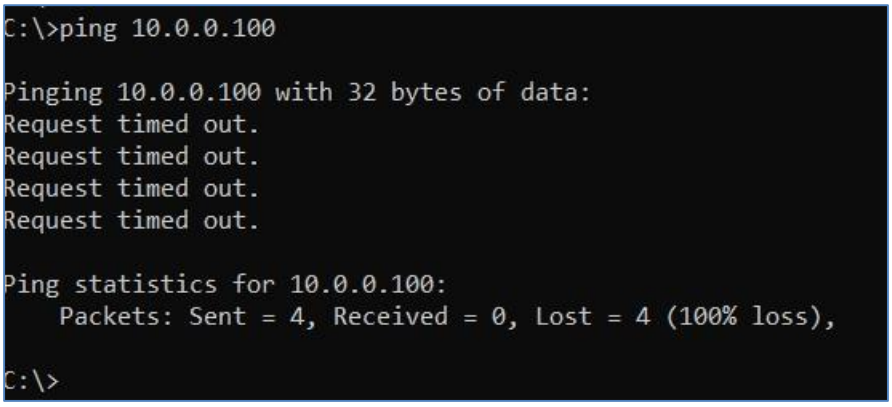
Slika 51. Prikaz IP adrese računala PC-2

Slika 52. prikazuje naredbu „ping“ na računalu PC-2 kojom se prikazuje dostupnost INSIDE sučelja vatroštita koje je ujedno i default gateway za računalo PC-2.



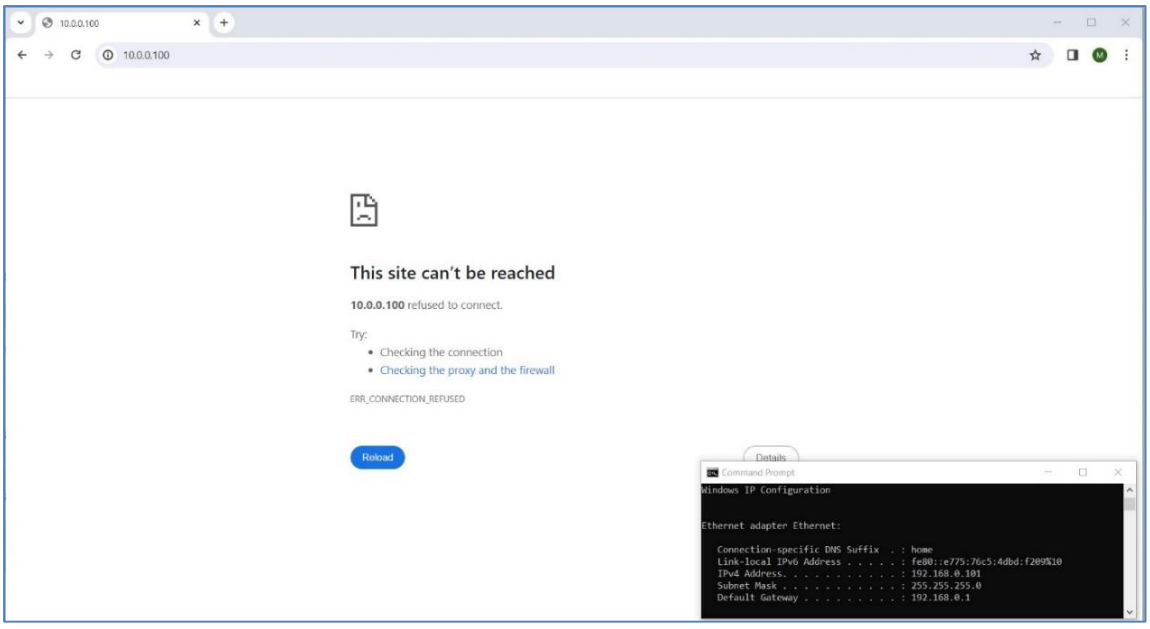
Slika 52. Naredba „ping“ prema ASA vatroštitu

Slika 53. prikazuje naredbu „ping“ na računalu PC-2 kojom se prikazuje nedostupnost servera Web server-1. Razlog nedostupnosti je linija 2 u pristupnost listi koja ne dopušta pristup PC-2 vanjskim destinacijskim adresama.



Slika 53. Naredba „ping“ prema Web serveru

Slika 54. prikazuje neuspješan dohvat Web stranice na serveru Web server-1. U donjem desnom kutu nalazi se naredbeni redak s naredbom “ipconfig“ gdje se vidi da je dohvat web stranice izvršen s računala PC-2.

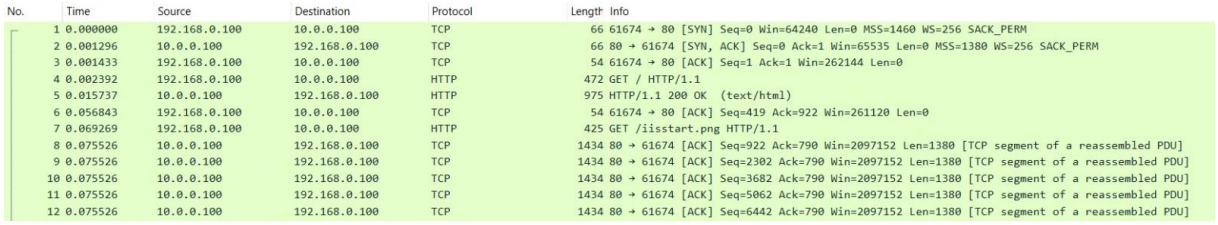


Slika 54. Stranica Web servera

3.2.5. Analiza mrežnog prometa u Wiresharku

Pomoću Wireshark aplikacije sniman je promet između računala PC-1 i web servera Web server-1. U snimci prometa može se vidjeti da u ovom scenariju nema šifriranja prometa zato što nema VPN tunela.

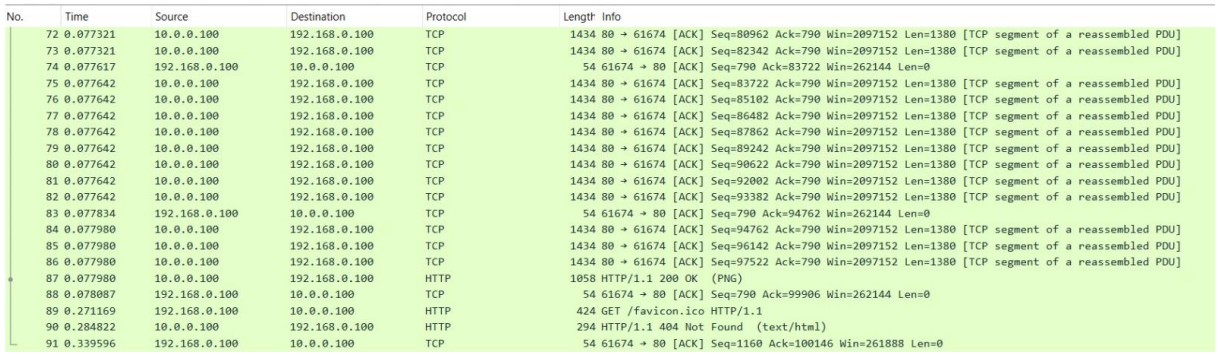
Kao i kod prvog scenarija, prvi redak slike 55. prikazuje početak komunikacije i trostrukog rukovanja između računala PC-1 s IP adresom 192.168.0.100 i web servera Web server-1 s IP adresom 10.0.0.100.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.100	10.0.0.100	TCP	66	61674 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.001296	10.0.0.100	192.168.0.100	TCP	66	80 → 61674 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=256 SACK_PERM
3	0.001433	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.002392	192.168.0.100	10.0.0.100	HTTP	472	GET / HTTP/1.1
5	0.015737	10.0.0.100	192.168.0.100	HTTP	975	HTTP/1.1 200 OK (text/html)
6	0.056843	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=419 Ack=922 Win=261120 Len=0
7	0.069269	192.168.0.100	10.0.0.100	HTTP	425	GET /iisstart.png HTTP/1.1
8	0.075526	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=922 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
9	0.075526	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=2302 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
10	0.075526	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=3682 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
11	0.075526	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=5062 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
12	0.075526	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=6442 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]

Slika 55. Wireshark snimka – inicijalizacija komunikacije

Slika 56. prikazuje daljnu komunikaciju između računala PC-1 i web servera Web server-1. U ovom scenariju nema VPN tunela i nema šifriranja te Wireshark može pročitati detalje komunikacije.



No.	Time	Source	Destination	Protocol	Length	Info
72	0.077321	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=80962 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
73	0.077321	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=82342 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
74	0.077617	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=790 Ack=83722 Win=262144 Len=0
75	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=83722 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
76	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=85102 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
77	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=86482 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
78	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=87862 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
79	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=89242 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
80	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=90622 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
81	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=92002 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
82	0.077642	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=93382 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
83	0.077834	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=790 Ack=94762 Win=262144 Len=0
84	0.077980	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=94762 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
85	0.077980	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=96142 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
86	0.077980	10.0.0.100	192.168.0.100	TCP	1434	80 → 61674 [ACK] Seq=97522 Ack=790 Win=2097152 Len=1380 [TCP segment of a reassembled PDU]
87	0.077980	10.0.0.100	192.168.0.100	HTTP	1058	HTTP/1.1 200 OK (PNG)
88	0.078087	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=790 Ack=99906 Win=262144 Len=0
89	0.271169	192.168.0.100	10.0.0.100	HTTP	424	GET /favicon.ico HTTP/1.1
90	0.284822	10.0.0.100	192.168.0.100	HTTP	294	HTTP/1.1 404 Not Found (text/html)
91	0.339596	192.168.0.100	10.0.0.100	TCP	54	61674 → 80 [ACK] Seq=1160 Ack=100146 Win=261888 Len=0

Slika 56. Wireshark snimka – nešifrirana komunikacija

4. Zaključak

Cilj ovog rada je bio pokazati implementaciju mrežnog vatroštita u računalnu mrežu korporacije u cilju ostvarenja dvije osnovne funkcionalnosti: udaljeni pristup putem Interneta računalu unutar lokalne mreže korporacije i pristup Internetu s računala na korporativnoj mreži.

Putem vatroštita je moguće implementirati još dosta korisnih funkcionalnosti, npr. mrežna segmentacija za smještaj troslojne arhitekture: frontend – backend – database, uspostava LAN-to-LAN VPN tunela, itd… Vatroštit korišten za potrebe ovog rada spada u vatroštite koji pokrivaju ISO razine 1-4. Vatroštiti koji pokrivaju svih 7 ISO razina su tzv. Next generation vatroštiti i oni izvršavaju inspekciju mrežnog prometa sve do razine aplikacije, uz mogućnost dekripcije i ponovne enkripcije mrežnog prometa.

Za konfiguriranje vatroštita su korištene dvije metode: terminalska emulacija (PuTTY) i grafičko sučelje (ASDM). Putem terminalske emulacije je izvršeno osnovno konfiguriranje vatroštita: konfiguriranje sučelja, kreiranje pristupnih listi te omogućavanje ASDM pristupa na management sučelje vatroštita. Putem grafičkog sučelja je konfiguriran VPN tunel za prihvat tzv. Remote Acces VPN korisnika. Na kraju rada su prikazani važniji dijelovi konfiguracije vatroštita gdje su objašnjeni važniji parametri konfiguracije.

U okviru prvog scenarija ovog rada, udaljenog pristupa putem Interneta računalu unutar lokalne mreže korporacije, pokazala se praktičnost Cisco AnyConnect rješenja. Naime, korisnik udaljenog pristupa, nakon inicijalne autentifikacije na vatroštitu, može jednostavno preuzeti instalacijske datoteke i instalirati Cisco AnyConnect bez naprednog poznavanja informacijskih tehnologija. Nakon instaliranja i pokretanja Cisco AnyConnecta te ponovne autentifikacije na vatroštitu, korisnik se spaja na mrežu korporacije i počinje koristiti računalne resurse na toj mreži.

U okviru drugog scenarija ovog rada, pristupa Internetu s računala na korporativnoj mreži, pokazan je osnovni pristup testnom web serveru, otvaranjem početne web stranice putem Internet preglednika. Za te potrebe korišteni su samo osnovni sigurnosni mehanizmi vatroštita: pristupne liste i prevođenje IP adresa. U stvarnim situacijama, poželjno je koristiti i dodatne sigurnosne mehanizme za zaštitu pristupa Internetu, kao npr. proxy server ili napredni vatroštit sa zaštitom od malicioznog koda.

Na kraju ovog rada u prilogu prikazani su važniji dijelovi konfiguracije vatroštita, u cilju boljeg shvaćanja primijenjenih mehanizama, protokola i algoritama. Iskusniji mrežni administratori pri konfiguriranju vatroštita izvršavaju direktne izmjene konfiguracije, putem terminalske emulacije, pri čemu je ključno znanje svakog dijela konfiguracije. I na kraju, vrlo je važno spremiti konfiguraciju vatroštita, lokalno i na serveru za spremanje konfiguracija.

Popis literature

[1] “Vatroštit“, (bez dat.), Cisco stranica. Dostupno:

https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-firewall.html

[pristupano 20.02.2024]

[2] “*Stateful* vatroštit“, (16.2.2020.). The Cisco Learning Network. Dostupno:

https://learningnetwork.cisco.com/s/question/0D53i00000Ksup8CAB/stateful-firewall-overview. [pristupano 20.02.2024]

[3] „Cisco ASA“, (bez dat.), U Wikipedia, the Free Encyclopedia. Dostupno:

https://en.wikipedia.org/wiki/Cisco_ASA

[4] Cisco Systems, Inc. (bez dat.). ASDM Book 1: Cisco ASA Series General Operations ASDM Configuration Guide, 7.6 [Na internetu]. Dostupno na:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/asdm76/general/asdm-76-general-config.pdf. [pristupano 21.02.2024]

[5] Cysco Systems, Inc. (bez dat.). Configuring Access Control Lists. Dostupno na:

https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_1/Cisco_Nexus_5000_Series_Switch_CLI_Software_Configuration_Guide_chapter21.pdf. [pristupano 21.02.2024]

Popis slika

Popis tablica

Prilozi

U ovom prilogu se nalazi ispis važnijih dijelova konfiguracije vatroštita s objašnjenjima. Radna konfiguracija vatroštita se ispisuje naredbom „show running-config“[5].

```
asa-petar# show running-config
: Saved
!
#Serijski broj i hardverska konfiguracija#
: Serial Number: JAD19280089
: Hardware:   ASA5585-SSP-20, 11883 MB RAM, CPU Xeon 5500 series 2133 MHz, 1 CPU
!
#Verzija Cisco ASA softvera#
ASA Version 9.12(4)38
!
#Naziv vatroštita, Internet domene i enable password#
hostname asa-petar
domain-name pix
enable password ***** pbkdf2
!
#Raspon IP adresa koje se dodjeljuju korisnicima koji koriste VPN tunel#
ip local pool USER-POOL 192.168.0.200-192.168.0.210 mask 255.255.255.0
!
#Popis sučelja s nazivima, IP adresama i razinama sigurnosti#
interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.0.0.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif INSIDE
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
interface GigabitEthernet0/2 …
!
interface Management0/0
 no management-only
 nameif management
 security-level 0
 ip address 172.18.0.1 255.255.255.0
!
#Mrežni objekti. Sadrže: ime i IP adresu objekta#
object network PC-1
 host 192.168.0.100
object network WEB-SERVER-1
 host 10.0.0.100
object network inside-subnet
```

```
 subnet 192.168.0.0 255.255.255.0
object network inside-network
 subnet 192.168.0.0 255.255.255.0
object network PC-2
 host 192.168.0.101
object network NETWORK_OBJ_192.168.0.0_24
 subnet 192.168.0.0 255.255.255.0
object network NETWORK_OBJ_192.168.0.192_27
 subnet 192.168.0.192 255.255.255.224
!
#Pristupna lista primijenjena na sučelje „INSIDE“#
access-list INSIDE_access_in extended permit ip object PC-1 any
access-list INSIDE_access_in extended deny ip object PC-2 any
!
#Maksimalna veličina paketa po sučeljima#
mtu OUTSIDE 1500
mtu INSIDE 1500
mtu management 1500
!
#Failover nije konfiguriran jer je korišten samo jedan vatroštit#
no failover
no failover wait-disable
!
#ARP postavke#
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 32768
!
#Postavke prevođenja IP adresa (NAT)#
nat (INSIDE,OUTSIDE) source dynamic PC-1 interface destination static WEB-SERVER-1
WEB-SERVER-1
nat (INSIDE,OUTSIDE) source static NETWORK_OBJ_192.168.0.0_24
NETWORK_OBJ_192.168.0.0_24 destination static NETWORK_OBJ_192.168.0.192_27
NETWORK_OBJ_192.168.0.192_27 no-proxy-arp route-lookup
!
#Pristupnom grupom se primjenjuje pristupna lista na određeno sučelje#
access-group INSIDE_access_in in interface INSIDE
!
#Vremenska ograničenja za NAT, PAT, veze i određene protokole#
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
timeout igp stale-route 0:01:10
!
#Korisnici su definirano lokalno na vatroštitu#
aaa authentication ssh console LOCAL
aaa authentication login-history
!
#Omogućen je HTTP server radi pristupa ASDM-u#
```

```
http server enable
http 172.18.0.0 255.255.255.0 management
!
#Predlošci za ikev2 protokol#
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
!
#Definirana kripto mapa i primijenjena na sučelje OUTSIDE#
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal
AES256 AES192 AES 3DES DES
crypto map OUTSIDE_map 65535 ipsec-isakmp dynamic
SYSTEM_DEFAULT_CRYPTO_MAP
crypto map OUTSIDE_map interface OUTSIDE
!
#Definiran Certificate Authority i samopotpisani certifikat#
crypto ca trustpoint ASDM_TrustPoint0
 enrollment self
 subject-name CN=asa-petar
 keypair ASDM
 crl configure
crypto ca trustpool policy
crypto ca certificate chain ASDM_TrustPoint0
 certificate d7915865
    308202e0 308201c8 a0030201 020204d7 91586530 0d06092a 864886f7 0d01010b
    985743fd …
!
#ikev2 politike#
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
```

```
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
!
#ikev2 je aktivan na sučelju OUTSIDE po portu 443#
crypto ikev2 enable OUTSIDE client-services port 443
crypto ikev2 remote-access trustpoint ASDM_TrustPoint0
#ssh parametri#
ssh timeout 5
ssh version 2
ssh key-exchange group dh-group14-sha256
ssh 172.18.0.100 255.255.255.255 management
!
#Timeout za pristup putem konzolnog kabela#
console timeout 0
!
#Aktivna je osnovna detekcija prijetnji#
threat-detection basic-threat
!
#Lokacija i naziv instalacijskih datoteka za Cisco AnyConnect. Grupa korisnika koja može
preuzeti ove instalacijske datoteke#
anyconnect image disk0:/anyconnect-win-4.9.05042-webdeploy-k9.pkg 1
 anyconnect profiles COMPANY-USERS_client_profile disk0:/COMPANY-
USERS_client_profile.xml
 anyconnect enable
 tunnel-group-list enable
 cache
  disable
 error-recovery disable
!
#Grupna politika za korisnike iz grupe COMPANY-USERS#
group-policy GroupPolicy_COMPANY-USERS internal
group-policy GroupPolicy_COMPANY-USERS attributes
 wins-server none
 dns-server value 8.8.8.8
 vpn-tunnel-protocol ikev2 ssl-client
#Postavke za ssl VPN#
webvpn
  anyconnect profiles value COMPANY-USERS_client_profile type user
dynamic-access-policy-record DfltAccessPolicy
!
#Korisnici definirani na vatroštitu#
username user-1 password ***** encrypted
```

```
username user-2 password ***** encrypted
username pkordic password ***** encrypted privilege 15
!
#Postavke tunel grupe COMPANY-USERS#
tunnel-group COMPANY-USERS type remote-access
tunnel-group COMPANY-USERS general-attributes
 address-pool USER-POOL
 default-group-policy GroupPolicy_COMPANY-USERS
tunnel-group COMPANY-USERS webvpn-attributes
 group-alias COMPANY-USERS enable
!
#Parametri za provjeru prometa#
class-map inspection_default
 match default-inspection-traffic
!
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
: end
asa-petar#
```