# Udaljeni pristup računalu te pristup Internetu s prilagodljivim sigurnosnim vatroštitom

Kordić, Petar

Undergraduate thesis / Završni rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:873868

Rights / Prava: Attribution 3.0 Unported / Imenovanje 3.0

Download date / Datum preuzimanja: 2024-12-19



Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository





# 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

# VARAŽDIN

Petar Kordić

Matični broj: 0016143797

Studij: Informacijski sustavi

# Udaljeni pristup računalu te pristup Internetu s prilagodljivim sigurnosnim vatroštitom

ZAVRŠNI RAD

Mentor:

lzv. 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

Sadržajiii
1. Uvod
2. Oprema u laboratoriju
2.1. Hardver
2.1.1. Vatroštit Cisco ASA
2.1.2. Računala
2.2. Softver
2.2.1. ASA i ASDM
2.2.2. PuTTY
2.2.3. Cisco AnyConnect
3. Scenariji
3.1. Udaljeni pristup s Interneta računalu unutar lokalne mreže korporacije6
3.1.1. Konfiguriranje VPN-ovih postavki na vatroštitu6
3.1.2. Pristup korisnika putem VPN tunela15
3.1.3. Analiza mrežnog prometa u Wiresharku
3.2. Pristup Internetu s računala na korporativnoj mreži
3.2.1. Pristupna lista
3.2.2. Prikaz veza i prevođenje
3.2.3. Uspješan pristup web serveru
3.2.4. Neuspješan pristup web serveru
3.2.5. Analiza mrežnog prometa u Wiresharku
4. Zaključak
Popis literature
Popis slika
Popis tablica
Prilozi

# 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<sup>[1]</sup>. 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<sup>[2]</sup>. 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<sup>[3]</sup>.

## 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<sup>[4]</sup>. 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.

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

Tablica 1: Prikaz karakteristika scenarija

# 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)".

🔄 Cisco ASDM 7.2 fo	or ASA - 172.18.0.1			
File View Tools	Wizards Window Help			
🖂 Home 🔐 Conf	Startup Wizard		Back 🕜 Forward 🦻 Help	
Pemote Access	VPN Wizards	>	Site-to-site VPN Wizard	
	High Availability and Scalal	bility Wizard	AnyConnect VPN Wizard	<b></b>
🖁 🖃 🗒 Network (	Packet Capture Wizard		Clientless SSL VPN Wizard	
AnyCo	onnect Connection Profiles	Remote Acces	IPsec (IKEv1) Remote Access VPN Wizard	e networks and applications to use
AnyCC     A	nnect Clent Profile nnnect Client Profile nnnect Client Profile nnnect Client Software lic Access Policies Policies IKEV 1) Connection Profiles IKEV 1) Connection Profiles IKEV 1) Connection Profiles IKEV 1) Connection Profiles Status Status Status Status IMage Stop Manager Management Localization chig Ver	The ASDM Ass Cief Clientier SSL or I	istant guides you step by step through the configuration o ss SSL VPN Remote Access (using Web Browser) (Psec(IKEv2) VPN Remote Access (using Cisco AnyConnect KEv1) VPN Remote Access (using Cisco VPN Client)	f the three types of Remote Access





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".

5	AnyConnect VPN Conne	ction Setup Wizard		×
Ste	eps	Connection Profile Identifie	cation	
1. 2.	Introduction Connection Profile	This step allows you to cor connections.	nfigure a Connection Profile Name and the Interface the remote access users will access for VPN	
3.	Identification VPN Protocols	Connection Profile Name:	COMPANY-USERS	
4. 5.	Client Images Authentication Methods	VPN Access Interface:	OUTSIDE ~	
6.	Client Address Assignme			
7.	Network Name Resolutio Servers			
8.	NAT Exempt			
9.	AnyConnect Client Deployment			
10	). Summary			
		< Back Next >	Cancel Hel	þ

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.

anyConnect	VPN Con	nection Setup Wizard	×
Steps	o Mana	a Add Identity Certificate	× × rotocols you
<ol> <li>Connection Identification</li> <li>VPN Protection</li> </ol>	Issued	Trustpoint Name:     ASDM_TrustPoint0       O Import the identity certificate from a file (PKCS12 format with Certificate(s) +Private Key):	tails
<ol> <li>Client Imag</li> <li>Authentica</li> </ol>		Decryption Passphrase: File to Import From: Browse	e
6. Client Addr		Add a new identity certificate:	t
7. Network Na Servers	Find:	Key Pair: ASDM V Show New	
9. AnyConnec P Deploymen	Public CA I	✓     Generate self-signed certificate	
10. Summary	Get you Entrust	Act as local certificate authority and issue dynamic certificates to TLS-Proxy	<b>.</b>
	Using a	Advanced	
		Add Certificate Cancel Help	
		<back next=""></back>	Cancel Help

Slika 6: Odabir certifikata (self-signed certifikat)

<b>Ба</b> А	nyConnect VPN Connection Setup Wiz	zard			×		
Stens	VPN Protocole						×
2.	Issued To	Issued By	Expiry Date	Associated Trustpoints	Usage Conoral Purpose	Public Key Type	Add
3. 4.	nosulaine—asa-petai, pix, en—asa-petri	ווטגעומוויב–מגמ קיבנמו קוא, ניו–מגמ קיבנמו	13.37.43 010 30 20 20 3		General Purpose	K3A (20+6 bits)	Show Details Delete
5. 6.							Export
7.	Find: O O	Match Case					Install
9.	Public CA Enrollment						
10	Get your Cisco ASA security appliance u trial certificates for testing.	p and running quickly with an SSL Advantag	le digital certificate from Entr	rust. Entrust offers Cisco	customers a specia	al promotional price	for certificates and
	Using a previously saved certificate sign	ning request, <u>enroll with Entrust</u> .	ASA 352 CEI UICERE WUITEIT	uust			
		ОК	Cancel	Help			
	< Back	Next >		Cancel	Help		

Slika 7: Odabir certifikata (ostali parametri)

AnyConnect VPN Connect	ction Setup Wizard	×
Steps	VPN Protocols	
<ol> <li>Introduction</li> <li>Connection Profile Identification</li> <li>VPN Protocols</li> <li>Client Images</li> <li>Authentication Methods</li> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>AnyConnect Client Deployment</li> <li>Summary</li> </ol>	AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols yo would like this connection profile to support.  SSL IPSec Device Certificate Device certificate Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA. Device Certificate: ASDM_TrustPoint0:hostname=asa-pet Manage	u
	< Back Next > Cancel Help	

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.

1. Introduction         2. Connection Profile Identification         3. VPN Protocols         4. Client Images         5. Authentication Methods         6. Client Address Assignme         7. Network Name Resolutio Servers         8. NAT Exempt         9. AnyConnect Client Deployment         10. Summary	Steps	Client Images
<ul> <li>S. Authentication Methods</li> <li>G. Client Address Assignme</li> <li>Network Name Resolutio Servers</li> <li>NAT Exempt</li> <li>AnyConnect Client Image: 0:/anyconnect-win-4.9.05042-webdeploy-k9.pkg Browse Flash</li> <li>ManyConnect Client Deployment</li> <li>OK Cancel Help</li> <li>You can download AnyConnect Client packages from Clisco by searching 'AnyConnect VPN Client' or click here.</li> </ul>	I. Introduction     Connection Profile     Identification     VPN Protocols     Client Images	ASA can automatically upload the latest AnyConnect package to the client device when it accesses the enterprise network. A regular expression can be used to match the user-agent of a browser to an image. You can also minimize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list.
<ul> <li>6. Client Address Assignme</li> <li>7. Network Name Resolutio Servers</li> <li>8. NAT Exempt</li> <li>9. AnyConnect Client Deployment</li> <li>10. Summary</li> <li>10.</li></ul>	5. Authentication Methods	📧 Add AnyConnect Client Image X
8. NAT Exempt 9. AnyConnect Client Deployment 10. Summary You can download AnyConnect Client packages from Cisco by searching 'AnyConnect VPN Client' or dick here.	<ol> <li>Client Address Assignme</li> <li>Network Name Resolutio Servers</li> </ol>	AnyConnect Image: 0:/anyconnect-win-4.9.05042-webdeploy-k9.pkg Browse Flash Upload
	<ol> <li>NAT Exempt</li> <li>AnyConnect Client Deployment</li> <li>Summary</li> </ol>	Regular expression to match user-agent       Image: Cancel Help         OK       Cancel Help         You can download AnyConnect Client packages from <u>Cisco</u> by searching 'AnyConnect VPN Client' or <u>click here</u> .

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.

	and and under	,
Steps	Authentication Methods	
Introduction     Introduction Profile     Identification     VPN Protocols     Client Images     Authentication     Methods     Client Address Assignme     Network Name Resolutio     Servers     NAT Exempt     AnyConnect Client     Deployment     Jo. Summary	This step lets you specify the location of the authentication server. You can click on the "New" button to create a new server group. AAA Server Group: LOCAL V New Local User Database Details User to be Added Username: user-2 Add >> Password: •••••••• Confirm Password: •••••••	
	< Back Next > Cancel	Help

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.

🔤 AnyConnect VPN Conne	ction Setup Wizard X
Steps	Client Address Assignment
1. Introduction	This step allows you to create a new address pool or select an existing address pool for IPv4 and IPv6. The AnyConnect clients
2. Connection Profile	will be assigned addresses from the pools when they connect.
Identification	IPv6 address pool is only supported for SSL connection.
<ol><li>VPN Protocols</li></ol>	
4. Client Images	IP v4 Address Pool IP v6 Address Pool
5. Authentication Methods	Address Pool: USER-POOL V New
6. Client Address Assignment	Details of the selected address pool
7. Network Name Resolutio	Starting IP Address: 192.168.0.200
Servers	Ending IP Address: 192, 168.0, 210
8. NAT Exempt	
<ol> <li>AnyConnect Client Deployment</li> </ol>	Subnet Mask: 255.255.255.0 V
10. Summary	
	< Back Next > Cancel Help

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.

🔄 AnyConnect VPN Conne	ction Setup Wiza	d	×
Steps	Network Name F	esolution Servers	
1. Introduction	This step lets yo	u specify how domain names are resolved for the remote user when accessing the internal network.	
2. Connection Profile Identification	DNS Servers:	8.8.8.8	
3. VPN Protocols	WINS Servers:		
4. Client Images	Domain Name:	pix	
5. Authentication Methods			
6. Client Address Assignme			
7. Network Name Resolution Servers			
8. NAT Exempt			
<ol> <li>AnyConnect Client Deployment</li> </ol>			
10. Summary			
	< Back	Vext > Cancel Help	

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.

teps	NAT Exempt
Introduction     Connection Profile     Identification     VPN Protocols     Client Images     Authentication Methods     Client Address Assignme     Network Name Resolutio     Servers	If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.  Exempt VPN traffic from network address translation Inside Interface is the interface directly connected to your internal network. Inside Interface: INSIDE Local Network is the network address(es) of the internal network that client can access.
<ol> <li>NAT Exempt</li> <li>AnyConnect Client Deployment</li> <li>Summary</li> </ol>	Local Network: 192.168.0.0/24

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.

anyConnect VPN Conne	ection Setup Wizard	×
Steps	AnyConnect Client Deployment	
1. Introduction	AnyConnect client program can be installed to a client device by one of the following two methods:	
2. Connection Profile Identification	<ol> <li>Web launch - On accessing the ASA using a Web Browser, the AnyConnect dient package will be automatically installed;</li> <li>Pre-deployment - Manually install the AnyConnect dient package.</li> </ol>	
3. VPN Protocols		
4. Client Images		
5. Authentication Methods	Allow Web Launch	
6. Client Address Assignme	Caution: Web launch is global setting, it affects all connections. AnyConnect SSL connections and clientless SSL connections was a set of the s	vill
<ol> <li>Network Name Resolutio Servers</li> </ol>	NOI work in it is turned off.	
8. NAT Exempt	For pre-deployment, please remember to include the dient profile 'disk0:/COMPANY-USERS_client_profile.xml' from the ASA in	n I
9. AnyConnect Client Deployment	your AnyConnect package, otherwise IPsec connection will NOT work.	
10. Summary		
	< Back Next > Cancel Help	

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".

🔄 AnyConnect VPN Connec	ction Setup Wizard	×
VPN Wizard	Summary Here is the summary of the configuration.	
B B Home Corporate Network	Name Summary Name/Alias of the Connection Profile VPN Access Interface Device Digital Certificate VPN Protocols Enabled AnyConnect Client Images Authentication Server Group Address Pool for the Client	Value COMPANY-USERS OUTSIDE ASDM_TrustPoint0:hostname=asa-petar.pix, cn=asa-pe IPsec and SSL 1 package LOCAL 192.168.0.200 - 192.168.0.210
	DNS Network Address Translation	Server: Domain Name: The protected traffic is not subjected to network address translation
	< Back Finish	Cancel Help

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.

AnyConnect Installation	x +			V	- 0	y X
< → C △ ▲ N	ot secure   https://10.0.0.1/CACHE/stc/1/index.html	哈 女	<b>Q</b> (7)	0 0	* 0	0
cisco Ang	yConnect Secure Mobility Client				0	
	AnyConnect Secure Mobility Client Download		4			
	Download & Install					
	Download Cisco AnyConnect Secure Mobility Client and install it on your computer.					
Start	0	nstructior	IS			-

Slika 18: Preuzimanje instalacijskih datoteka za Cisco AnyConnect



Slika 19. Instaliranje Cisco AnyConnect: Prva stranica

Secu	Cisco AnyConnect Secure Mobility Client Setup × End-User License Agreement Please read the following license agreement carefully
	Supplemental End User License Agreement for AnyConnect® Secure Mobility Client v4.x and other VPN-related Software
	IMPORTANT: READ CAREFULLY This Supplemental End User License Agreement ("SEULA") contains additional terms and conditions for the Software Product licensed under the End User License Agreement ("EULA") between You ("You" as used herein means You v
	I accept the terms in the License Agreement     I do not accept the terms in the License Agreement
	< Back Next > Cancel
Dowr	aload Cisco AnyConnect Secure Mobility Client and install it on your computer.
	Download for Windows

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.

S Cisco AnyC	Connect Secure Mobility Client X		
A	Untrusted Server Blocked! AnyConnect cannot verify server: 10.0.0.1 Connecting to this server may result in a severe security compromise! Security Risks Explained AnyConnect is configured to block untrusted servers by default. Most users choose to keep this setting. If this setting is changed, AnyConnect will no konger automatically block connections to potentially malicious network devices.		
	Change Setting Keep Me Safe	Gisco AnyConnect Secure Mobility Client —	
		VPN: Contacting 10.0.0.1. 10.0.0.1	Connect
		<b>\$</b> ()	

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.

S Cisco AnyCo	onnect Secure Mobility Client	—		$\times$
	VPN: Connection attempt has failed. 10.0.0.1	~	Connect	
				_
<b>۞</b> (i)				uluilu cisco



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.



🚳 c	isco AnyConnect	t   10.0.0.1 🛛 🗙	
ſ			
_	Group:	COMPANY-USERS ~	
	Username:	user-1	
	Password:	*****	
		OK Cancel	

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

S Cisco AnyCo	onnect Secure Mobility Client		_		×
	VPN: Connected to 10.0.0.1. 10.0.0.1	×	C	Disconnect	:
00:00:32					IPv4
<b>۞</b>					uluilu cisco



## Korak 5: Prijava na datotečni server

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

🔶 🔍 Map N	etwork Drive	×
What ne Specify the	etwork folder would you like to map?	
E Folder:	Z:          \\192.168.0.10\Datoteke       >         Browse       Example: \\server\share         Reconnect at sign-in          Connect using different credentials       Connect to a Web site that you can use to store your documents and pictures.	
	Finish Canc	el

Slika 29. Pristup mapi na datotečnom serveru

Windows Security	×					
Enter network credentia	als					
Enter your credentials to connect to: 192.168.0.10						
192.168.0.10\Petar						
•••••						
✓ Remember my credentials						
More choices						
ОК	Cancel					

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

🛫   🗹 📙 =   Datoteke (\\192.168.0.10) (Z:)						-
File Home Share View						
$\leftarrow$ $\rightarrow$ $\checkmark$ $\uparrow$ $\checkmark$ $\rightarrow$ This PC $>$ Datoteke (	\\192.168.0.10) (Z:)	~	ر ن	Search Datotel	ke (\\192.1	168.0.10) (Z:)
Anne Anne	Date modified	Туре		Size		
Test.txt	20.3.2022. 23:43	Text Do	ocument	1 KB		
Test.txt - Notepad				-		×
File Edit Format View Help Test						^

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	
14	15 21.725970	10.0.0.100	10.0.0.1	DTLSv1.2	176 Application Data	
14	46 21.726059	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
14	17 21.726118	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
14	48 21.726162	10.0.0.100	10.0.0.1	DTLSv1.2	136 Application Data	
14	19 21.726199	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	60 21.726235	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
19	51 21.726274	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	52 21.726309	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
19	53 21.726345	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	54 21.726384	10.0.0.100	10.0.0.1	DTLSv1.2	141 Application Data	
15	5 21.726424	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	6 21.726461	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	57 21.726632	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	68 21.726681	10.0.0.100	10.0.0.1	DTLSv1.2	120 Application Data	
15	59 21.726725	10.0.0.100	10.0.0.1	DTLSv1.2	139 Application Data	
16	60 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.

No. Time Source	Destination	Protocol	Lengti Info
1 0.000000 10.0.100	10.0.0.1	NBNS	92 Name guery NBSTAT *<00><00><00><00><00><00><00><00><00><00
2 0.002971 fe80::c72b:2310:808	ff02::1:3	LLMNR	101 Standard guery 0x5dd6 PTR 1.0.0.10.in-addr.arpa
3 0.003161 10.0.0.100	224.0.0.252	LLMNR	81 Standard query 0x5dd6 PTR 1.0.0.10.in-addr.arpa
4 0.428373 fe80::c72b:2310:808	ff02::1:3	LLMNR	101 Standard query 0x5dd6 PTR 1.0.0.10.in-addr.arpa
5 0.428461 10.0.0.100	224.0.0.252	LLMNR	81 Standard query 0x5dd6 PTR 1.0.0.10.in-addr.arpa
6 1.513296 10.0.0.100	10.0.0.1	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
7 3.018590 10.0.0.100	10.0.0.1	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
- 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
<pre>v Cipher Suites (22 suites) Cipher Suite: 115,485,256,GCM. Cipher Suite: 115,485,256,GCM. Cipher Suite: 115,100H,ERSA WIT Cipher Suite: 115,100H,WITA WIT Cipher Suite: 115,100H,WITA WITA WITS Cipher Suite: 115,100H,WITA WITA WITA Cipher Suite: 115,100H,WITA WITA WITA WITA WITA WITA WITA WITA</pre>	SHA384 (0x1302) SHA256 (0x1301) SHA256 (0x1301) TH LASS_256, GCN SHA384 NTH LASS_256, GCN SHA384 AES_256, GCN SHA384 AES_256, GCN SHA384 (AES_256, GCN SHA384 (AES_256, GCN SHA384 (AES_256, GCN SHA384 (AES_256, GCN SHA356 (AES_256, GCN SHA356 (AES_256, GCN SHA356 (AES_256, GCN SHA356 (AES_256, GCN SHA356 (AES_256, GCN SHA256 (AES_2128, GCN SHA256 (AES_2128, GCN SHA256 (AES_2128, GCN SHA256 (AES_2128, GCN SHA256 (AES_2128, GCN SHA256 (AES_2128, GCN SHA256 (AES_256, GN SHA556 (AES_256, GN	4 (0xc030) 584 (0xc02c) 184 (0xc02c) 184 (0xc02d) 184 (0xc0d) 184	A 0000 e8 65 49 28 09 b2 e8 6a 64 ab 44 b9 08 09 45 00 e71(-; j d.D: [j d.D.

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.

No.		Time	Source	Destination	Protocol	Lengti Info
	4	0.428373	fe80::c72b:2310:808	ff02::1:3	LLMNR	101 Standard query 0x5dd6 PTR 1.0.0.10.in-addr.arpa
	5	0.428461	10.0.0.100	224.0.0.252	LLMNR	81 Standard query 0x5dd6 PTR 1.0.0.10.in-addr.arpa
	6	1.513296	10.0.0.100	10.0.0.1	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
	7	3.018590	10.0.0.100	10.0.0.1	NBNS	92 Name query NBSTAT *<00><00><00><00><00><00><00><00><00><00
-	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
> T	ransm	ission Control	Protocol, Src Port:	443. Dst Port: 56096	Seg: 1. Ack: 518. Le	an: 1191
Ú,	nansn	ort Laver Secu	rity	445, 550 1010, 50050	, seq. 1, Acc. 510, cc	0090 03 03 02 ee 0b 00 02 ea 00 02 e7 00 02 e4 30 82
		(1.2 Record La	ver: Handshake Proto	ol: Server Hello		00a0 02 e0 30 82 01 c8 a0 03 02 01 02 02 04 d7 91 580X
		ontent Type:	Handshake (22)	ion perfer nerro		00b0 65 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 e0*.H
		Version: TIS 1	2 (0x0303)			0000 30 32 31 12 30 10 00 03 55 04 03 13 09 01 73 01 021 00 0 00 03 55 04 03 13 09 01 73 01 021 00 0 00 00 00 0
		ength: 84	.2 (0x0505)			9040 20 70 97 40 11 99 27 50 41 61 73 61 24 00 65 74 61 72
	~	landshake Prot	col: Server Hello			00f0 2e 70 69 78 30 1e 17 0d 32 33 31 31 31 38 31 32 .pix0 ··· 23111812
		Handshake Ty	(ne: Server Hello (2)			0100 30 38 30 32 5a 17 0d 33 33 31 31 31 35 31 32 30 08022··3 31115120
		Length: 80	(-/			0110 38 30 32 5a 30 32 31 12 30 10 06 03 55 04 03 13 8022021· 0···U···
		Version: TI	5 1 2 (0x0303)			0120 09 61 73 61 2d 70 65 74 61 72 31 1c 30 1a 06 09 - asa-pet ar1-0
		Random: 07d	af6c4bfc15149ff4940a	f2356a97a15fa58dffb8a	728ea1983fd2aed2846	0130 20 00 17 20 70 01 01 00 02 10 00 01 23 0 00 01 07 01 20 70 01
		Session TD I	ength: 32	125508578151650011006	200010001020000	0150 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 *.H
		Session ID:	7cf3ab02389d4573o09a	3h9aho278ahfd9h39o2o1	h8aadhc9c3ead7aa9adc3t	b7 0160 30 82 01 0a 02 82 01 01 00 d5 f5 6d 6e 15 00 67 0mn.g
		Cinhan Suite	. TIS ECOHE RSA WITH	AES 256 GCM SHA384 (	Axc030)	0170 6e 1c 16 b9 39 73 d2 77 1c 4e 1e 41 9f 2d 64 d4 n9s.w.N.Ad-
		Compression	Mathod: pull (M)	_Ac5_250_001_5104504 (	0,0000)	0180 94 b5 fd af 0c a3 78 eb 48 2b 30 5a 89 0a 0a 21x H+0Z
		Extensions I	ength: 8		0190 de 30 6 45 73 40 60 42 22 31 73 60 ec de 10 60 $(1.165)$	
		> Extension: (	s point formate (lon	-4)	01b0 67 37 d2 a4 49 ba 56 4d e3 70 fa d7 46 5e bf 35 g7-I-VM -p-F^-5	
		[1A3S Eulled	ring: 771 49289 111		01c0 6a 48 07 63 60 a3 b4 d7 6e f2 41 93 e1 db f3 9c jH c n.A	
		[]A35+ fd478	2000do5830o3178b3d037	22050001	01d0 c2 77 ad 82 49 b6 0b 67 06 3f 83 d9 b5 fd 70 5c -w-I-g -?p	
	TIS	1 2 Record La	ver: Handshake Proto	ol: Certificate	0160 /1 23 e67 fb d8 61 83 29 ae 0e 0a a8 ab 30 ab b6 $q$ $q$ +, $q$ , $0.5$	
		Content Type: 1	Handshake (22)	ioar certaritate	$0200$ da 1b da 13 de $e^7$ da $ac$ 67 fa $ac$ 67 da $ac$ 68 fa fa $ac$ 7. $a$	
		Version: TIS 1	2 (0v0303)		0210 6a 78 23 dc d5 16 ff d8 49 92 40 51 40 1d b6 c2 jx# I @Q@	
		113 1	(0,0505)			✓ 0220 22 5a 67 30 34 22 8a b5 26 0a 47 c7 c6 as 05 09 "7004" &.G

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.

asa-petar(config)# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list INSIDE_access_in; 2 elements; name hash: 0xb71cec1d
access-list INSIDE_access_in line 1 extended permit ip object PC-1 any (hitcnt=4) 0x5e8b3dfa
access-list INSIDE_access_in line 1 extended permit ip host 192.168.0.100 any (hitcnt=4)
access-list INSIDE_access_in line 2 extended deny ip object PC-2 any (hitcnt=0) 0x626db8a3
access-list INSIDE_access_in line 2 extended deny ip host 192.168.0.101 any (hitcnt=0) 0x626db8a3



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

asa-petar# sh access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
access-list INSIDE_access_in; 2 elements; name hash: 0xb71cec1d
access-list INSIDE_access_in line 1 extended permit ip object PC-1 any (hitcnt=6) 0x5e8b3dfa
access-list INSIDE_access_in line 1 extended permit ip host 192.168.0.100 any (hitcnt=6) 0x5e8b3dfa
access-list INSIDE_access_in line 2 extended deny ip object PC-2 any (hitcnt=53) Access_access
access-list INSIDE_access_in line 2 extended deny ip host 192.168.0.101 any (hitcnt=53) 0x626db8a3

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.

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.

```
C:\>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time<1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=1ms TTL=128
Reply from 10.0.0.100: bytes=32 time=6ms TTL=128
Reply from 10.0.0.100: bytes=32 time=6ms TTL=128
Ping statistics for 10.0.0.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 6ms, Average = 1ms</pre>
```

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.

```
C:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Reply from 192.168.0.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```



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.

C:\>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data: Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 10.0.0.100: Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

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
Г	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 $\rightarrow$ 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 $\rightarrow$ 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	Lengtr 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 $\rightarrow$ 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 $\rightarrow$ 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 $\rightarrow$ 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)
L	91 0.339596	192.168.0.100	10.0.100	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-firewalloverview. [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-generalconfig.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

Slika 1: Fizički izgled opreme	2
Slika 2: Shema scenarija 1	6
Slika 3: Odabir vrste VPN tunela	7
Slika 4: Objašnjenje Remote Access VPN tunela	7
Slika 5: Odabir imena VPN profila i vanjskog sučelja	8
Slika 6: Odabir certifikata (self-signed certifikat)	8
Slika 7: Odabir certifikata (ostali parametri)	9
Slika 8: Odabir VPN protokola (SSL i IPsec)	9
Slika 9: Odabir načina instalacije Cisco AnyConnect softvera	. 10
Slika 10: Odabir metode autentifikacije i kreiranje korisnika	.11
Slika 11: Kreiranje raspona IP adresa	.11
Slika 12. Odabir DNS servera	. 12
Slika 13. Izuzeće od translacije IP adresa i mrežni raspon kojemu mogu pristupiti korisnici	. 13
Slika 14. Dopuštenje za preuzimanje instalacijskih datoteka za Cisco AnyConnect	. 13
Slika 15. Sažetak VPN postavki	. 14
Slika 16: Inicijalno povezivanje na vatroštit	. 15
Slika 17: Korisnički podaci za prijavu na vatroštit	. 15
Slika 18: Preuzimanje instalacijskih datoteka za Cisco AnyConnect	. 16
Slika 19. Instaliranje Cisco AnyConnect: Prva stranica	. 16
Slika 20. Instaliranje Cisco AnyConnect: Uvjeti korištenja	. 17
Slika 21. Instaliranje Cisco AnyConnect: Završetak	. 17
Slika 22. Cisco AnyConnect: upozorenje da je blokirano povezivanje na nepovjerljiv VPN	
server	. 18
Slika 23. Cisco AnyConnect: Odznačavanje blokiranja nepovjerljivih VPN servera	. 19
Slika 24. Cisco AnyConnect: ponovno pokretanje povezivanja na vatroštit	. 19
Slika 25. Cisco AnyConnect: ponovno pokretanje povezivanja na vatroštit	. 20
Slika 26. Cisco AnyConnect: Prijava na VPN server	. 20
Slika 27. Cisco AnyConnect: Obavijest o uspješnoj prijavi	. 20
Slika 28. Cisco AnyConnect: Cisco AnyConnect nakon uspješne prijave	. 21
Slika 29. Pristup mapi na datotečnom serveru	. 21
Slika 30. Pristup mapi na datotečnom serveru – nastavak	. 22
Slika 31. Pristup datoteci na datotečnom serveru	. 22
Slika 32. Otvaranje datoteke na datotečnom serveru	. 23
Slika 33. Wireshark – inicijalna komunikacija na vitrualnom sučelju	. 24
Slika 34. Wireshark – detalji o komunikaciji na virtualnom sučelju	. 24

Slika 35. Wireshark snimka – inicijalna komunikacija: uspostava VPN tunela	
Slika 36. Wireshark snimka – šifrirana komunikacija putem VPN tunela	
Slika 37. Wireshark snimka - Client Hello (paket 11)	
Slika 38. Wireshark snimka - Sever Hello (paket 13)	
Slika 39. Shema scenarija 2	
Slika 40. Pristupna lista	
Slika 41. Prikaz "hitcnt"	
Slika 42. Prikaz parametra "hitcnt" prije korištenja linije u pristupnoj listi	
Slika 43. Prikaz parametra "hitcnt" nakon korištenja linije u pristupnoj listi	
Slika 44. Prikaz veza	
Slika 45. Naredba "show xlate"	
Slika 46. Naredba "sh run nat"	
Slika 47. Prikaz IP adrese računala PC-1	
Slika 48. Naredba "ping" s računala PC-1 prema default gatewayu	
Slika 49. Naredba "ping" s računala PC-1 prema server Web server-1	
Slika 50. Uspješan dohvat web stranice servera Web server-1 s računala PC-1	
Slika 51. Prikaz IP adrese računala PC-2	
Slika 52. Naredba "ping" prema ASA vatroštitu	
Slika 53. Naredba "ping" prema Web serveru	
Slika 54. Stranica Web servera	
Slika 55. Wireshark snimka – inicijalizacija komunikacije	
Slika 56. Wireshark snimka – nešifrirana komunikacija	

# Popis tablica

Tablica 1: Prikaz karakteristika scenarija	
--	--

# Prilozi

U ovom prilogu se nalazi ispis važnijih dijelova konfiguracije vatroštita s objašnjenjima. Radna konfiguracija vatroštita se ispisuje naredbom "show runningconfig"<sup>[5]</sup>.

asa-petar# show running-config : Saved I #Serijski broj i hardverska konfiguracija# : Serial Number: JAD19280089 : Hardware: ASA5585-SSP-20, 11883 MB RAM, CPU Xeon 5500 series 2133 MHz, 1 CPU L #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 l interface GigabitEthernet0/1 nameif INSIDE security-level 100 ip address 192.168.0.1 255.255.255.0 I 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
I

#Vremenska ograničenja za NAT, PAT, veze i određene protokole# timeout xlate 3:00:00

timeout xiate 5.00.00 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#

L

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 I

#### #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 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#