

UNIVERZITET „DŽEMAL BIJEDIĆ“  
FAKULTET INFORMACIJSKIH TEHNOLOGIJA

**ZADAĆA**

S2S VPN LINK IZMEĐU DVA FIREWALLA ZA KOMUNIKACIJU  
IZMEĐU DVIJE MREŽE

Asistent:

mr. Adel Handžić

Student:

Zaim Mehić

Mostar, 2023.

## SADRŽAJ

1. UVOD.....	3
2. „PODIZANJE“ I SPAJANJE VIRTUELNIH MAŠINA.....	4
2.1. Priprema .....	4
2.2. Linux Lite virtuelne mašine .....	4
2.3. pfSense virtuelne mašine .....	9
3. KREIRANJE S2S TUNELA .....	13
3.1. FIT SIDE.....	13
3.2. ETF SIDE.....	17
4. POKRETANJE TUNELA .....	21
5. GATEWAY.....	23
6. PING.....	24

# 1. UVOD

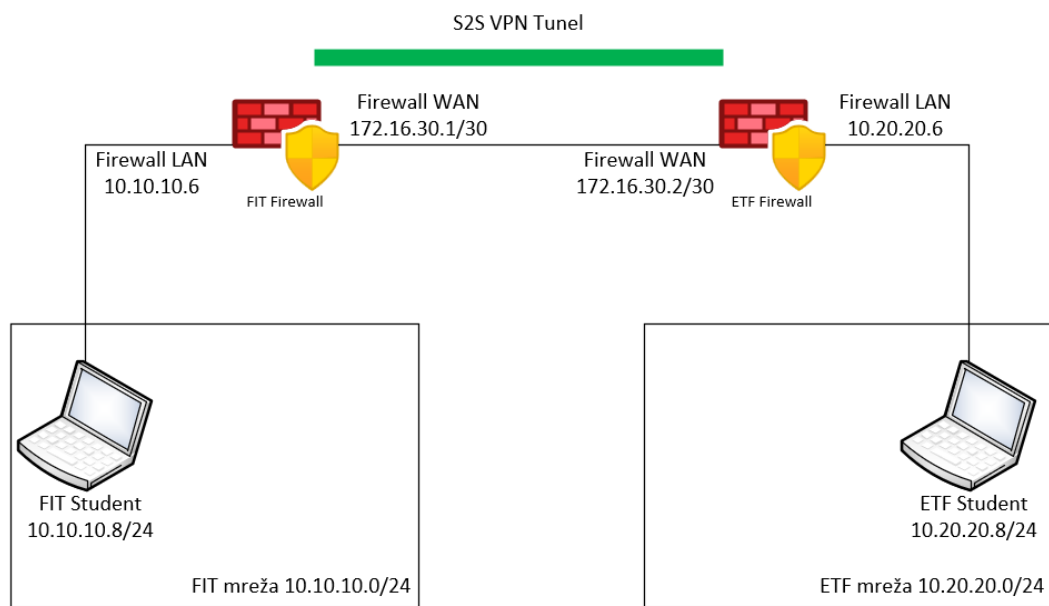
VPN (virtual private network) je sigurna, enkriptovana konekcija preko javne mreže.

Tuneliranje je proces kod kojeg VPN paketi čija izvorišna adresa je u nekoj privatnoj mreži, dolaze do destinacijske adrese, koja je najčešće unutar neke druge privatne mreže.

Mnoge VP mreže koriste grupu protokola IPsec (Internet Protocol secure). IPsec je grupa protokola koja se izvršava na mrežnom sloju. Promet u IPsec tunelu je u potpunosti enkriptovan, a dekripcija se dešava onda kada promet dođe do destinacijske mreže ili uređaja.

U poređenju sa drugim VPN protokolima za tuneliranje kao što su: SSL, TLS, SSH ili L2TP, IPsec tunel kreira „čvrste“ sigurnosne slojeve da u potpunosti zaštiti podatke koji se šalju putem mreže. IPsec tunel enkriptuje paket do te mjere da bilo koji entitet ne može vidjeti izvorišnu adresu ili destinacijsku adresu.

Način na koji je potrebno povezati zadanu mrežu nalazi se u nastavku:



Slika 1: Zadana mreža

U svrhu ovog zadatka „podignut“ ćemo četiri virtuelna mašine, od kojih je na dvije instaliran operativni sistem Linux Lite (zbog manjeg korištenja RAM memorije), a na druge dvije instaliran je firewall – pfSense.

Jedan od Linux Lite operativnih sistema bit će povezan sa jednim pfSense Firewall-om u mreži „10.10.10.0/24“, a drugi Linux Lite operativni sistem bit će povezan sa drugim pfSense Firewall-om u mreži „10.20.20.0/24“.

Firewall-i su međusobno povezani u mreži „172.16.30.0/30“ i između njih ćemo uspostaviti IPsec S2S VPN tunel kako bi dva kreirana operativna sistema mogla komunicirati.

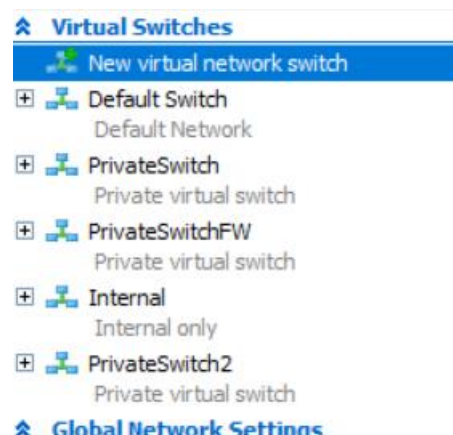
## 2. „PODIZANJE“ I SPAJANJE VIRTUELNIH MAŠINA

### 2.1. Priprema

Za podizanje virtuelnih mašina koristi ćemo Hyper-V Manager. Kako bismo uspostavili veze između virtuelnih mašina na način na koji želimo potrebno je da kreiramo Virtuelne Switch-eve.

Kreirani i korišteni Virtuelni Switch-evi su:

- a) PrivateSwitch – Za komunikaciju između jedne Linux Lite virtuelne mašine i jednog Firewall-a
- b) PrivateSwitch2 – Za komunikaciju između druge Linux Lite virtuelne mašine i drugog Firewall-a
- c) PrivateSwitchFW – Za komunikaciju između dva Firewall-a



Slika 2. – Virtuelni Switch-evi

U međuvremenu (prije ili nakon kreiranje Switch-eva) preuzimamo ISO file za:

- a) Operativni sistem Linux Lite 4.6 sa linka: <https://mirror.alpix.eu/linuxliteos/isos/4.6/>
- b) pfSense Firewall sa linka: <https://www.pfsense.org/download/>

### 2.2. Linux Lite virtuelne mašine

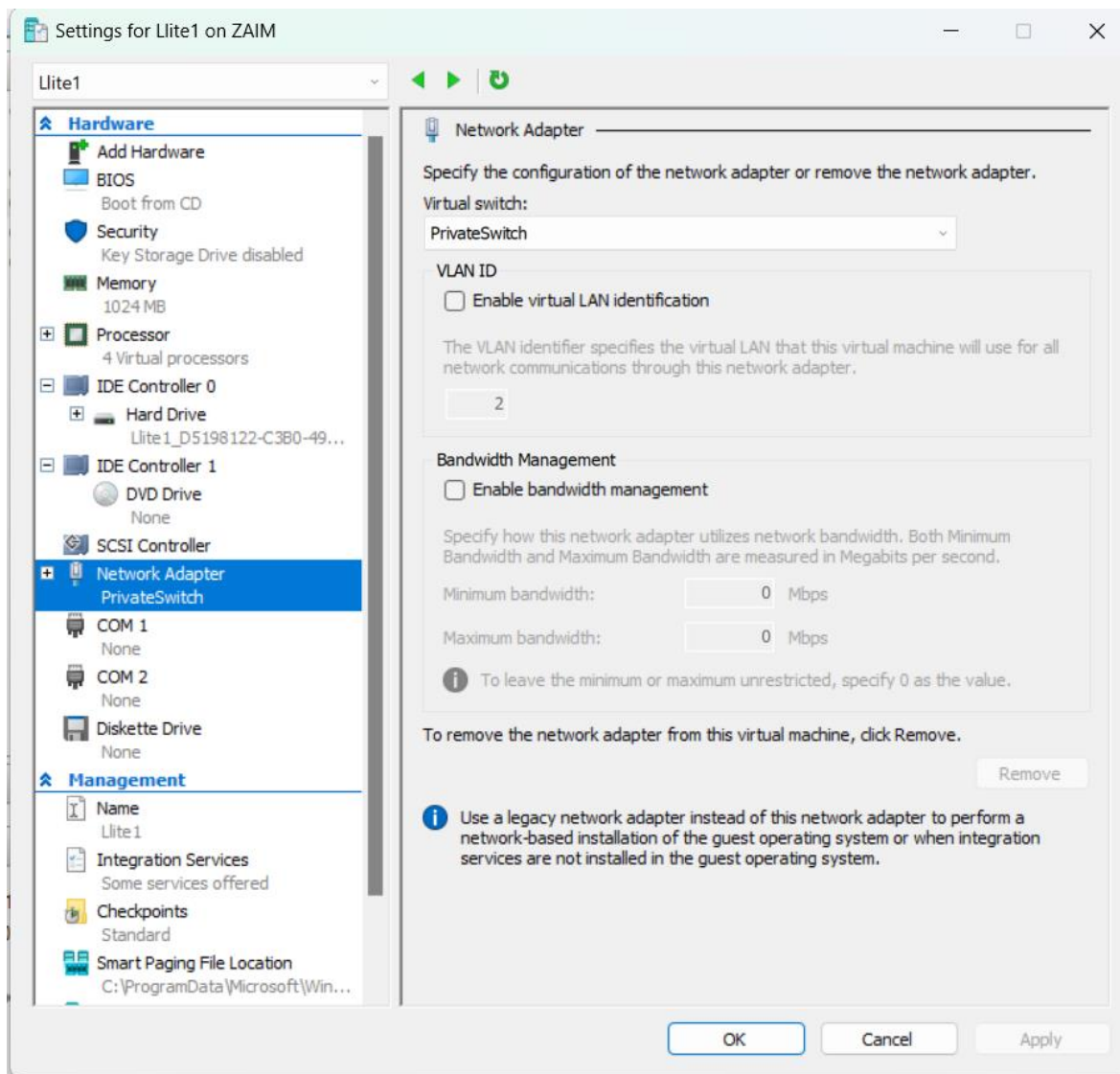
Minimalne sistemske specifikacije koje zahtjeva Linux Lite su:

- a) 1 GHz CPU

- b) 768 MB RAM
- c) 8 GB HDD ili SSD

Prvo ćemo kreirati virtuelnu mašinu Lite1, koja odgovara FIT Student računar na dijagramu.

Kreiranje virtuelne mašine izvodi se klasičnim putem, uz napomenu da se bira Generacija 1 prilikom kreiranja, te da se kao Network Adapter bira PrivateSwitch iz liste ponuđenih Virtuelnih Switch-eva.

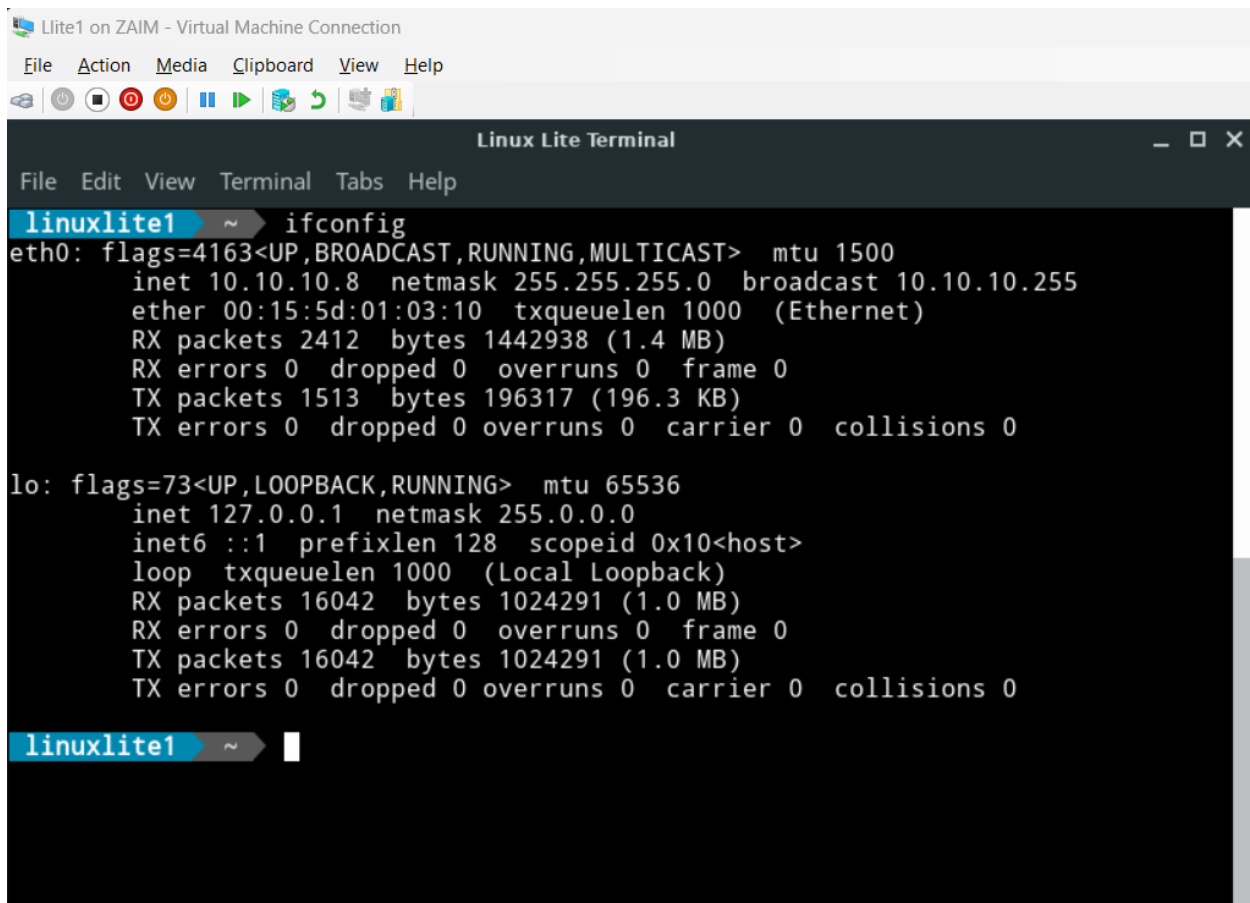


Slika 3. Linux Lite 1 Adapter Settings

Nakon podizanja sistema, potrebno je postaviti mrežne postavke. Sada ćemo postaviti IP adresu i Subnet masku, dok ćemo se sa Gateway-em pozabaviti nešto kasnije, pošto ćemo ga tek kasnije konfigurirati (sa drugačijom IP adresom od standardne).

Za postavljanje IP adrese i Subnet maske koristimo komandu:

- `sudo ifconfig eth0 10.10.10.8/24`



The screenshot shows a virtual machine window titled "Lite1 on ZAIM - Virtual Machine Connection". Inside, there is a "Linux Lite Terminal" window. The terminal has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The prompt is "linuxlite1 ~". The command "ifconfig" has been executed, showing the configuration for the "eth0" and "lo" interfaces. The "eth0" interface is configured with IP address 10.10.10.8, netmask 255.255.255.0, and broadcast address 10.10.10.255. The "lo" interface is configured with IP address 127.0.0.1 and netmask 255.0.0.0.

```
linuxlite1 ~ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.8 netmask 255.255.255.0 broadcast 10.10.10.255
    ether 00:15:5d:01:03:10 txqueuelen 1000 (Ethernet)
    RX packets 2412 bytes 1442938 (1.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1513 bytes 196317 (196.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 16042 bytes 1024291 (1.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16042 bytes 1024291 (1.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

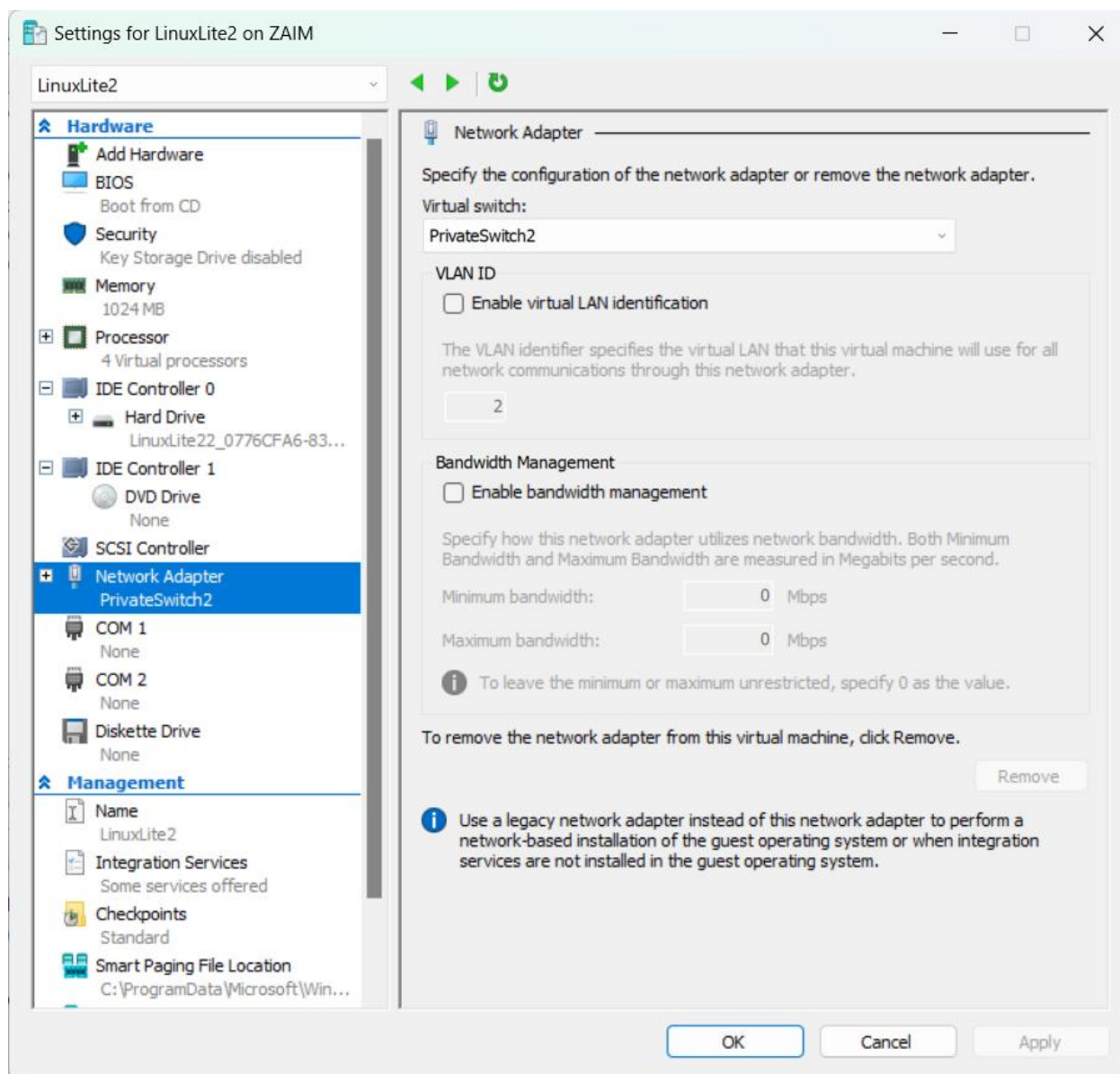
linuxlite1 ~
```

Slika 4. ifconfig Lite1

Koristeći komandu `ifconfig` možemo potvrditi da je IP adresa Network Adapter-a na Lite1 virtualnoj mašini uistinu 10.10.10.8.

Nakon što smo (za sada) završili sa Lite1 virtuelnom mašinom, kreiramo drugu koja se naziva „LinuxLite2“ i ekvivalentna je ETF Student računar sa dijagrama iznad.

Virtuelnu mašinu kreiramo na isti način kao prethodnu, uz iznimku gdje za Network Adapter ove mašine biramo PrivateSwitch2.



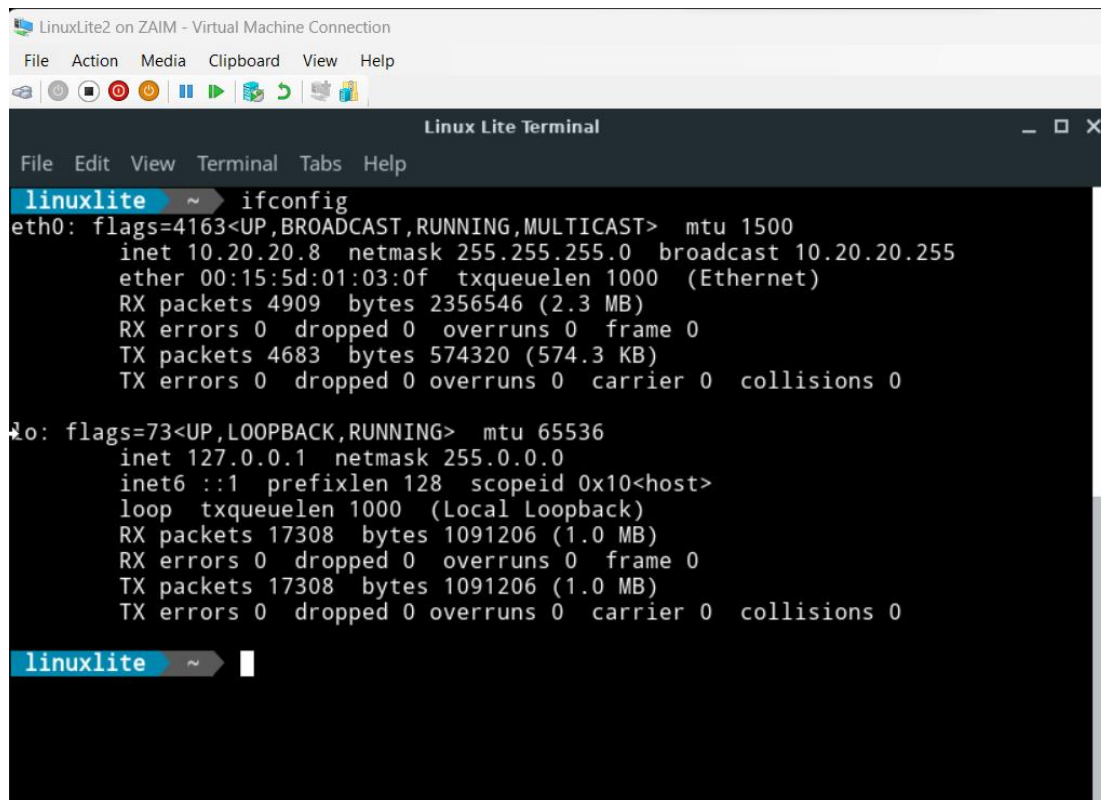
Slika 5. LinuxLite2 Adapter Settings

Na isti način kao i na prethodnoj mašini postavljajmo IP adresu i subnet masku koristeći komandu:

- `sudo ifconfig eth0 10.20.20.8/24`

Ova komanda postavlja IP adresu mrežnog adaptera ove virtualna mašine na 10.20.20.8, a Subnet maska je 255.255.255.0.

Koristeći komandu ifconfig pregledat ćemo mrežne postavke na ovoj virtualnoj mašini.



```
Linux Lite Terminal
File Edit View Terminal Tabs Help

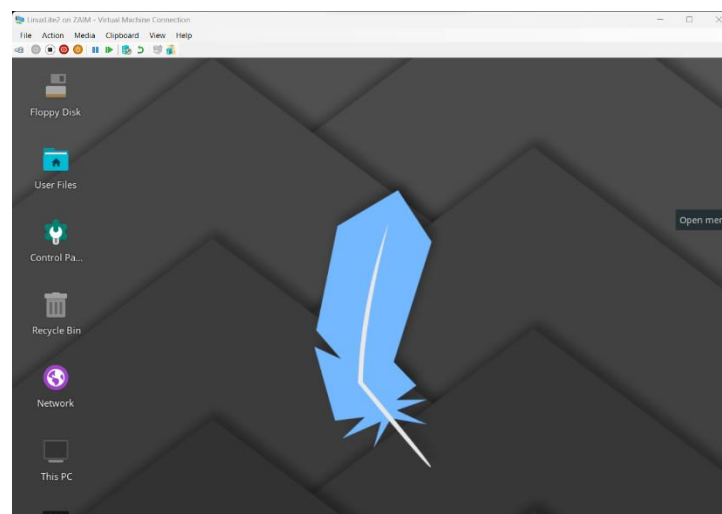
linuxlite ~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.20.8 netmask 255.255.255.0 broadcast 10.20.20.255
    ether 00:15:5d:01:03:0f txqueuelen 1000 (Ethernet)
    RX packets 4909 bytes 2356546 (2.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4683 bytes 574320 (574.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 17308 bytes 1091206 (1.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 17308 bytes 1091206 (1.0 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

linuxlite ~$
```

Slika 6. ifconfig LinuxLite2

Uvidom u rezultat navedene komande zaključujemo da su komande izvršene prije postavile vrijednosti onako kako to smo i željeli.



Slika 7. Linux Lite OS

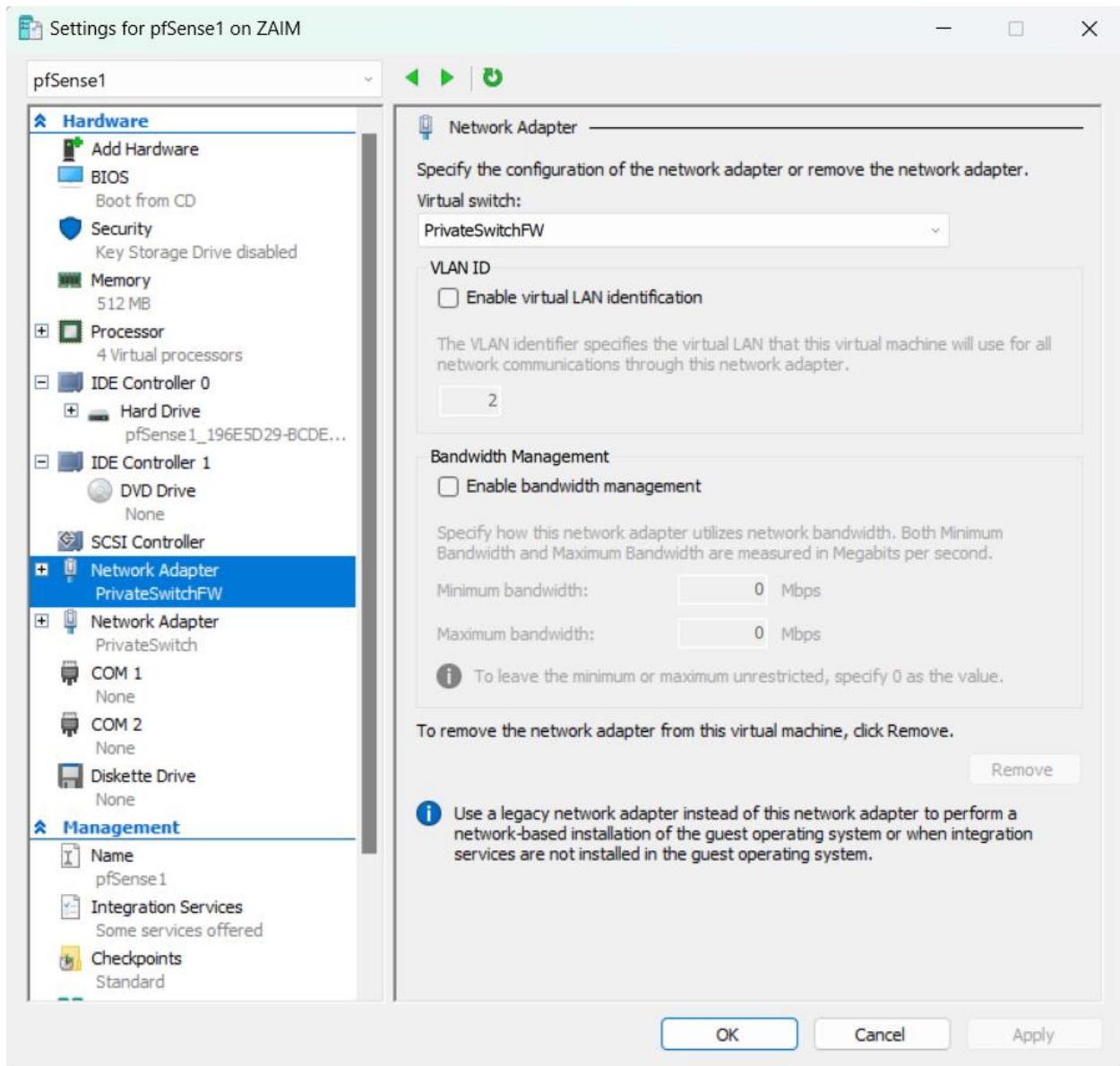


### 2.3. pfSense virtualne mašine

Prvo ćemo kreirati Firewall koji ima konekciju sa FIT mrežom, virtualnom mašinom FIT Student ili u našem slučaju Lite1.

Kreiranje mašine izvodi se na klasičan način, sa napomenom da se izabere Generacija 1. Što se tiče mrežnih adaptera, u slučaju Firewall-a trebaju nam dva. Jedan za konekciju sa lokalnom mrežom (PrivateSwitch), te jedan za konekciju sa „eksternim“ mrežama (PrivateSwitchFW).

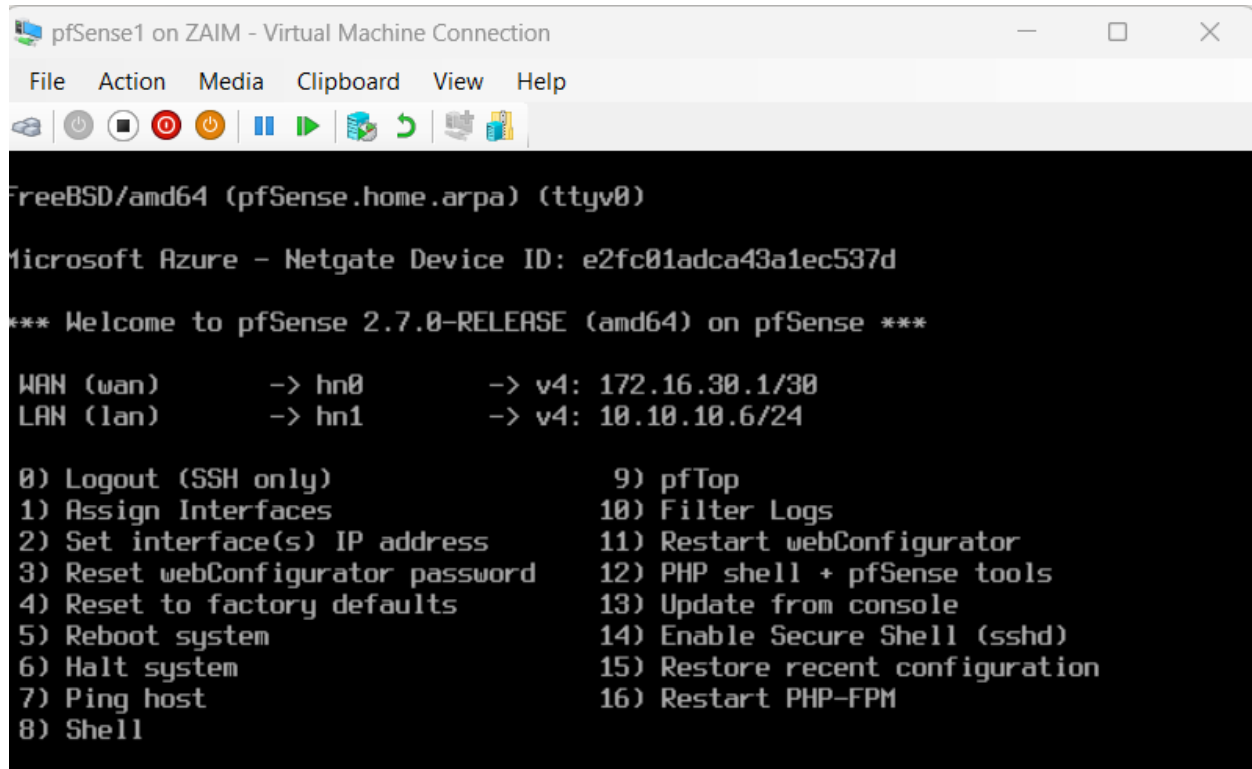
Pa tako nakon kreiranje virtualna mašine za prvi Firewall, pfSense1, postavke mrežnih adaptera prikazane su u nastavku.



Slika 8. – pfSense1 Adapter Settings

Nakon što smo definisali ove postavke krećemo sa instalacijom Firewall-a. O instalaciji nećemo pretjerano govoriti, pošto smo istu obrađivali na Vježbama, pa ćemo se više fokusirati na postavke Firewall-a.

Nakon instalacije prikaže nam se određeni UI u komandnoj liniji koji je prikazan u nastavku



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

Microsoft Azure - Netgate Device ID: e2fc01adca43a1ec537d

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> hn0      -> v4: 172.16.30.1/30
LAN (lan)      -> hn1      -> v4: 10.10.10.6/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell
```

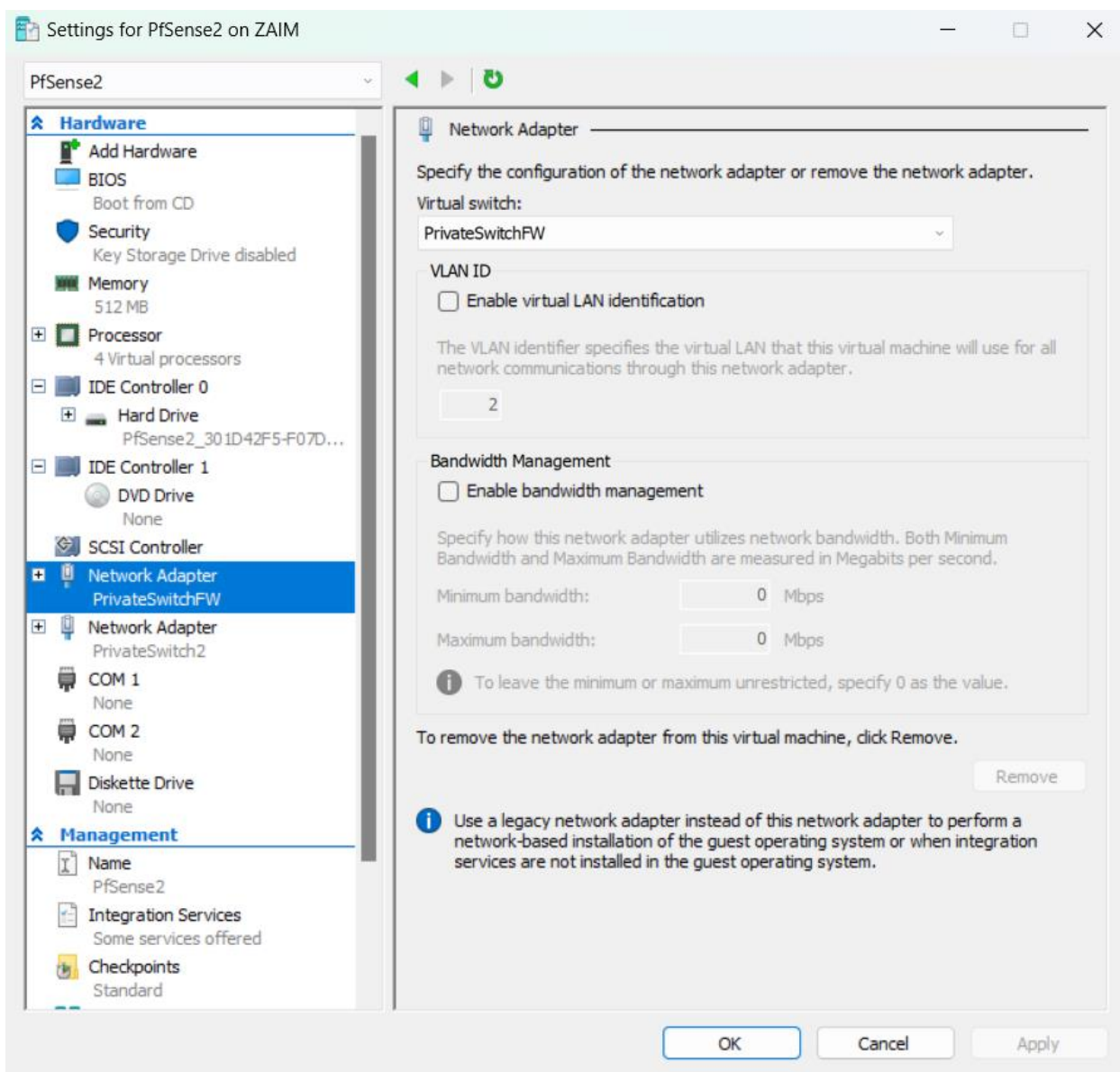
Slika 9. – pfSense1 UI

WAN i LAN IPv4 adrese u inicijalnom pokretanju Firewall-a nisu bile definisane na način prikazan na slici iznad. Da bismo iste definisali odabrali smo opciju 2) Set interface(s) IP address i krenuli smo sa WAN IP adresom. Prema zadatom dijagramu postavljena je adresa 172.16.30.1/30 i preko nje će se povezati sa drugim Firewall-om.

Ponovo istom opcijom mijenjali smo LAN IP adresu, i ta adresa koristit će se kao Gateway za našu mrežu prema ostalim mrežama. Odabrana je adresa 10.10.10.6/24 za potrebe ove vježbe, a inače se koristi prva iskoristiva ili 10.10.10.1/24.

Nakon definisanja ovih postavki, omogućeno je računaru Lite1 da putem lokalne mreže komunicira sa Firewall-om. Kucanjem adrese 10.10.10.6 u web browser prikazuje se UI za upravljanje Firewall-om, što znači da smo uspostavili dobru komunikaciju.

Istu priču ponovimo i za drugi Firewall, pfSense2:

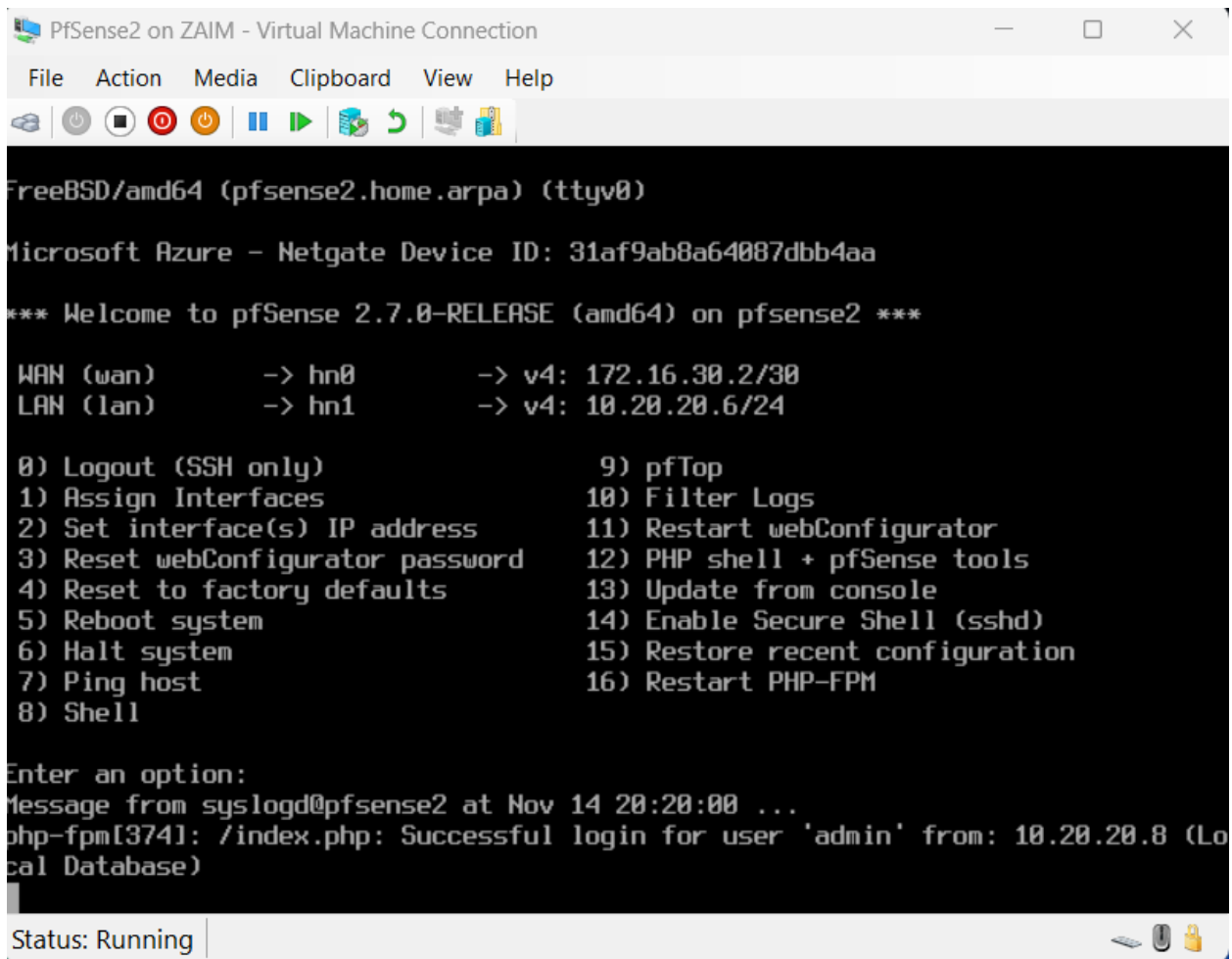


Slika 10. – pfSense2 Adapter Settings

Što se tiče WAN i LAN adresa, postavljamo ih na isti način kao i za prethodni Firewall, uz važnu napomenu da LAN nije u istoj mreži kao i kod prethodnog, pošto se ovaj Firewall nalazi na drugoj strani komunikacije, u mreži ETF. Shodno tome LAN IP adresa je 10.20.20.6/24 i predstavlja Gateway za tu mrežu prema „eksternim“ mrežama.

Preko WAN interfejsa Firewall pfSense2(ETF) povezan je sa Firewall-om pfSense1(FIT), odnosno u istoj su mreži, pa smo za njegovu IP adresu uzeli 172.16.30.2/30.

Kucanjem u Web Browser LAN IP adrese pristupa se kontrolnom okruženju Firewall-a kojim ćemo se baviti u nastavku.



Slika 11. pfSense2 UI

Nakon što smo odradili prethodne korake, imamo 4 virtuelne mašine i to:

- a) Lite1 (FIT Student, OS Linux Lite)
- b) LinuxLite2 (ETF Student, OS Linux Lite)
- c) pfSense1 (FIT Firewall, pfSense)
- d) pfSense2(ETF Firewall, pfSense)

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuratio...
Kali Linux	Off					11.0
LinuxLite2	Running	0%	1024 MB	01:08:57		11.0
Lite1	Running	0%	1024 MB	00:57:25		11.0
pfSense1	Running	0%	512 MB	01:07:20		11.0
PfSense2	Running	0%	512 MB	01:01:38		11.0

Slika 12. Virtuelne mašine


### 3. KREIRANJE S2S TUNELA

#### 3.1. FIT SIDE


Da bismo kreirali S2S VPN tunel potrebno je da uđemo na pfSense UI putem browsera, logiramo se koristeći podatke username: admin, password: pfsense. Na navigacijskoj traci tražimo VPN i nakon klika otvara nam se padajući meni gdje biramo IPsec.



Krenirimo od pfSense1. Dodajemo P1 i unosimo sljedeću konfiguraciju:

General Information	
Description	<input type="text" value="Side FIT"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1

IKE Endpoint Configuration	
Key Exchange version	<input type="text" value="IKEv2"/> <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	<input type="text" value="IPv4"/> <small>Select the Internet Protocol family.</small>
Interface	<input type="text" value="WAN"/> <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	<input type="text" value="172.16.30.2"/> <small>Enter the public IP address or host name of the remote gateway. </small>

Slika 13. pfSense1 P1/1

Phase 1 Proposal (Authentication)	
Authentication Method	<input type="text" value="Mutual PSK"/> <small>Must match the setting chosen on the remote side.</small>
My identifier	<input type="text" value="My IP address"/>
Peer identifier	<input type="text" value="Peer IP address"/>
Pre-Shared Key	<input type="text" value="6c92dc4f59b3d1cac8e1d6241f8846aeeb2d496d088f4l"/> <small>Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.</small> 

Phase 1 Proposal (Encryption Algorithm)	
Encryption Algorithm	<input type="text" value="AES"/> <input type="text" value="256 bits"/> <input type="text" value="SHA256"/> <input type="text" value="20 (nist ecp384)"/> 
<small>Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</small>	
Add Algorithm	

Slika 14. pfSense1 P1/2

Expiration and Replacement	
<b>Life Time</b>	<input type="text" value="86400"/> Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)
<b>Rekey Time</b>	<input type="text" value="77760"/> Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.
<b>Reauth Time</b>	<input type="text" value="0"/> Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.
<b>Rand Time</b>	<input type="text" value="8640"/> A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Slika 15. pfSense1 P1/3

Remote Gateway je WAN adresa drugog Firewall-a. Na Slici 11. vidimo da je to 172.16.30.2. U ovoj fazi generišemo Pre-Shared Key koji ćemo trebati prekopirati u P1 konfiguraciju drugog Firewalla. Ostatak konfiguracije za ovaj Firewall ostaje nepromijenjen.

Nakon što smo završili sa P1 ovog Firewall-a, dodajemo P2 i postavljamo sljedeću konfiguraciju:

General Information	
<b>Description</b>	<input type="text" value="Side FIT P2"/> A description may be entered here for administrative reference (not parsed).
<b>Disabled</b>	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
<b>Mode</b>	<input type="text" value="Tunnel IPv4"/>
<b>Phase 1</b>	Side FIT (IKE ID 1)
<b>P2 reqid</b>	1
Networks	
<b>Local Network</b>	<div> <input type="text" value="Network"/> <input type="text" value="10.10.10.0"/> <input type="text" value="24"/> </div> Type Address Local network component of this IPsec security association.
<b>NAT/BINAT translation</b>	<div> <input type="text" value="None"/> <input type="text" value="0"/> </div> Type Address If NAT/BINAT is required on this network specify the address to be translated
<b>Remote Network</b>	<div> <input type="text" value="Network"/> <input type="text" value="10.20.20.0"/> <input type="text" value="24"/> </div> Type Address

Slika 16. pfSense1 P2/1

Phase 2 Proposal (SA/Key Exchange)	
<b>Protocol</b>	<div>ESP</div> <div>Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.</div>
<b>Encryption Algorithms</b>	<div> <input checked="" type="checkbox"/> AES <div>256 bits</div> </div> <div> <input type="checkbox"/> AES128-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> AES192-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> AES256-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> CHACHA20-POLY1305 </div>
<b>Hash Algorithms</b>	<div> <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC </div> <div>Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.</div>
<b>PFS key group</b>	<div>20 (nist ecp384)</div> <div>Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</div>

Slika 17. pfSense1 P2/2

Expiration and Replacement	
<b>Life Time</b>	<div>3600</div> <div>Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.</div>
<b>Rekey Time</b>	<div>3240</div> <div>Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.</div>
<b>Rand Time</b>	<div>360</div> <div>A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.</div>

Slika 18. pfSense1 P2/3

Ostatak konfiguracije ostaviti nepromijenjenim i prelazimo na konfiguraciju tunela za drugi Firewall pfSense2.

Tuneli na pfSense1 izgledaju ovako:

Lite1 on ZAIM - Virtual Machine Connection

File Action Media Clipboard View Help

pfSense.home.arpa - VPN: IPsec: Tunnels - Mozilla Firefox

File Edit View History Bookmarks Tools Help

pfSense.home.arpa - VPN x

https://10.10.10.6/vpn\_ipsec.php

Help Manual Support Forums Google Search

**WARNING:** The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

VPN / IPsec / Tunnels

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

IPsec Tunnels									
	ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
<input type="checkbox"/> Disable	1	V2	WAN 172.16.30.2		AES (256 bits)	SHA256	20 (nist ecp384)	Side FIT	

	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
<input type="checkbox"/> Disable	1	tunnel	10.10.10.0/24	10.20.20.0/24	ESP	AES (256 bits)	SHA256	Side FIT P2	

+ Add P2

+ Add P1 Delete P1s


Slika 19. – pfSense1 Tunnels



### 3.2. ETF SIDE


Vršimo u potpunosti istu konfiguraciju, jedina razlika je što Pre-Shared Key ne generišemo, nego isti prepisemo za prvog Firewall-a, pa konfiguracija za P1 izgleda ovako:

General Information	
Description	<input type="text" value="Side ETF P1"/> <small>A description may be entered here for administrative reference (not parsed).</small>
Disabled	<input type="checkbox"/> Set this option to disable this phase1 without removing it from the list.
IKE ID	1

IKE Endpoint Configuration	
Key Exchange version	<input type="text" value="IKEv2"/> <small>Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.</small>
Internet Protocol	<input type="text" value="IPv4"/> <small>Select the Internet Protocol family.</small>
Interface	<input type="text" value="WAN"/> <small>Select the interface for the local endpoint of this phase1 entry.</small>
Remote Gateway	<input type="text" value="172.16.30.1"/> <small>Enter the public IP address or host name of the remote gateway. </small>

Slika 20. – pfSense2 P1/1

Phase 1 Proposal (Authentication)	
Authentication Method	<input type="text" value="Mutual PSK"/> <small>Must match the setting chosen on the remote side.</small>
My identifier	<input type="text" value="My IP address"/>
Peer identifier	<input type="text" value="Peer IP address"/>
Pre-Shared Key	<input type="text" value="6c92dc4f59b3d1cac8e1d6241f8846aeedb2d496d088f4l"/> <small>Enter the Pre-Shared Key string. This key must match on both peers. This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.</small> <a href="#">Generate new Pre-Shared Key</a>


Phase 1 Proposal (Encryption Algorithm)					
Encryption Algorithm	<input type="text" value="AES"/>	<input type="text" value="256 bits"/>	<input type="text" value="SHA256"/>	<input type="text" value="20 (nist ecp384)"/>	 Delete
	Algorithm	Key length	Hash	DH Group	
<small>Note: SHA1 and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</small>					
Add Algorithm	<a href="#">+ Add Algorithm</a>				

Slika 21. – pfSense2 P1/2

Expiration and Replacement	
<b>Life Time</b>	<input type="text" value="86400"/> Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)
<b>Rekey Time</b>	<input type="text" value="77760"/> Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.
<b>Reauth Time</b>	<input type="text" value="0"/> Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.
<b>Rand Time</b>	<input type="text" value="8640"/> A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Slika 22. – pfSense2 P1/3

Nakon što završimo sa ovom konfiguracijom, nastavljamo sa P2.

General Information	
<b>Description</b>	<input type="text" value="Side ETF P2"/> A description may be entered here for administrative reference (not parsed).
<b>Disabled</b>	<input type="checkbox"/> Disable this phase 2 entry without removing it from the list.
<b>Mode</b>	<input type="text" value="Tunnel IPv4"/>
<b>Phase 1</b>	Side ETF P1 (IKE ID 1) 
<b>P2 reqid</b>	1

Networks	
<b>Local Network</b>	<div> <input type="text" value="Network"/> <input type="text" value="10.20.20.0"/> <input type="text" value="24"/> </div> Type Address Local network component of this IPsec security association.
<b>NAT/BINAT translation</b>	<div> <input type="text" value="None"/> <input type="text" value="0"/> </div> Type Address If NAT/BINAT is required on this network specify the address to be translated
<b>Remote Network</b>	<div> <input type="text" value="Network"/> <input type="text" value="10.10.10.0"/> <input type="text" value="24"/> </div> Type Address

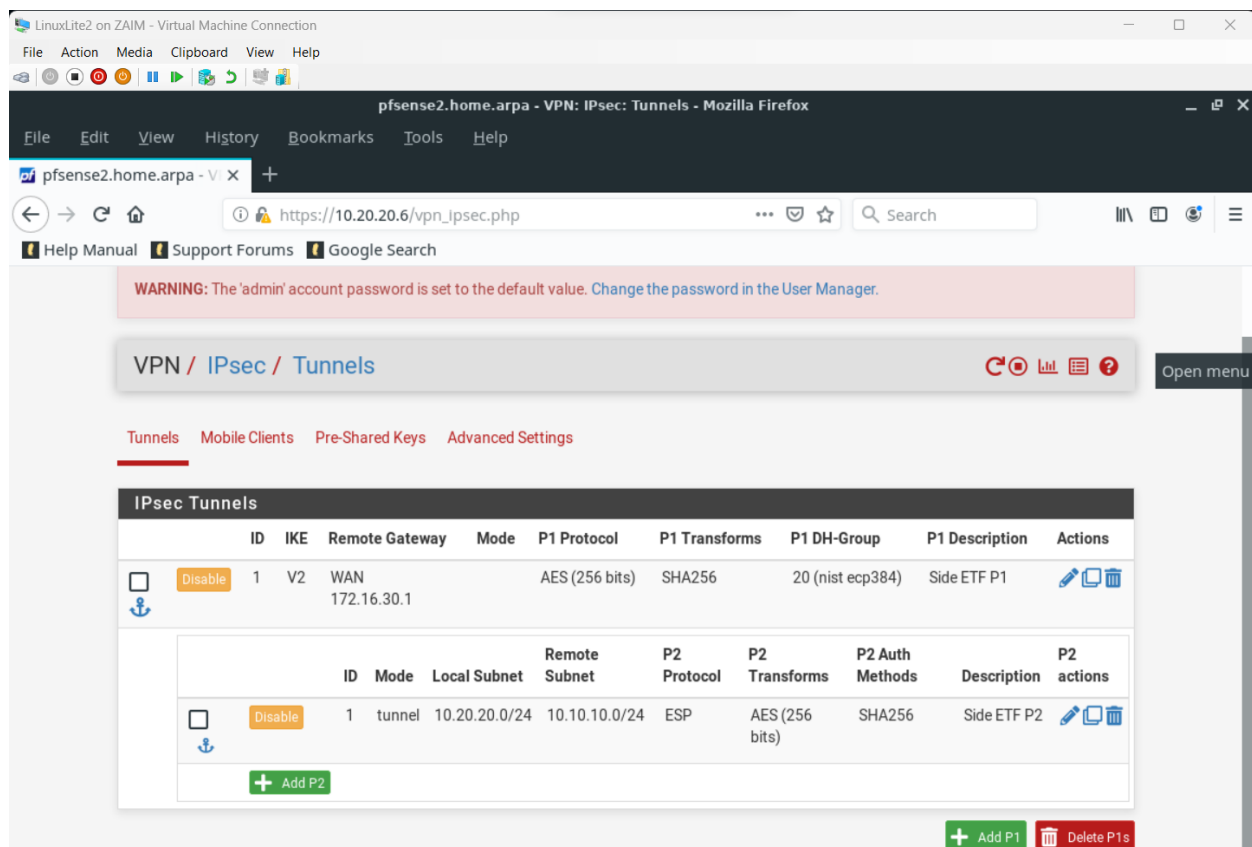
Slika 23. – pfSense2 P2/1

Phase 2 Proposal (SA/Key Exchange)	
<b>Protocol</b>	<div>ESP</div> <div>Encapsulating Security Payload (ESP) performs encryption and authentication, Authentication Header (AH) is authentication only.</div>
<b>Encryption Algorithms</b>	<div> <input checked="" type="checkbox"/> AES <div>256 bits</div> </div> <div> <input type="checkbox"/> AES128-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> AES192-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> AES256-GCM <div>Auto</div> </div> <div> <input type="checkbox"/> CHACHA20-POLY1305 </div>
<b>Hash Algorithms</b>	<div> <input type="checkbox"/> SHA1 <input checked="" type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC </div> <div>Note: Hash is ignored with GCM algorithms. SHA1 provides weak security and should be avoided.</div>
<b>PFS key group</b>	<div>20 (nist ecp384)</div> <div>Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.</div>

Slika 24. pfSense2 P2/2

Expiration and Replacement	
<b>Life Time</b>	<div>3600</div> <div>Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.</div>
<b>Rekey Time</b>	<div>3240</div> <div>Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.</div>
<b>Rand Time</b>	<div>360</div> <div>A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.</div>

Slika 25. pfSense P2/3



Slika 26. – pfSense2 Tunnels

## 4. POKRETANJE TUNELA

IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	Side FIT	ID: 172.16.30.1 Host: 172.16.30.1	ID: 172.16.30.2 Host: 172.16.30.2				Disconnected <a href="#">➡ Connect P1 and P2s</a> <a href="#">➡ Connect P1</a>

Slika 27. pfSense1 Tunnels Status

Klikom na dugme „Connect P1 and P2s“ uspostavlja se tunel i istu operaciju ne bismo trebali ponoviti na drugom Firewall-u pošto se ista automatski postavi.

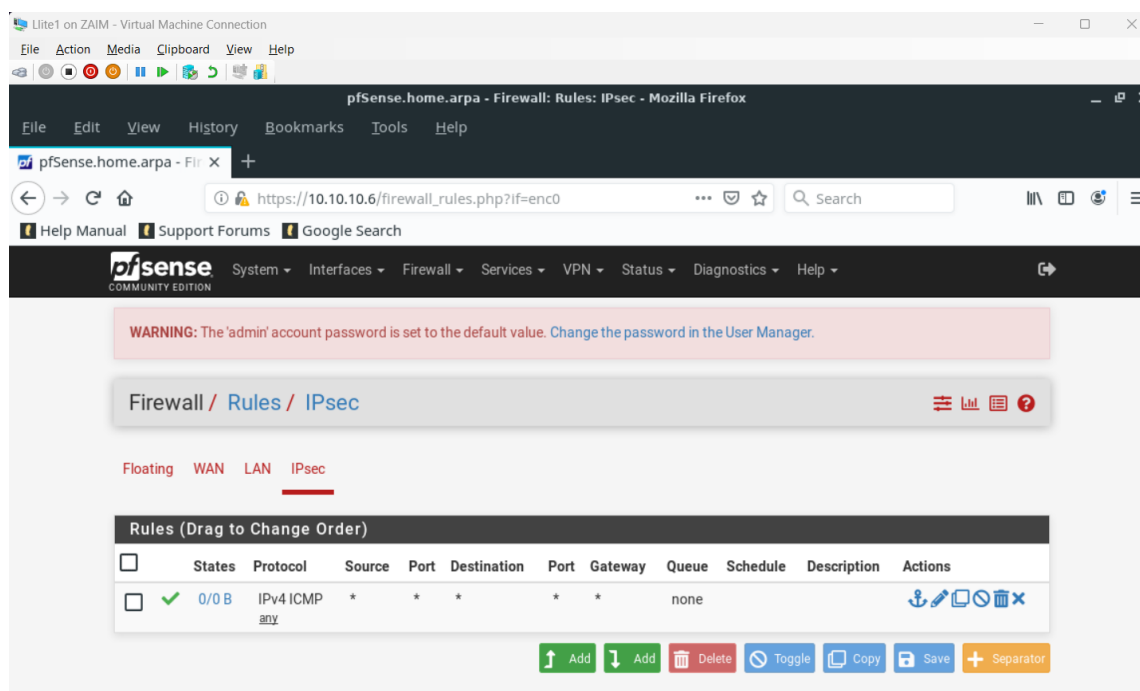
IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #4	Side FIT	ID: 172.16.30.1 Host: 172.16.30.1:500 SPI: 35de65f379bd16c7	ID: 172.16.30.2 Host: 172.16.30.2:500 SPI: 697acd31b2356912	IKEv2 Initiator	Rekey: 76090s (21:08:10) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 ECP_384	Established 14 seconds (00:00:14) ago <a href="#">Disconnect P1</a>
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #10	Side FIT P2	10.10.10.0/24	Local: cfe22144 Remote: c012f48a	10.20.20.0/24	Rekey: 2982s (00:49:42) Life: 3586s (00:59:46) Install: 14s (00:00:14)	AES_CBC (256) HMAC_SHA2_256_128 IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0 Installed <a href="#">Disconnect P2</a>

Slika 28. – pfSense1 IPsec Status

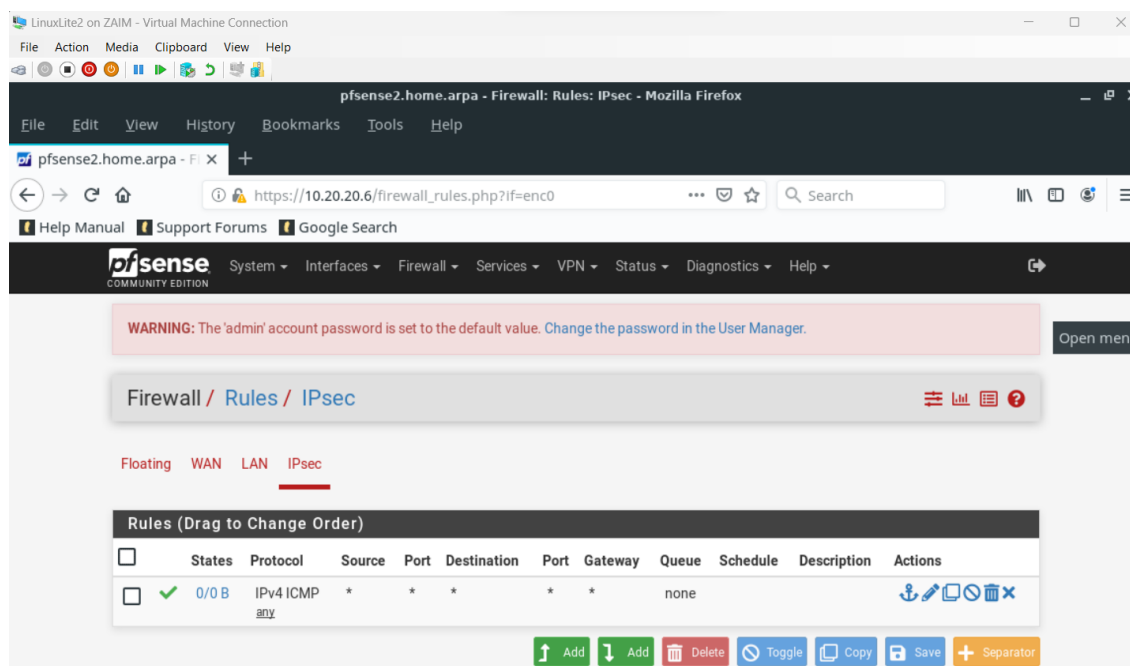
IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #4	Side ETF P1	ID: 172.16.30.2 Host: 172.16.30.2:500 SPI: 697acd31b2356912	ID: 172.16.30.1 Host: 172.16.30.1:500 SPI: 35de65f379bd16c7	IKEv2 Responder	Rekey: 75296s (20:54:56) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 ECP_384	Established 55 seconds (00:00:55) ago <a href="#">Disconnect P1</a>
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #6	Side ETF P2	10.20.20.0/24	Local: c012f48a Remote: cfe22144	10.10.10.0/24	Rekey: 3061s (00:51:01) Life: 3545s (00:59:05) Install: 55s (00:00:55)	AES_CBC (256) HMAC_SHA2_256_128 IPComp: None	Bytes-In: 0 (0 B) Packets-In: 0 Bytes-Out: 0 (0 B) Packets-Out: 0 Installed <a href="#">Disconnect P2</a>

Slika 29. - pfSense2 IPsec Status

Nakon uspostavljanja tunela potrebno je definisati pravila (Rules) putem kojih će se određivati koji saobraćaj želimo propustiti kroz Firewall, a koji saobraćaj želimo blokirati. Ukoliko pravilno ne postavimo pravila, ETF i FIT Student neće moći komunicirati.



Slika 30. – pfSense1 Rules

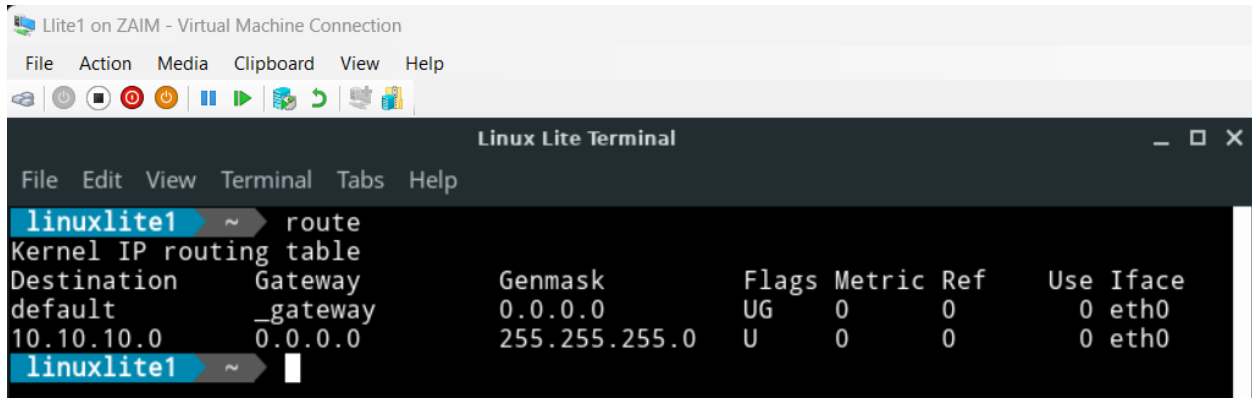


Slika 31. – pfSense2 Rules

## 5. GATEWAY

Prije nego što uspostavimo komunikaciju između ETF i FIT studenta, potrebno je da se vratimo na njihove mašine i da konfigurišemo Gateway. Gateway predstavlja izlaz iz lokalne mreže i potrebno je svakom od računara pokazati gdje mu je izlaz.

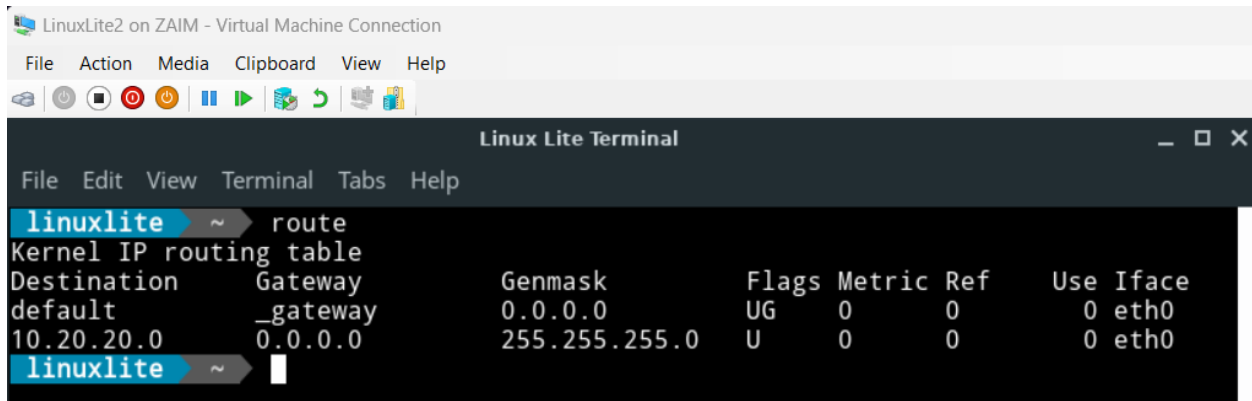
Komandom „`sudo route add default gw 10.10.10.6`“ postavili smo adresu Gateway-a, a komandom „`route`“ možemo pregledati konfiguraciju.



```
linuxlite1 ~ ➤ route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          _gateway        0.0.0.0         UG    0      0      0 eth0
10.10.10.0       0.0.0.0         255.255.255.0   U     0      0      0 eth0
linuxlite1 ~ ➤
```

Slika 32. – Lite1 Route

Isto moramo učiniti i za ETF Studenta, ovoga puta komandom „`sudo route add default gw 10.20.20.6`“



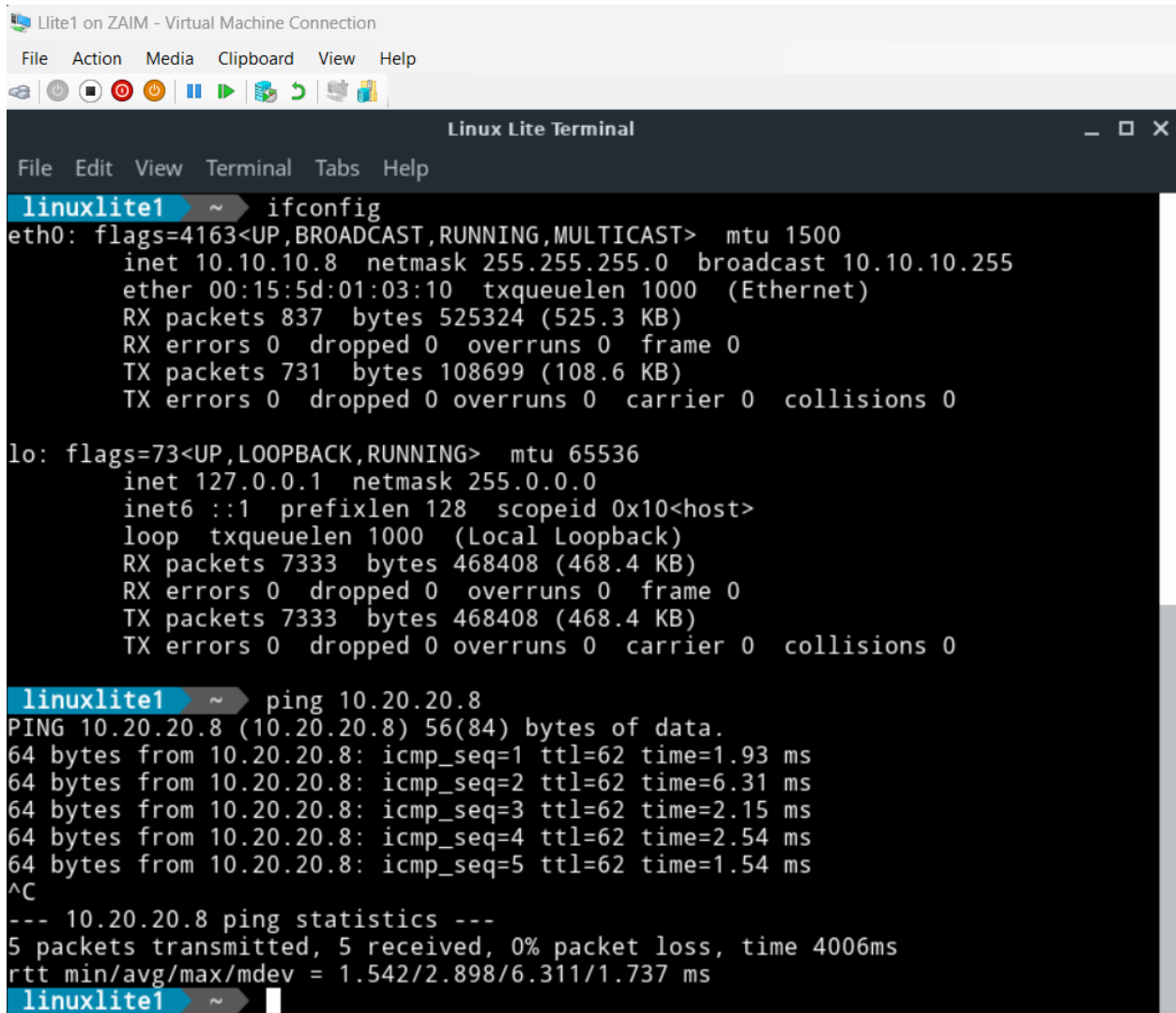
```
linuxlite ~ ➤ route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          _gateway        0.0.0.0         UG    0      0      0 eth0
10.20.20.0       0.0.0.0         255.255.255.0   U     0      0      0 eth0
linuxlite ~ ➤
```

Slika 33. LinuxLite2 Route.

Od ovog trenutka moguće je komunicirati sa FIT Student virtuelne mašine sa IP adresom 10.10.10.8/24 sa ETF Student virtuelnom mašinom sa IP adresom 10.20.20.8/24 preko IPsec S2S VPN tunela.

## 6. PING

Kako bismo dokazali da virtuelne mašine mogu komunicirati koristit ćemo komandu „ping“ da vidimo da li pakekti mogu doći do odredišta i da li će se vratiti.



```
Linux Lite Terminal
File Edit View Terminal Tabs Help

linuxlite1 ~ # ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.8 netmask 255.255.255.0 broadcast 10.10.10.255
    ether 00:15:5d:01:03:10 txqueuelen 1000 (Ethernet)
    RX packets 837 bytes 525324 (525.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 731 bytes 108699 (108.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 7333 bytes 468408 (468.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7333 bytes 468408 (468.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

linuxlite1 ~ # ping 10.20.20.8
PING 10.20.20.8 (10.20.20.8) 56(84) bytes of data:
64 bytes from 10.20.20.8: icmp_seq=1 ttl=62 time=1.93 ms
64 bytes from 10.20.20.8: icmp_seq=2 ttl=62 time=6.31 ms
64 bytes from 10.20.20.8: icmp_seq=3 ttl=62 time=2.15 ms
64 bytes from 10.20.20.8: icmp_seq=4 ttl=62 time=2.54 ms
64 bytes from 10.20.20.8: icmp_seq=5 ttl=62 time=1.54 ms
^C
--- 10.20.20.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.542/2.898/6.311/1.737 ms
linuxlite1 ~ #
```

Slika 34. – Ping sa FIT na ETF Student



```
LinuxLite2 on ZAIM - Virtual Machine Connection
File Action Media Clipboard View Help

Linux Lite Terminal
File Edit View Terminal Tabs Help

linuxlite ~ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.20.20.8 netmask 255.255.255.0 broadcast 10.20.20.255
    ether 00:15:5d:01:03:0f txqueuelen 1000 (Ethernet)
    RX packets 344 bytes 272647 (272.6 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 356 bytes 51908 (51.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 5220 bytes 340240 (340.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 5220 bytes 340240 (340.2 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

linuxlite ~ ping 10.10.10.8
PING 10.10.10.8 (10.10.10.8) 56(84) bytes of data.
64 bytes from 10.10.10.8: icmp_seq=1 ttl=62 time=1.78 ms
64 bytes from 10.10.10.8: icmp_seq=2 ttl=62 time=2.64 ms
64 bytes from 10.10.10.8: icmp_seq=3 ttl=62 time=1.61 ms
64 bytes from 10.10.10.8: icmp_seq=4 ttl=62 time=1.84 ms
64 bytes from 10.10.10.8: icmp_seq=5 ttl=62 time=1.75 ms
^C
--- 10.10.10.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.611/1.928/2.641/0.364 ms
linuxlite ~
```

Slika 35. – Ping sa ETF na FIT Student