

# Criptografia e Segurança Informática

## 2ª Trabalho Prático

Henrique Coutinho, Nº 16984

**Curso Técnico Superior Profissional em Redes e Segurança Informática**

Barcelos, janeiro 2020

## Índice

Introdução .....	4
Instalação da pfSense .....	5
Criação e Configuração das Interfaces .....	6
DHCP Server.....	9
Definições Avançadas do Sistema .....	10
User Manager.....	11
Funcionalidades SSH .....	11
Regras de Firewall .....	13
VPN IPsec – Fase 1.....	15
VPN IPsec – Fase 2.....	16
System Logs.....	18
Snort.....	20
Certificados.....	24
Conclusão .....	26

## Índice de Imagens

Figura 1 - Máquina Virtual .....	5
Figura 2 - Máquina Virtual – LAN.....	5
Figura 3 - Máquina Virtual – DMZ.....	5
Figura 4 - Consola pfSense .....	6
Figura 5 - Hostname e Domain.....	6
Figura 6 - Interface Assignments .....	7
Figura 7 - Configuração WAN .....	7
Figura 8 - Configuração LAN .....	8
Figura 9 - Configuração DMZ .....	8
Figura 10 - DHCP Server LAN .....	9
Figura 11 - Definições Avançadas do Sistema 1 .....	10
Figura 12 - Definições Avançadas do Sistema 2 .....	10
Figura 13 - User Manager .....	11
Figura 14 - PuTTY GEN.....	11
Figura 15 - Passphrase .....	12
Figura 16 - Processo Iniciado Em segundo Plano.....	12
Figura 17 - Configuração PuTTY.....	12
Figura 18 - PuTTY SSH.....	13
Figura 19 - Regras WAN.....	13
Figura 20 - Regras LAN.....	14
Figura 21 - Regras DMZ.....	14
Figura 22 - Regras IPsec.....	14
Figura 23 - VPN IPsec – Fase 1 .....	15
Figura 24 - VPN IPsec - Fase 2 .....	16
Figura 25 - Ipsec Status .....	17
Figura 26 - Ping Rede Filial.....	17
Figura 27 - System Logs VPN .....	18
Figura 28 - Definições System Logs.....	19
Figura 29 - Zabbix.....	19
Figura 30 - System Logs no ZABBIX.....	20
Figura 31 - Snort Oinkcode.....	20
Figura 32 - Package Manager.....	21
Figura 33 - Definições Globais Snort.....	21
Figura 34 - Snort WAN Settings .....	22
Figura 35 - Política IDS .....	23
Figura 36 - Interfaces Snort.....	23
Figura 37 - Hosts bloqueados .....	24
Figura 38 - CA's.....	24
Figura 39 - Certificado web config.....	25
Figura 40 - Certificado Servidor .....	25
Figura 41 - Certificado Admin .....	25

## Introdução

Com este relatório, pretendemos esclarecer todos os detalhes da nossa abordagem ao 2º trabalho prático, proposto na disciplina de criptografia e segurança informática, relativo à implementação de políticas e técnicas de segurança de sistemas de comunicação, explicando todas as fases do desenvolvimento do trabalho, que foram executadas, conforme solicitado no enunciado que nos foi fornecido pelo professor da disciplina.

O programa de virtualização que escolhemos foi o VirtualBox. Nele instalamos a pfSense, na versão mais recente (2.4.4).

Também recorremos ao uso do programa PuTTY para testar o acesso remoto ao servidor por SSH e ao puTTYgen para gerar private e public keys.

Os sistemas operativos que usamos como clientes foram o Ubuntu Desktop 18.04.03 LTS Bionic, o Windows 7 Ultimate e o Ubuntu Server 18.04.03 LTS Bionic. Nesta última máquina instalamos o Zabbix 4.4 para servir como ferramenta de logging remoto.

## Instalação da pfSense

Após a criação da máquina virtual com a imagem ISO do sistema operativo pfSense na versão 2.4.4, instalamos o mesmo com as definições padrão. As definições de rede da máquina que utilizamos para os adaptadores foram uma bridged para a WAN e uma internal network para a LAN e outra para a DMZ. O adaptador de rede utilizado nas máquinas Windows e Ubuntu foi também a internal network “pfsense”. A finalidade era utilizar a bridged adapter para receber a ligação à internet do router e a fornecer à pfSense que por sua vez iria funcionar como uma firewall e enviar uma ligação à internet segura para a internal network.

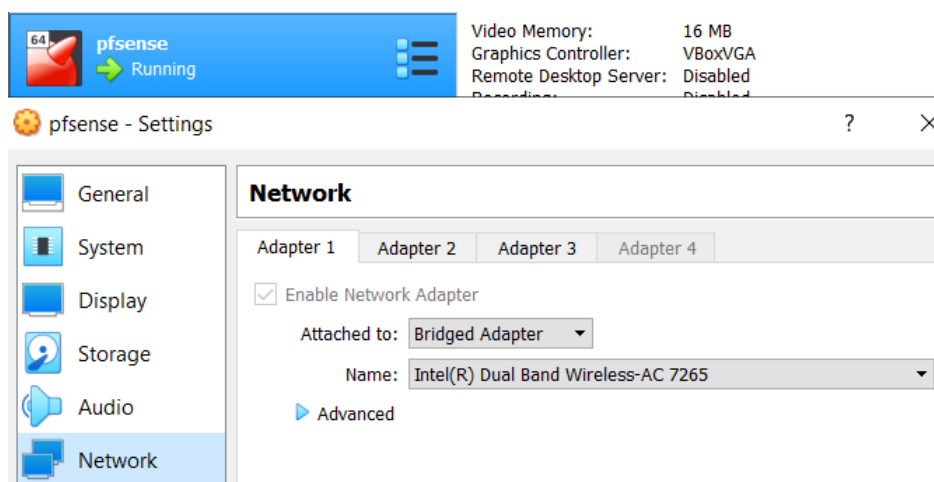


FIGURA 1 - MÁQUINA VIRTUAL

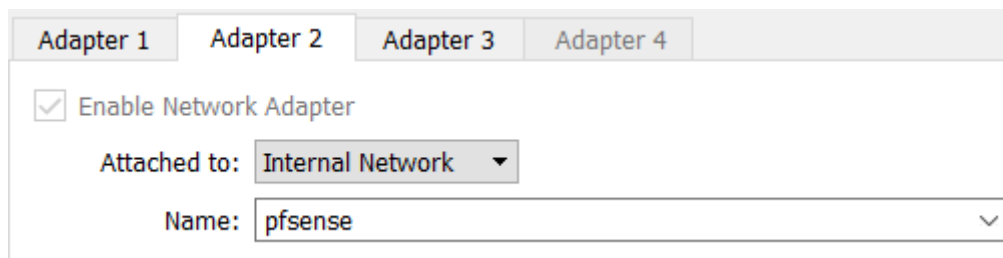


FIGURA 2 - MÁQUINA VIRTUAL – LAN

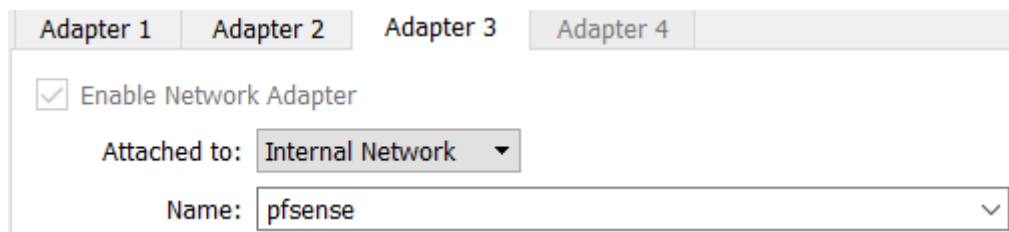
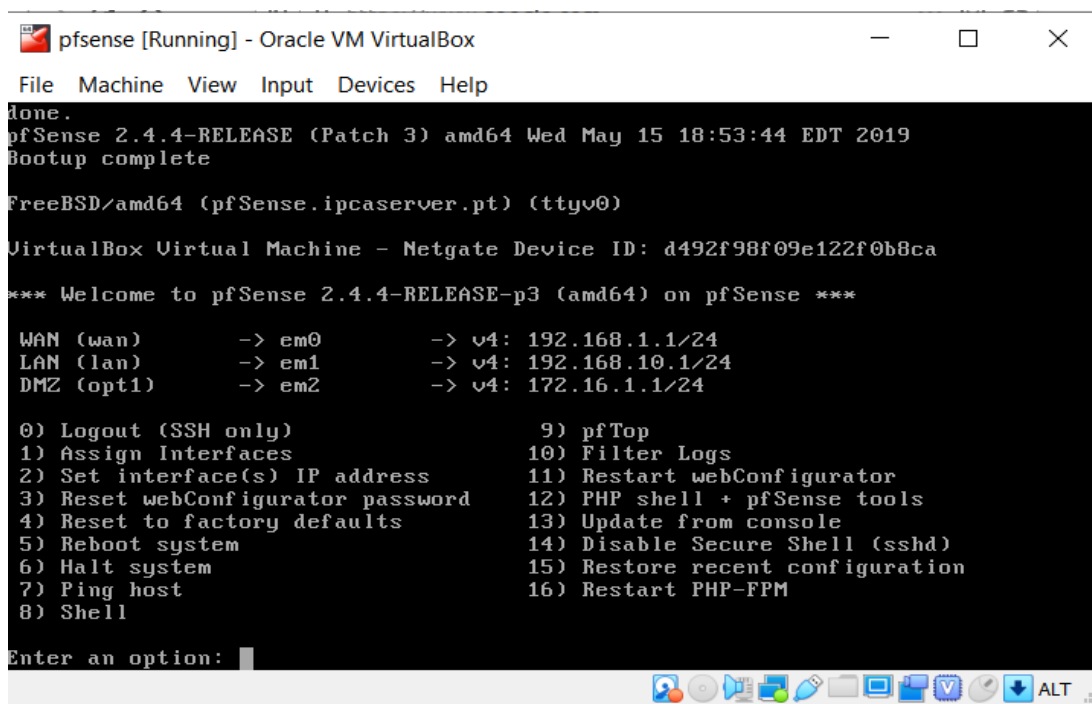


FIGURA 3 - MÁQUINA VIRTUAL – DMZ

## Criação e Configuração das Interfaces

Já com a pfSense aberta configuramos as interfaces como pedido, sendo que na consola apenas designamos os IP's da WAN e da LAN. No web config procedemos ao resto da configuração e atribuição da DMZ.



```
pfsense [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
done.
pfSense 2.4.4-RELEASE (Patch 3) amd64 Wed May 15 18:53:44 EDT 2019
Bootup complete

FreeBSD/amd64 (pfSense.ipcaserver.pt) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: d492f98f09e122f0b8ca

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

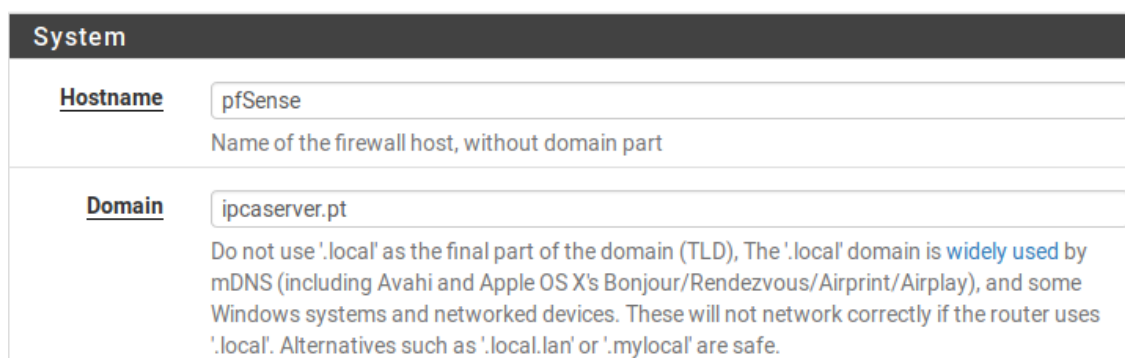
WAN (wan)      -> em0      -> v4: 192.168.1.1/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 172.16.1.1/24

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) Disable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

FIGURA 4 - CONSOLA PFSense

No setup inicial definimos o *hostname* e o *domain* da pfsense sendo que optamos por utilizar os servidores DNS do provedor. Também alteramos a password do admin no aviso que apareceu no cabeçalho.



System	
<b>Hostname</b>	<input type="text" value="pfSense"/> Name of the firewall host, without domain part
<b>Domain</b>	<input type="text" value="ipcaserver.pt"/> Do not use '.local' as the final part of the domain (TLD), The '.local' domain is widely used by mDNS (including Avahi and Apple OS X's Bonjour/Rendezvous/Airprint/Airplay), and some Windows systems and networked devices. These will not network correctly if the router uses '.local'. Alternatives such as '.local.lan' or '.mylocal' are safe.

FIGURA 5 - HOSTNAME E DOMAIN

Aqui ativamos a interface DMZ que estava desativada na configuração inicial (adaptador 3).

Interface	Network port
WAN	em0 (08:00:27:76:7e:9e)
LAN	em1 (08:00:27:47:c7:b1) <span>Delete</span>
DMZ	em2 (08:00:27:1a:34:7b) <span>Delete</span>

FIGURA 6 - INTERFACE ASSIGNMENTS

Na WAN deixamos a rede estática com a gateway 192.168.1.254 e desativamos as redes reservadas pois essa definição estava a bloquear a comunicação da WAN com a LAN.

**General Configuration**

**Enable** ☒ Enable interface

**Description** WAN  
Enter a description (name) for the interface here.

**IPv4 Configuration Type** Static IPv4

**IPv6 Configuration Type** None

**Static IPv4 Configuration**

**IPv4 Address** 192.168.1.1 / 24

**IPv4 Upstream gateway** WANGW - 192.168.1.254 + Add a new gateway

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.  
On local area network interfaces the upstream gateway should be "none". Gateways can be managed by [clicking here](#).

**Reserved Networks**

**Block private networks and loopback addresses** ☐  
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

**Block bogon networks** ☐  
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.  
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

FIGURA 7 - CONFIGURAÇÃO WAN

Na interface LAN utilizamos endereços estáticos mais uma vez sendo que de seguida configuramos o DHCP server para atribuir os IP's às máquinas que tentassem estabelecer uma ligação à rede.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>

FIGURA 8 - CONFIGURAÇÃO LAN

Na interface DMZ utilizamos o mesmo procedimento da interface LAN.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>

FIGURA 9 - CONFIGURAÇÃO DMZ



## DHCP Server

Ativamos o DHCP Server na interface LAN para atribuir endereços IP's automaticamente às máquinas que se ligassem à rede.

Definimos um range da rede desde o endereço 192.168.10.10 até ao 192.168.10.245 pela razão de no trabalho ser pedido permissões especiais para o IP 192.168.10.10, portanto achamos que devia ser o primeiro IP de rede de forma a facilitar a configuração.

General Options	
<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
<b>BOOTP</b>	<input type="checkbox"/> Ignore BOOTP queries
<b>Deny unknown clients</b>	<input type="checkbox"/> Only the clients defined below will get DHCP leases from this server.
<b>Ignore denied clients</b>	<input type="checkbox"/> Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
<b>Ignore client identifiers</b>	<input type="checkbox"/> If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.
<b>Subnet</b>	192.168.10.0
<b>Subnet mask</b>	255.255.255.0
<b>Available range</b>	192.168.10.1 - 192.168.10.254
<b>Range</b>	<div><div>192.168.10.10</div><div>192.168.10.245</div><div>FromTo</div></div>

FIGURA 10 - DHCP SERVER LAN

## Definições Avançadas do Sistema

Nas configurações avançadas do sistema ativamos o serviço HTTPS, criamos o certificado para o endereço da pfsense, ativamos a porta do web config para a 10443, desativamos o anti-lockout, por causa do túnel VPN que criamos e ativamos a o server da Secure Shell para permitir o acesso remoto por SSH.

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
SSL Certificate	<input type="text" value="ipcaserver.pt"/>
TCP port	<input type="text" value="10443"/>
Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.	

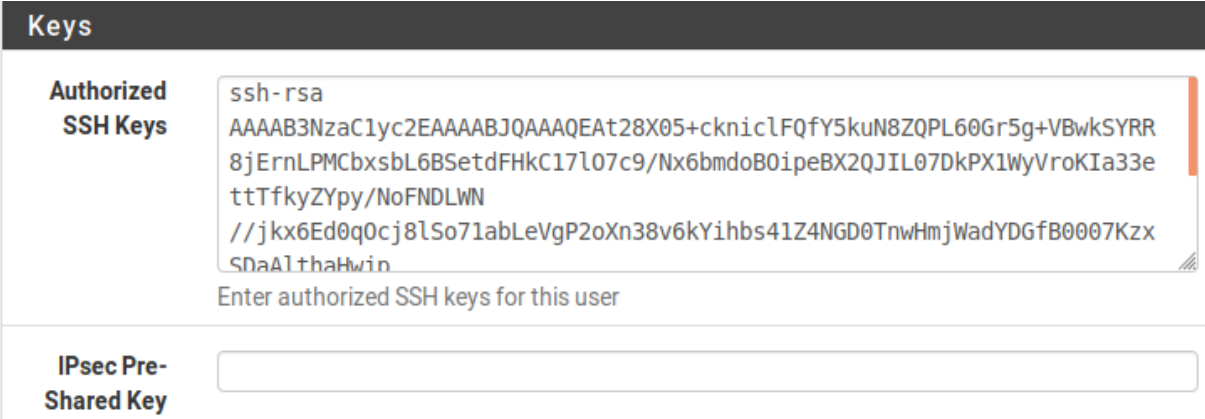
FIGURA 11 - DEFINIÇÕES AVANÇADAS DO SISTEMA 1

Anti-lockout	<input checked="" type="checkbox"/> Disable webConfigurator anti-lockout rule When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) <i>Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.</i>
Secure Shell	
Secure Shell Server	<input checked="" type="checkbox"/> Enable Secure Shell
SSHd Key Only	<input type="text" value="Public Key Only"/> When set to <i>Public Key Only</i> , SSH access requires authorized keys and these keys must be configured for each <b>user</b> that has been granted secure shell access. If set to <i>Require Both Password and Public Key</i> , the SSH daemon requires both authorized keys <b>and</b> valid passwords to gain access. The default <i>Password or Public Key</i> setting allows either a valid password or a valid authorized key to login.
Allow Agent Forwarding	<input type="checkbox"/> Enables ssh-agent forwarding support.
SSH port	<input type="text" value="22"/> Note: Leave this blank for the default of 22.

FIGURA 12 - DEFINIÇÕES AVANÇADAS DO SISTEMA 2

## User Manager

No user manager definimos a chave SSH do admin que lhe permite aceder remotamente à consola.



The screenshot shows the 'Keys' configuration page in User Manager. It has a dark header with the word 'Keys'. Below the header, there are two main sections. The first section is titled 'Authorized SSH Keys' and contains a text area with a long SSH public key. The key starts with 'ssh-rsa' and ends with 'SDaAlthaHwin'. Below the text area is a label 'Enter authorized SSH keys for this user'. The second section is titled 'IPsec Pre-Shared Key' and contains an empty text input field.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAt28X05+ckniclFQfY5kuN8ZQPL60Gr5g+VBwksYRR
8jErnLPMcbxsbl6BSetdFHkC17l07c9/Nx6bmdb0ipeBX2QJIL07DkPX1WyVroKIa33e
ttTfkyZYpy/NoFNDLWN
//jkx6Ed0q0cj8lSo71abLeVgP2oXn38v6kYihbs41Z4NGD0TnwHmjWadYDGfB0007Kzx
SDaAlthaHwin
```

Enter authorized SSH keys for this user

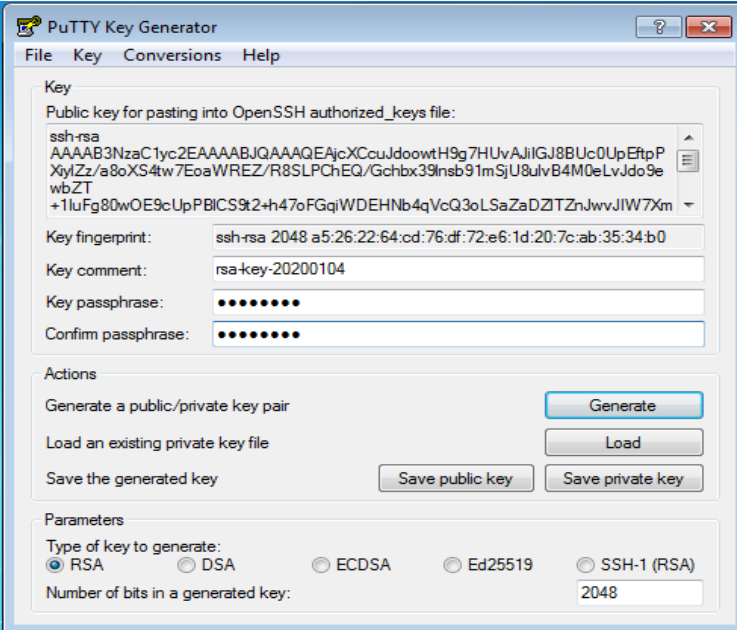
IPsec Pre-Shared Key

FIGURA 13 - USER MANAGER

## Funcionalidades SSH

Para criar as chaves públicas e privadas recorreremos ao PuTTY Gen. Nele recorreremos ao uso de uma passphrase, que é a mesma chave do admin no pfsense, para confirmar se é o admin que está a usar a chave, que tem encriptação RSA de 2048 bites.

Depois disso gravamos a public key num .txt e utilizamos a mesma como chave autorizada do admin no pfsense como mostramos anteriormente e gravamos a private key para utilizar no acesso remoto do PuTTY.



The screenshot shows the PuTTY Key Generator window. It has a menu bar with 'File', 'Key', 'Conversions', and 'Help'. The 'Key' tab is selected. The 'Key' section contains a text area for the public key, a 'Key fingerprint' field showing 'ssh-rsa 2048 a5:26:22:64:cd:76:df:72:e6:1d:20:7c:ab:35:34:b0', a 'Key comment' field with 'rsa-key-20200104', and two password fields for 'Key passphrase' and 'Confirm passphrase'. The 'Actions' section has buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section has radio buttons for 'Type of key to generate' (RSA, DSA, ECDSA, Ed25519, SSH-1 (RSA)) and a 'Number of bits in a generated key' field set to '2048'.

FIGURA 14 - PUTTY GEN

Na prática, para acedermos à pfsense no PuTTY, abrimos a private key (inicia processo em segundo plano), introduzimos a passphrase e depois inserimos o ip a que queríamos aceder no PuTTY.

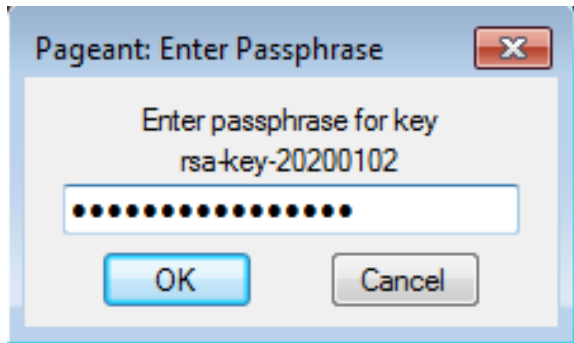


FIGURA 15 - PASSPHRASE



FIGURA 16 - PROCESSO INICIADO EM SEGUNDO PLANO

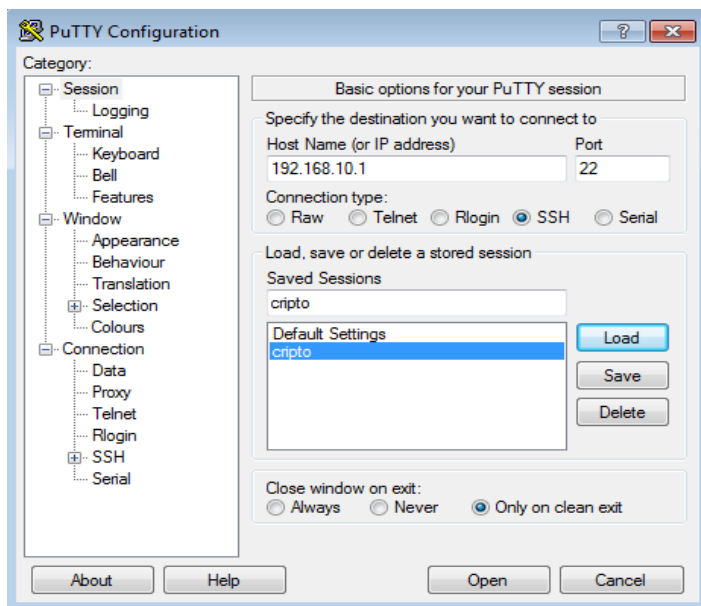
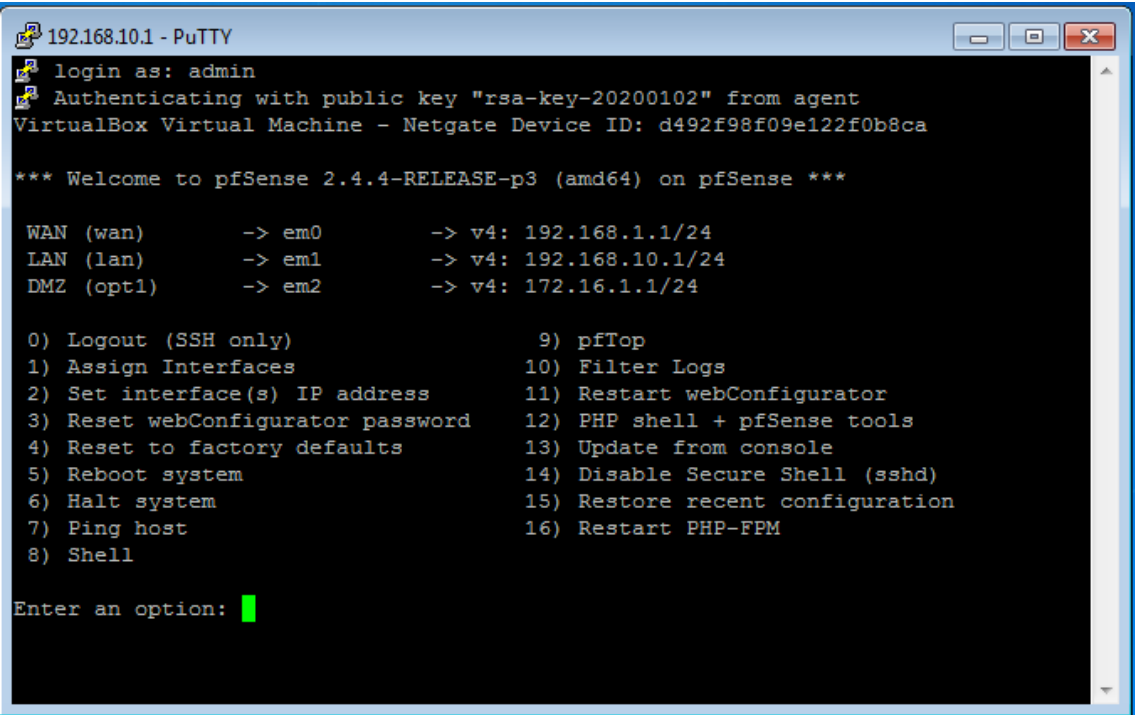


FIGURA 17 - CONFIGURAÇÃO PUTTY

Depois deste procedimento o acesso à consola do pfsense fica estabelecido após a introdução do login.



```
192.168.10.1 - PuTTY
login as: admin
Authenticating with public key "rsa-key-20200102" from agent
VirtualBox Virtual Machine - Netgate Device ID: d492f98f09e122f0b8ca

*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.1.1/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
DMZ (opt1)     -> em2      -> v4: 172.16.1.1/24

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) Disable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```

FIGURA 18 - PuTTY SSH

## Regras de Firewall

Aqui criamos diversas regras para permitir a comunicação entre as redes.

Na WAN criamos as regras que nos foram pedidas no enunciado para permitir a ligação VPN do túnel e permissão do protocolo ICMP de qualquer fonte para qualquer destino para permitir-nos utilizar o comando ping para testar conectividade.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	*	*	none		ICMP any	
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	4500	*	none		(IPsec NAT-T)	
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	500	*	none		(ISAKMP)	
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	*	*	none		AH	
<input type="checkbox"/>	✓	0/0 B	IPv4	*	*	*	*	none		ESP	

FIGURA 19 - REGRAS WAN

Na LAN para além das regras por defeito acrescentamos as que nos foram pedidas. Uma para permitir ao cliente com o IP 192.168.10.10 o acesso na porta 22 do SSH e na outra utilizamos um invert match para permitir apenas ao utilizador com o ip 192.168.10.10 o acesso ao web config.





















Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.10	*	*	22 (SSH)	*	none			<div></div>
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	! 192.168.10.10	*	This Firewall	10443	*	none		Block Access to Web Config	<div></div>
<input type="checkbox"/>	✓ 1 /4.77 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	<div></div>
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<div></div>

FIGURA 20 - REGRAS LAN

Na DMZ apenas criamos a regra pedida para permitir apenas acesso dos clientes ao servidor web.





Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	✗	0/0 B	IPv4 TCP	!	192.168.10.1/24	*	DMZ address	*	*	none	<div></div>	

FIGURA 21 - REGRAS DMZ

Mais à frente criamos uma regra do IPsec para permitir a comunicação entre a rede da filial com a rede da sede.

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action	
<input type="checkbox"/>	✓	1 / 28 KiB	IPv4 *	192.168.20.1/24	*	192.168.10.1/24	*	*	none		<div><div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div></div></div></div>	

FIGURA 22 - REGRAS IPSEC

## VPN IPsec – Fase 1

Começamos por adicionar um túnel e o configurar com as definições pedidas no enunciado e adicionamos a remote gateway da rede da filial.

<b>Key Exchange version</b>	Auto	Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.		
<b>Internet Protocol</b>	IPv4	Select the Internet Protocol family.		
<b>Interface</b>	WAN	Select the interface for the local endpoint of this phase1 entry.		
<b>Remote Gateway</b>	192.168.1.2	Enter the public IP address or host name of the remote gateway.		
<b>Description</b>				
A description may be entered here for administrative reference (not parsed).				
<b>Phase 1 Proposal (Authentication)</b>				
<b>Authentication Method</b>	Mutual PSK	Must match the setting chosen on the remote side.		
<b>Negotiation mode</b>	Aggressive	Aggressive is more flexible, but less secure.		
<b>My identifier</b>	My IP address			
<b>Peer identifier</b>	Peer IP address			
<b>Pre-Shared Key</b>	#\$ipca\$#			
Enter the Pre-Shared Key string. This key must match on both peers.				
<b>Phase 1 Proposal (Encryption Algorithm)</b>				
<b>Encryption Algorithm</b>	3DES	SHA1	2 (1024 bit)	Delete
	Algorithm	Key length	Hash	DH Group
Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.				
<b>Add Algorithm</b>	+ Add Algorithm			
<b>Lifetime (Seconds)</b>	28800			

FIGURA 23 - VPN IPSEC – FASE 1

## VPN IPsec – Fase 2

Aqui introduzimos o endereço da rede LAN da sede como rede local e o endereço da rede LAN da filial como rede remota. Nos algoritmos utilizamos os que foram pedidos para este trabalho.

<b>Mode</b>	Tunnel IPv4		
<b>Local Network</b>	Network	192.168.10.1	/ 24
	Type	Address	
	Local network component of this IPsec security association.		
<b>NAT/BINAT translation</b>	None		/ 0
	Type	Address	
	If NAT/BINAT is required on this network specify the address to be translated		
<b>Remote Network</b>	Network	192.168.20.1	/ 24
	Type	Address	
	Remote network component of this IPsec security association.		
<b>Description</b>	Túnel sede por filial		
	A description may be entered here for administrative reference (not parsed).		
<b>Phase 2 Proposal (SA/Key Exchange)</b>			
<b>Protocol</b>	ESP		
	Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.		
<b>Encryption Algorithms</b>	<input checked="" type="checkbox"/> AES	128 bits	
	<input type="checkbox"/> AES128-GCM	Auto	
	<input type="checkbox"/> AES192-GCM	Auto	
	<input type="checkbox"/> AES256-GCM	Auto	
	<input type="checkbox"/> Blowfish	Auto	
	<input checked="" type="checkbox"/> 3DES		
<b>Hash Algorithms</b>	<input checked="" type="checkbox"/> MD5 <input checked="" type="checkbox"/> SHA1 <input type="checkbox"/> SHA256 <input type="checkbox"/> SHA384 <input type="checkbox"/> SHA512 <input type="checkbox"/> AES-XCBC		
	Note: MD5 and SHA1 provide weak security and should be avoided.		
<b>PFS key group</b>	2 (1024 bit)		
	Note: Groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.		
<b>Lifetime</b>	3600		
	Specifies how often the connection must be rekeyed, in seconds		

FIGURA 24 - VPN IPSEC - FASE 2



Após esta configuração o túnel foi estabelecido e comprovamos que as redes estão a comunicar uma com a outra.

IPsec Status									
IPsec ID	Description	Local ID	Local IP	Remote ID	Remote IP	Role	Reauth	Algo	Status
con1000: #10		192.168.1.1	192.168.1.1	192.168.1.2	192.168.1.2	IKEv2 initiator	23408 seconds (06:30:08)	3DES_CBC HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	ESTABLISHED 4302 seconds (01:11:42) ago <div>Disconnect</div>
<div>Show child SA entries</div>									

FIGURA 25 - IPSEC STATUS

Ping

Hostname

192.168.1.2

IP Protocol

IPv4

Source address

WAN

Select source address for the ping.

Maximum number of pings

3

Select the maximum number of pings.

Ping

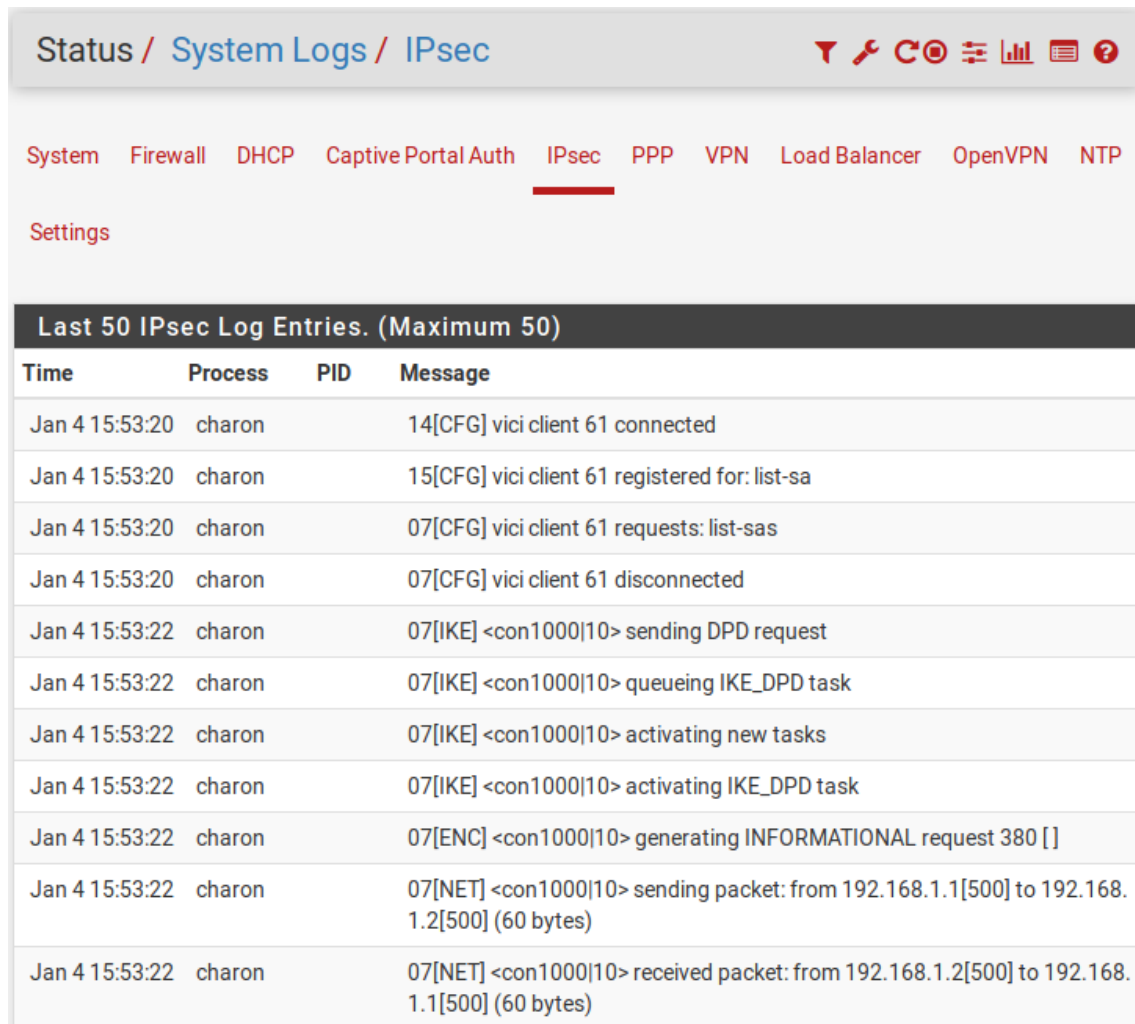
Results

PING 192.168.1.2 (192.168.1.2) from 192.168.1.1: 56 data bytes  
64 bytes from 192.168.1.2: icmp\_seq=0 ttl=64 time=0.366 ms  
64 bytes from 192.168.1.2: icmp\_seq=1 ttl=64 time=0.728 ms  
64 bytes from 192.168.1.2: icmp\_seq=2 ttl=64 time=0.702 ms  
  
--- 192.168.1.2 ping statistics ---  
3 packets transmitted, 3 packets received, 0.0% packet loss  
round-trip min/avg/max/stddev = 0.366/0.599/0.728/0.165 ms

FIGURA 26 - PING REDE FILIAL

## System Logs

O system logs foi uma das áreas mais importantes para este trabalho. Aqui verificamos as ligações que a firewall recusava para conseguirmos retificar as regras para conseguir estabelecer as ligações e os acessos estabelecidos pelo serviço VPN.



The screenshot shows the Mikrotik WinBox interface with the 'System Logs / IPsec' path selected. The 'IPsec' tab is active in the top navigation bar. Below the navigation bar, there is a section titled 'Last 50 IPsec Log Entries. (Maximum 50)' containing a table of log entries.

Time	Process	PID	Message
Jan 4 15:53:20	charon		14[CFG] vici client 61 connected
Jan 4 15:53:20	charon		15[CFG] vici client 61 registered for: list-sa
Jan 4 15:53:20	charon		07[CFG] vici client 61 requests: list-sas
Jan 4 15:53:20	charon		07[CFG] vici client 61 disconnected
Jan 4 15:53:22	charon		07[IKE] <con1000 10> sending DPD request
Jan 4 15:53:22	charon		07[IKE] <con1000 10> queueing IKE_DPD task
Jan 4 15:53:22	charon		07[IKE] <con1000 10> activating new tasks
Jan 4 15:53:22	charon		07[IKE] <con1000 10> activating IKE_DPD task
Jan 4 15:53:22	charon		07[ENC] <con1000 10> generating INFORMATIONAL request 380 []
Jan 4 15:53:22	charon		07[NET] <con1000 10> sending packet: from 192.168.1.1[500] to 192.168.1.2[500] (60 bytes)
Jan 4 15:53:22	charon		07[NET] <con1000 10> received packet: from 192.168.1.2[500] to 192.168.1.1[500] (60 bytes)

FIGURA 27 - SYSTEM LOGS VPN

Para acedermos ao logging remoto criamos a máquina Ubuntu Server com a ferramenta de monitoramento ZABBIX. Após terminarmos a configuração do ZABBIX ligamos o mesmo à rede da filial, onde devíamos receber os logs da pfsense da sede. Para conseguirmos receber no ZABBIX os logs, definimos nas definições do system logs da sede que devia enviar todos logs para o ip remoto 192.168.20.3 (IP do ZABBIX).

<b>Enable Remote Logging</b>	<input checked="" type="checkbox"/> Send log messages to remote syslog server
<b>Source Address</b>	<div>LAN</div> <p>This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.</p> <p>NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.</p>
<b>IP Protocol</b>	<div>IPv4</div> <p>This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.</p>
<b>Remote log servers</b>	<div>192.168.20.3</div> <div>IP[:port]</div> <div>IP[:port]</div>
<b>Remote Syslog Contents</b>	<input checked="" type="checkbox"/> Everything <input type="checkbox"/> System Events <input type="checkbox"/> Firewall Events

**FIGURA 28 - DEFINIÇÕES SYSTEM LOGS**

Já no ZABBIX, verificamos que os logs do pfsense da sede estavam a ser recebidos.

```

Ubuntu 18.04.3 LTS ipcasrv tty1

ipcasrv login: ipca
Password:
Last login: Sat Jan  4 16:09:16 UTC 2020 on tty1
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jan  4 16:12:17 UTC 2020

System load:  0.14               Processes:    139
Usage of /:   17.0% of 36.61GB   Users logged in:  0
Memory usage: 28%               IP address for enp0s3: 192.168.20.3
Swap usage:   0%

111 packages can be updated.
61 updates are security updates.

ipca@ipcasrv:~$ cd /etc
ipca@ipcasrv:/etc$ cd /var/log
ipca@ipcasrv:/var/log$ ls
alternatives.log  bootstrap.log      dist-upgrade      journal           lxd               unattended-upgrades
apache2           btmp               dpkg.log          kern.log          mysql             wtmp
apt               cloud-init.log     faillog           landscape         syslog            zabbix
auth.log          cloud-init-output.log installer          lastlog          tallylog
ipca@ipcasrv:/var/log$ tail -f syslog

```

**FIGURA 29 - ZABBIX**

```

Jan  4 16:14:39 192.168.10.1 charon: 11[ENC] <con1000|10> parsed INFORMATIONAL response 508 [ ]
Jan  4 16:14:39 192.168.10.1 charon: 11[IKE] <con1000|10> activating new tasks
Jan  4 16:14:39 192.168.10.1 charon: 11[IKE] <con1000|10> nothing to initiate
Jan  4 16:14:39 192.168.10.1 charon: 08[CFG] vici client 315 connected
Jan  4 16:14:39 192.168.10.1 charon: 11[CFG] vici client 315 registered for: list-sa
Jan  4 16:14:39 192.168.10.1 charon: 11[CFG] vici client 315 requests: list-sas
Jan  4 16:14:39 192.168.10.1 charon: 11[CFG] vici client 315 disconnected
Jan  4 16:14:39 pfsense.ipcaserver.pt nginx: 192.168.10.10 - - [04/Jan/2020:16:14:39 +0000] "POST /s
tatus_ipsec.php HTTP/2.0" 200 818 "https://192.168.10.1:10443/status_ipsec.php" "Mozilla/5.0 (X11; U
buntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0"
Jan  4 16:14:44 192.168.10.1 charon: 08[CFG] vici client 316 connected
Jan  4 16:14:44 192.168.10.1 charon: 11[CFG] vici client 316 registered for: list-sa
Jan  4 16:14:44 192.168.10.1 charon: 05[CFG] vici client 316 requests: list-sas
Jan  4 16:14:44 192.168.10.1 charon: 05[CFG] vici client 316 disconnected
Jan  4 16:14:44 pfsense.ipcaserver.pt nginx: 192.168.10.10 - - [04/Jan/2020:16:14:44 +0000] "POST /s
tatus_ipsec.php HTTP/2.0" 200 818 "https://192.168.10.1:10443/status_ipsec.php" "Mozilla/5.0 (X11; U
buntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0"
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> sending DPD request
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> queueing IKE_DPD task
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> activating new tasks
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> activating IKE_DPD task
Jan  4 16:14:49 192.168.10.1 charon: 05[ENC] <con1000|10> generating INFORMATIONAL request 509 [ ]
Jan  4 16:14:49 192.168.10.1 charon: 05[NET] <con1000|10> sending packet: from 192.168.1.1[500] to 1
92.168.1.2[500] (60 bytes)
Jan  4 16:14:49 192.168.10.1 charon: 05[NET] <con1000|10> received packet: from 192.168.1.2[500] to
192.168.1.1[500] (60 bytes)
Jan  4 16:14:49 192.168.10.1 charon: 05[ENC] <con1000|10> parsed INFORMATIONAL response 509 [ ]
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> activating new tasks
Jan  4 16:14:49 192.168.10.1 charon: 05[IKE] <con1000|10> nothing to initiate
Jan  4 16:14:49 192.168.10.1 charon: 07[CFG] vici client 317 connected
Jan  4 16:14:49 192.168.10.1 charon: 08[CFG] vici client 317 registered for: list-sa
Jan  4 16:14:49 192.168.10.1 charon: 05[CFG] vici client 317 requests: list-sas
Jan  4 16:14:49 192.168.10.1 charon: 05[CFG] vici client 317 disconnected
Jan  4 16:14:49 pfsense.ipcaserver.pt nginx: 192.168.10.10 - - [04/Jan/2020:16:14:49 +0000] "POST /s
tatus_ipsec.php HTTP/2.0" 200 818 "https://192.168.10.1:10443/status_ipsec.php" "Mozilla/5.0 (X11; U
buntu; Linux x86_64; rv:70.0) Gecko/20100101 Firefox/70.0"

```

**FIGURA 30 - SYSTEM LOGS NO ZABBIX**

## Snort

Para procedermos à configuração do snort entramos no seu website e registamos um utilizador. Depois copiamos o nosso oinkcode para ativarmos o snort na nossa pfsense.

a16984@alunos.ipca.pt

- Account
- Oinkcode**
- Subscription
- Receipts
- False Positive

Oinkcode

3c62e7309528d31c6106bf540615f439a12f7d58

Regenerate

**FIGURA 31 - SNORT OINKCODE**

Agora que já tínhamos o oinkcode, precisávamos de instalar o snort no pfsense, para isso recorreremos ao package Manager.

Installed Packages

Available Packages

Installed Packages

Name	Category	Version	Description	Actions
<div>✓</div> <div>snort</div>	security	3.2.9.10	<div> <div> Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. </div> <div> <div>Package Dependencies:</div> <div> <div> <div>🔗</div> <div>snort-2.9.15</div> </div> <div> <div>🔗</div> <div>barnyard2-1.13_1</div> </div> </div> </div> </div>	<div> <div>🗑️</div> <div>↺</div> <div>📘</div> </div>

FIGURA 32 - PACKAGE MANAGER

O snort ficou ativo então podemos agora configurá-lo. Nas definições globais introduzimos o nosso oinkcode e ativamos o download de todos os serviços do snort.

Snort Subscriber Rules	
Enable Snort VRT	<input checked="" type="checkbox"/> Click to enable download of Snort free Registered User or paid Subscriber rules
<a href="#">Sign Up for a free Registered User Rules Account</a> <a href="#">Sign Up for paid Snort Subscriber Rule Set (by Talos)</a>	
Snort Oinkmaster Code	<input type="text" value="3c62e7309528d31c6106bf540615f439a12f7d58"/> Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)
Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.	
Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
<a href="#">Sign Up for an ETPro Account</a> ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> Click to enable download of Sourcefire OpenAppID Detectors

FIGURA 33 - DEFINIÇÕES GLOBAIS SNORT

Depois ativamos o snort na WAN, LAN e na DMZ, sempre com as mesmas definições nas três interfaces.

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

WAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG\_AUTH

Select system log Facility to use for reporting. Default is LOG\_AUTH.

System Log Priority

LOG\_ALERT

Select system log Priority (Level) to use for reporting. Default is LOG\_ALERT.

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert

Kill States

☒ Checking this option will kill firewall states for the blocked IP. Default is checked.

Which IP to Block

BOTH

Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search

AC-BNFA

FIGURA 34 - SNORT WAN SETTINGS

Na política IDS definimos uma política do nível “Security” para mantermos a segurança na nossa rede e selecionamos todos as regras do snort.

Snort Subscriber IPS Policy Selection

Use IPS Policy

☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Security

Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.

Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files

- Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Save

Enable

Ruleset: Snort GPLv2 Community Rules

☒

Snort GPLv2 Community Rules (Talos certified)

Enable

Ruleset: Snort Text Rules

Enable

Ruleset: Snort SO Rules

Snort OPENAF rules are not enabled

☒

emerging-activex.rules

☐

snort\_app-detect.rules

☐

snort\_browser-chrome.so.rules

FIGURA 35 - POLÍTICA IDS

Depois disso a snort estava configurada e, portanto, ativamos com sucesso a mesma nas interfaces.

Interface Settings Overview						
Interface	Snort Status	Pattern Match	Blocking	Barnyard2 Status	Description	Actions
<input type="checkbox"/> WAN (em0)		AC-BNFA	ENABLED	DISABLED	WAN	
<input type="checkbox"/> LAN (em1)		AC-BNFA	ENABLED	DISABLED	LAN	
<input type="checkbox"/> DMZ (em2)		AC-BNFA	ENABLED	DISABLED	DMZ	

FIGURA 36 - INTERFACES SNORT

Com a ativação do snort verificamos que o mesmo estava a bloquear a ligação IPsec que tínhamos criado entre a rede da sede e a da filial, portanto no separador “Blocked” do snort removemos esse bloqueio.

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP Lists

SID MgmtLog MgmtSync

Blocked Hosts and Log View Settings

Blocked Hosts

Download

Clear

All blocked hosts will be saved

All blocked hosts will be removed

Refresh and Log View

Save

Refresh

500

Save auto-refresh and view settings

Default is ON

Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Snort

#	IP	Alert Descriptions and Event Times	Remove
There are currently no hosts being blocked by Snort.			

FIGURA 37 - HOSTS BLOQUEADOS

Certificados

Para criarmos um certificado auto assinado para o endereço da pfsense recorremos ao *Certificate Manager*. Primeiro criamos o CA auto assinado e depois criamos um CA root.









Certificate Authorities						
Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
IPCA root CA	✓	self-signed	3	ST=Braga, O=IPCA, L=Barcelos, CN=internal-ca, C=PT Valid From: Thu, 02 Jan 2020 21:40:28 +0000 Valid Until: Sun, 30 Dec 2029 21:40:28 +0000		   
IPCA sub CA	✓	IPCA root CA	0	ST=Braga, O=IPCA, L=Barcelos, CN=IPCA sub CA, C=PT Valid From: Thu, 02 Jan 2020 21:43:12 +0000 Valid Until: Sun, 30 Dec 2029 21:43:12 +0000		   

FIGURA 38 - CA's



Com o CA criado pudemos então criar um certificado para o nosso web configurator.

ipcaserver.pt	IPCA	ST=Braga, O=IPCA, L=Barcelos,	webConfigurator
Server Certificate	root CA	CN=ipcaserver.pt, C=PT	
CA: No			
Server: Yes		Valid From: Thu, 02 Jan 2020 22:27:53	
		+0000	
		Valid Until: Sun, 30 Dec 2029 22:27:53	
		+0000	

FIGURA 39 - CERTIFICADO WEB CONFIG

Os certificados ficaram então ativados no web config como mostramos abaixo.

**Hierarquia do certificado**

ipcaserver.pt

**Campos do certificado**

- ipcaserver.pt
  - Certificado
    - Versão
    - Número de série
    - Algoritmo da assinatura do certificado
    - Emissor**
    - Validade
      - Não antes de
      - Não depois de

**Valor do campo**

O = IPCA  
L = Barcelos  
ST = Braga  
C = PT  
CN = internal-ca

FIGURA 40 - CERTIFICADO SERVIDOR

Criamos também um certificado para o utilizador admin com recurso à CA “Ipca root CA”.



User Certificates		
Name	CA	
admin	IPCA root CA	
 Add		

FIGURA 41 - CERTIFICADO ADMIN

## Conclusão

Com a aprendizagem teórica que adquirimos nas aulas da disciplina que nos foram disponibilizadas, conseguimos ter uma percepção do que alguns componentes da pfsense deveriam fazer e também conhecíamos os protocolos e as suas portas, e assim, com a realização deste trabalho e consequente consolidação dos conhecimentos obtidos, conseguimos provar ter os saberes requeridos para a resolução deste trabalho e terminar quase as tarefas que nos foram propostas.

Consideramos que foi uma atividade extremamente enriquecedora, porque com a sua execução conseguimos simular uma firewall e perceber como são fornecidos os serviços de internet aos clientes. Também aprendemos a criar túneis VPN e assim percebemos como funcionam as VPN's na prática. Já todos utilizamos VPN's, mas nunca tínhamos pensado como seriam programados estes serviços e por essa razão damos esta importância a este trabalho.

Foi extremamente trabalhoso ao início, até nos habituarmos à plataforma da pfsense e tivemos alguns problemas com o DNS, mas conseguimos resolver o problema, que se encontrava nas gateways estarem mal configuradas e, portanto, o tráfego da internet não chegava aos clientes.