



ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

LICENCIATURA EM SEGURANÇA INFORMÁTICA EM REDES DE COMPUTADORES

SEGURANÇA DE REDES

Trabalho Prático II

Realizado por:
Francisco Sousa N°8200397

Conteúdo

1.	Cenário	3
2.	Configuração	4
	Passos da configuração seguindo as guidelines da introdução:	4
	Configuração das regras na Firewall:	4
	WAN:	4
	LAN:	5
3.	Demonstração	6
	Lista de todas as regras implementadas	6
	WAN:	6
	LAN:	6
	Demonstrar que as políticas implementadas estão de facto a funcionar	7
	Provar o acesso TELNET da rede interna para uma máquina da rede externa e da internet:	7
	Provar o acesso FTP da rede interna para uma máquina da rede externa e da internet:	7
	Provar O PING da rede interna para uma máquina da rede externa e da internet:	8
	Provar o acesso HTTP E HTTPS da rede interna para uma máquina da rede externa e da internet:	8
	Provar o bloqueio TELNET da rede externa para uma máquina da rede interna:	8
	Provar o bloqueio FTP da rede externa para uma máquina da rede interna:	9
	Provar o bloqueio ICMP (PING) da rede externa para uma máquina da rede interna:	9
	Provar o acesso HTTP da rede externa para uma máquina da rede interna:	9
	Identificar os protocolos inseguros e propor alterações às tabelas de regras de firewall listadas na introdução	9
	Protocolos inseguros:	9
	A alteração que eu proponha seria alterar de:	9
4.	IPS/IDS	10
	Instalação do Snort:	10
	Analisar as assinaturas existentes. Mostrar evidencia.	10
	Configurar alerta para tráfego ICMP (pings) do exterior (host).	11
	Verificar nos logs o registo do alerta do ponto anterior.	11
	Configurar para barrar o tráfego anterior.	12
	Configurar alerta para detectar login de um utilizador root em ftp (serviço a instalar num dos servidores do cenário). Demonstrar.	13
	Configurar alerta para acesso a uma página com referência á palavra “Adult”. Origem nas máquinas internas. Demonstração dessa configuração.	13
5.	VPN	15
	Demonstrar as configurações, a subnet usada e os utilizadores criados.	15
	Criar acesso do host para o servidor de FTP.	15
	Altere as regras da firewall de modo a permitir tráfego. Demonstrar.	16

1. Cenário

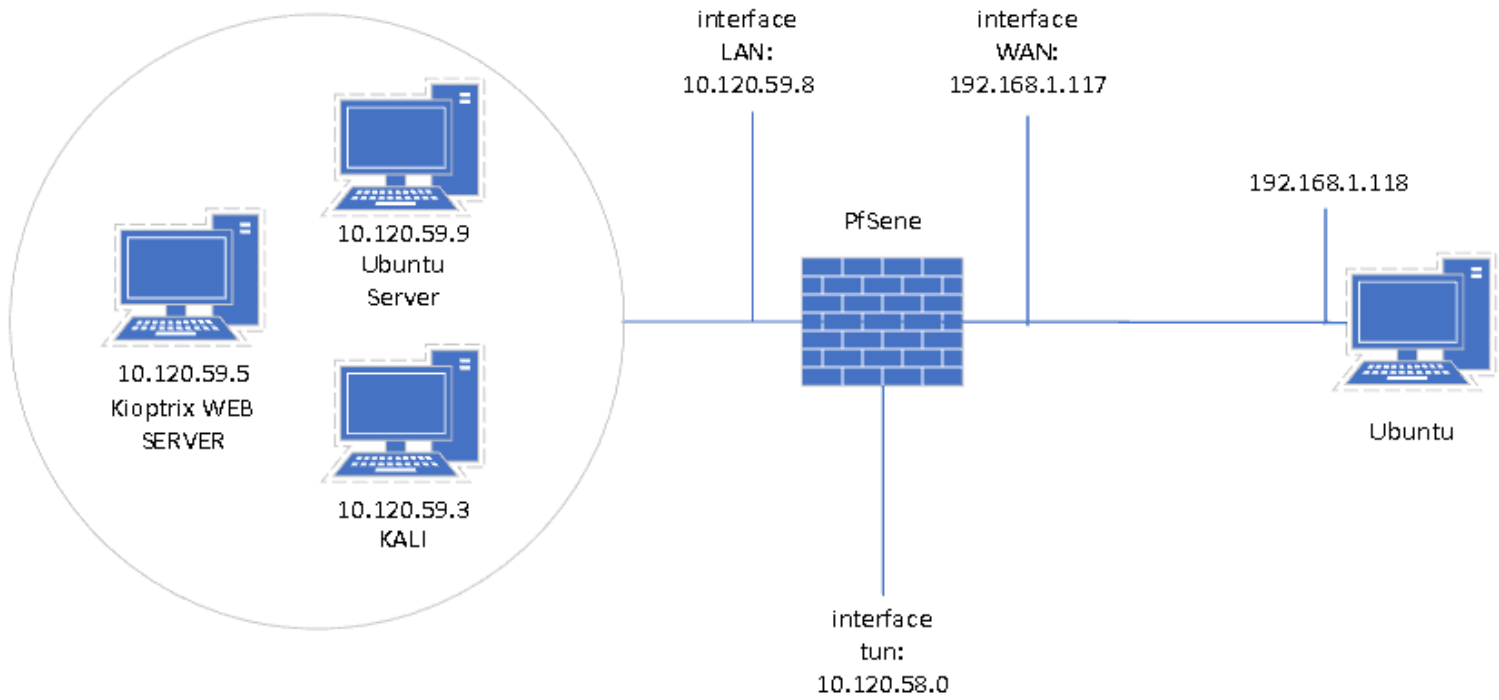


Figura 1- Cenário.

2. Configuração

Passos da configuração seguindo as guidelines da introdução:

Na interface WAN acabei por retirar as políticas default, e na LAN removi a regra relativa ao ipv6 e na regra de permitir tudo mudei para negar tudo.

Vou ter de criar regras novas tanto na interface WAN como na LAN.

Esta firewall tem como objetivo permitir que os seguintes protocolos, telnet, FTP, Ping (ICMP), devam conseguir sair da rede interna para a internet, mas não passar da internet para a rede interna. Os protocolos WEB (http e https) devem conseguir chegar da rede interna à internet e chegar da internet à rede interna. O protocolo Email só deve conseguir chegar da internet à rede interna.

Regras:

TELNET: rede interna → internet deixa passar | rede interna ← internet não deixa passar

FTP: rede interna → internet deixa passar | rede interna ← internet não deixa passar

PING: rede interna → internet deixa passar | rede interna ← internet não deixa passar

WEB: rede interna → internet deixa passar | rede interna ← internet deixa passar

EMAIL: rede interna → internet não deixa passar | rede interna ← internet deixa passar

Depois de analisar bem o esquema e o objetivo da firewall, para tornar esta mais segura, como disse em cima coloquei uma regra em cada interface a bloquear qualquer tráfego, sendo assim as regras de bloqueio poderão ser todas omitidas. Cheguei a conclusão também que se eu quero negar ou permitir tráfego vindo da internet para a rede interna devo o fazer na interface mais perto da internet (WAN) para garantir mais segurança, e vice versa se quiser negar ou permitir tráfego da rede interna para a internet devo o fazer na interface mais perto da rede interna (LAN).

Para verificar se estas regras estão corretas irei realizar testes às mesmas, como por exemplo realizar pings entre as máquinas.

Configuração das regras na Firewall:

WAN:

Como tinha dito anteriormente na WAN as regras default foram apagadas e colocada a seguinte regra:

DENY ALL TRAFFIC										
<input type="checkbox"/>		0 / 0 B	IPv4 *	*	*	*	*	none	Deny ALL	

Esta regra permite bloquear todo o tráfego com origem any para um destino any (bloqueia tudo).

As seguintes regras são para deixar passar tráfego tcp das portas 80 e 443, http e https, com origem any e destino o nosso servidor web na rede interna.

ALLOW RULES											
<input type="checkbox"/>		0 / 33 KiB	IPv4 TCP	*	*	10.120.59.5	80 (HTTP)	*	none	WAN Allow HTTP	
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	*	*	10.120.59.5	443 (HTTPS)	*	none	WAN Allow HTTPS	








LAN:

Como tinha dito anteriormente na LAN as regras default uma delas foi mudada e outra removida:

DENY ALL TRAFFIC											
<input type="checkbox"/>		0 / 0 B	IPv4 *	LAN net	*	*	*	*	none	Default Block LAN to any rule	

A relativa a ipv6 foi removida e a relativa ao ipv4 em vez de permitir todo o tráfego, bloqueia.

- Regra para permitir tráfego TCP da porta 23 (TELNET), com origem na rede interna e destino any (neste caso vai ser a internet).

ALLOW RULES											
<input type="checkbox"/>		0 / 2 KiB	IPv4 TCP	LAN net	*	*	23 (Telnet)	*	none	LAN Allow Telnet	    

- Regra para permitir tráfego TCP da porta 21 (FTP), com origem na rede interna e destino any (neste caso vai ser a internet).

<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	21 (FTP)	*	none	LAN Allow FTP	
--------------------------	--	---------	----------	---------	---	---	----------	---	------	---------------	--

- Regra para permitir tráfego ICMP (PING), com origem na rede interna e destino any (neste caso vai ser a internet).

<input type="checkbox"/>		0 / 0 B	IPv4 ICMP	LAN net	*	*	*	*	none	LAN Allow ICMP	
--------------------------	--	---------	-----------	---------	---	---	---	---	------	----------------	--

- Regra para permitir tráfego TCP/UDP da porta 53 (DNS), com origem na rede interna e destino any (neste caso vai ser a internet).

<input type="checkbox"/>		0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		
--------------------------	--	---------	--------------	---------	---	---	----------	---	------	--	--





















- Regras para permitir tráfego TCP das portas 80 e 443 (HTTP E HTTPS), com origem na rede interna e destino any (neste caso vai ser a internet).

<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	LAN Allow HTTP	
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none	LAN Allow HTTPS	













































3. Demonstração

Lista de todas as regras implementadas

WAN:

ALLOW RULES											
<input type="checkbox"/>		0 / 33 KiB	IPv4 TCP	*	*	10.120.59.5	80 (HTTP)	*	none	WAN Allow HTTP	    
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	*	*	10.120.59.5	443 (HTTPS)	*	none	WAN Allow HTTPS	    
DENY ALL TRAFFIC											
<input type="checkbox"/>		0 / 13 KiB	IPv4 *	*	*	*	*	*	none	Deny ALL	    

LAN:

ALLOW RULES											
<input type="checkbox"/>		0 / 2 KiB	IPv4 TCP	LAN net	*	*	23 (Telnet)	*	none	LAN Allow Telnet	    
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	21 (FTP)	*	none	LAN Allow FTP	    
<input type="checkbox"/>		0 / 336 B	IPv4 ICMP any	LAN net	*	*	*	*	none	LAN Allow ICMP	    
<input type="checkbox"/>		0 / 0 B	IPv4 TCP/UDP	LAN net	*	*	53 (DNS)	*	none		    
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	80 (HTTP)	*	none	LAN Allow HTTP	    
<input type="checkbox"/>		0 / 0 B	IPv4 TCP	LAN net	*	*	443 (HTTPS)	*	none	LAN Allow HTTPS	    
DENY ALL TRAFFIC											
<input type="checkbox"/>		0 / 1 KiB	IPv4 *	LAN net	*	*	*	*	none	Default Block LAN to any rule	    

Demonstrar que as políticas implementadas estão de facto a funcionar

Provar o acesso TELNET da rede interna para uma máquina da rede externa e da internet:

Usando o site SHODAN conseguir obter um endereço de uma porta 23 aberta para testar a regra colocada.

Como podemos ver pelas imagens seguintes temos acesso às máquinas via TELNET, tanto a uma que esteja na internet como uma na rede externa:

✓	Jun 13 14:39:22	LAN	LAN Allow Telnet (1654891556)	10.120.59.3:53396	88.210.67.177:23	TCP:S
TELNET a uma máquina na internet						
✓	Jun 13 14:40:23	LAN	LAN Allow Telnet (1654891556)	10.120.59.3:35866	192.168.1.118:23	TCP:S
TELNET a uma máquina na rede externa						

Provar o acesso FTP da rede interna para uma máquina da rede externa e da internet:

Também usando o SHODAN encontrei um endereço com a porta 21 aberta para provar a conectividade à internet via FTP.

Como podemos ver pelas imagens seguintes temos acesso às máquinas via FTP, tanto a uma que esteja na internet como uma na rede externa:

✓	Jun 13 14:39:37	LAN	LAN Allow FTP (1654890326)	10.120.59.3:51280	80.172.252.81:21	TCP:S
FTP a uma máquina na internet						
✓	Jun 13 14:40:36	LAN	LAN Allow FTP (1654890326)	10.120.59.3:55074	192.168.1.118:21	TCP:S
FTP a uma máquina na rede externa						

Provar O PING da rede interna para uma máquina da rede externa e da internet:

Para testar o PIGN para a internet usei também o endereço do FTP.

Como podemos ver pelas imagens seguintes temos conectividade PING às máquinas, tanto a uma que esteja na internet como uma na rede externa:

✓	Jun 13 14:40:50	LAN	LAN Allow ICMP (1654887862)	10.120.59.3	80.172.252.81	ICMP
PING a uma máquina na internet						

✓	Jun 13 14:40:42	LAN	LAN Allow ICMP (1654887862)	10.120.59.3	192.168.1.118	ICMP
PING a uma máquina na rede externa						

Provar o acesso HTTP E HTTPS da rede interna para uma máquina da rede externa e da internet:

Para testar o acesso HTTP E HTTPS à internet arranjei os seguintes sites:

HTTP: www.grupojap.pt | 80.172.255.234

HTTPS: www.youtube.com | 142.250.200.78

Como podemos ver pelas imagens seguintes temos acesso HTTP E HTTPS a sites, que esteja na internet como na rede externa:

✓	Jun 13 14:49:38	LAN	LAN Allow HTTP (1654888042)	10.120.59.3:56098	80.172.255.234:80	TCP:S
✓	Jun 13 14:50:01	LAN	LAN Allow HTTPS (1654908174)	10.120.59.3:38296	142.250.200.78:443	TCP:S
HTTP E HHTTPS a uma máquina na internet						

✓	Jun 13 15:02:18	LAN	LAN Allow HTTP (1654888042)	10.120.59.3:54674	192.168.1.118:80	TCP:S
HTTP a uma máquina na rede externa						

Provar o bloquei TELNET da rede externa para uma máquina da rede interna:

Como podemos ver pela imagem é negado o acesso TELNET de uma máquina da rede externa para a rede interna:

✗	Jun 13 15:06:54	WAN	Deny ALL (1654906063)	192.168.1.118:39320	10.120.59.9:23	TCP:S
TELENT negado da rede externa para a interna						

Provar o bloqueio FTP da rede externa para uma máquina da rede interna:

Como podemos ver pela imagem é negado o acesso FTP de uma máquina da rede externa para a rede interna:

✗	Jun 13 15:07:04	WAN	Deny ALL (1654906063)	192.168.1.118:42528	10.120.59.9:21	TCP:S
FTP negado da rede externa para a interna						

Provar o bloqueio ICMP (PING) da rede externa para uma máquina da rede interna:

Como podemos ver pela imagem é negado o ICMP (PING) de uma máquina da rede externa para a rede interna:

✗	Jun 13 15:06:00	WAN	Deny ALL (1654906063)	192.168.1.118	10.120.59.3	ICMP
PING negado da rede externa para a interna						

Provar o acesso HTTP da rede externa para uma máquina da rede interna:

Como podemos ver pela imagem é permitido o acesso de uma máquina da rede externa para a rede interna:

✓	Jun 13 15:06:38	WAN	WAN Allow HTTP (1654907397)	192.168.1.118:58436	10.120.59.5:80	TCP:S
HTTP da rede externa para a interna						

Identificar os protocolos inseguros e propor alterações às tabelas de regras de firewall listadas na introdução

Protocolos inseguros:

- TELNET
- FTP
- HTTP

A alteração que eu proponha seria alterar de:

- TELNET → SSH
- FTP → SFTP
- HTTP → HTTPS

4. IPS/IDS

Coloquei o nosso IPS/IDS na pfsense e usei o snort.

Instalação do Snort:

Segui a instalação e configuração deste site.

<https://techexpert.tips/pfsense/snort-installation-pfsense/#:~:text=PFsense%20%2D%20Snort%20Installation&text=After%20a%20successful%20login%2C%20you,and%20install%20the%20Snort%20package>

Num dos pontos da instalação é selecionado a opção Blocking Mode, eu de início deixei disable.

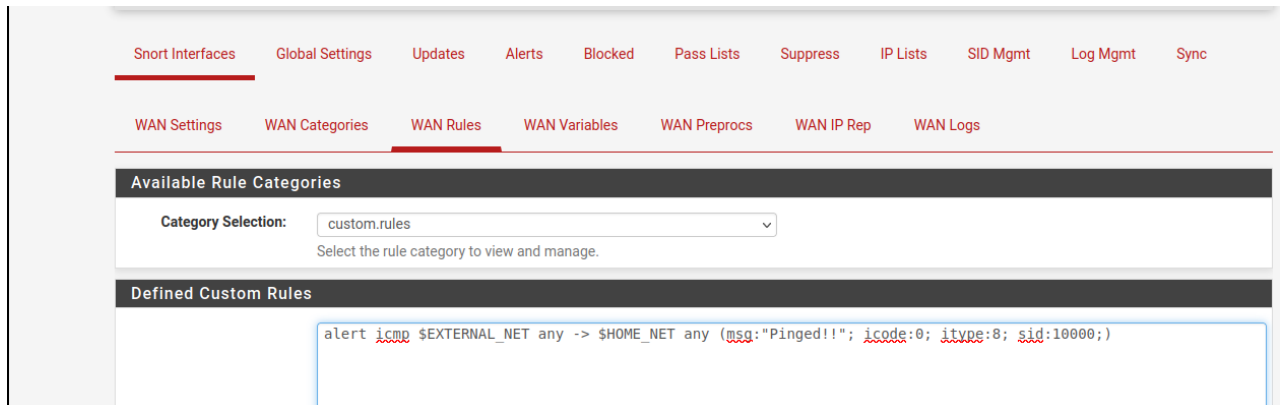
Analisar as assinaturas existentes. Mostrar evidencia.

Installed Rule Set MD5 Signature		
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	d9607d45dabb57a84b8ca912f49c97ac	Saturday, 11-Jun-22 00:05:45 UTC
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	Not Enabled	Not Enabled
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
Update Your Rule Set		
Last Update	Jun-13 2022 00:05	Result: Success
Update Rules	✓ Update Rules	⬇ Force Update
Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.		

Configurar alerta para tráfego ICMP (pings) do exterior (host).

Para configura regras custom, temos de nos dirigir a esta janela da PfSense e definir as regras que queremos usar.

Neste caso defini a regra para alertar se existir alertas do exterior.

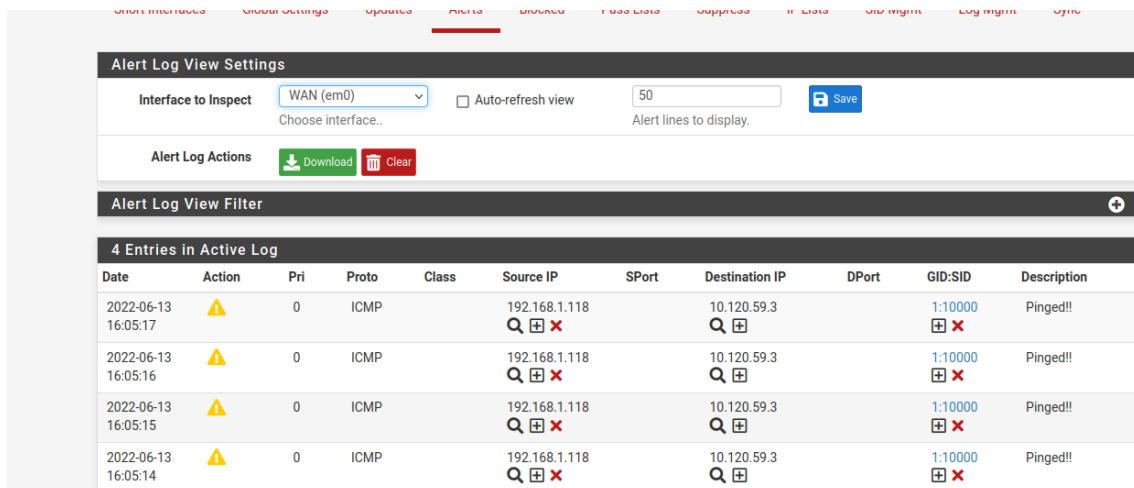


Regra definida:

- alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"Pinged!!"; icode:0; itype:8; sid:10000;)

Icode e iType é para referir para alertar só pings do protocolo ICMP.

Verificar nos logs o registo do alerta do ponto anterior.



Configurar para barrar o tráfego anterior.

Para barrar o tráfego ativei na Snort Interface → WAN Settings → Block Settings o Block Offenders e colocar o IPS Mode em Legacy Mode.

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Legacy Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established 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.

Como podemos ver agora, recebe o alerta e também bloqueia o endereço ip de quem realizou o ping.

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

50

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

+

16 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-06-13 16:09:59		0	ICMP		192.168.1.118		10.120.59.3		1:10000	Pinged!!

Services / Snort / Blocked Hosts

Snort InterfacesGlobal SettingsUpdatesAlertsBlockedPass ListsSuppressIP ListsSID 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 (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	192.168.1.118	Pinged!! – 2022-06-13 16:09:47	

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

Configurar alerta para detectar login de um utilizador root em ftp (serviço a instalar num dos servidores do cenário). Demonstrar.

Para este alerta adicionamos a regra:

- alert tcp \$EXTERNAL_NET any -> \$HOME_NET 21 (content:"USER root"; nocase; msg:"FTP root user access attempt"; sid:10003)

Vai dar alerta se alguém do exterior fizer login de um utilizador root em FTP numa máquina na rede interna.

The screenshot shows the 'Alerts' tab in the Snort interface. It includes sections for 'Alert Log View Settings' (Interface to Inspect: WAN (em0), Auto-refresh view: unchecked, Alert lines to display: 50), 'Alert Log Actions' (Download, Clear), and 'Alert Log View Filter'. Below these is a table titled '1 Entries in Active Log' with columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The table contains one entry: 2022-06-13 16:14:52, Action: [Warning icon], Pri: 0, Proto: TCP, Class: [Search icon], Source IP: 192.168.1.118, SPort: 42536, Destination IP: 10.120.59.9, DPort: 21, GID:SID: 1:10003, and Description: FTP francisco user access attempt.

Configurar alerta para acesso a uma página com referência á palavra “Adult”. Origem nas máquinas internas. Demonstração dessa configuração.

Não estava a conseguir obter alertas com estas regras, mas penso que estejam bem colocadas:

- alert tcp \$HOME_NET any -> \$EXTERNAL_NET 80 (msg:"Adult content found"; content:"adult"; nocase; sid:10001; react:block,msg;)
- alert tcp \$HOME_NET any -> \$EXTERNAL_NET 443 (msg:"Adult content found"; content:"adult"; nocase; sid:10002; react:block,msg;)

No fim das regras tem o campo react que faz com que ao haver este alerta ele bloqueia o endereço ip que realizou o pedido http ou https.

Fiz uma tentativa ao acaso e em vez de colocar no content “adult” coloquei um site “hltv.org”. Ficaram assim as regras:

- alert tcp \$HOME_NET any -> \$EXTERNAL_NET 80 (msg:"Adult content found"; content:"hltv.org"; nocase; sid:10001; react:block,msg;)
- alert tcp \$HOME_NET any -> \$EXTERNAL_NET 443 (msg:"Adult content found"; content:"hltv.org"; nocase; sid:10002; react:block,msg;)

Services / Snort / Alerts

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Alert Log View Settings

Interface to Inspect

WAN (em0)

Choose interface..

☐ Auto-refresh view

50

Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

2 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2022-06-13 16:39:30	⚠	0	TCP		192.168.1.117	24415	104.18.3.89	443	1:10002	CSGO content found
					Q		Q			
2022-06-13 16:39:30	⚠	0	TCP		192.168.1.117	3222	104.18.3.89	443	1:10002	CSGO content found
					Q		Q			

Services / Snort / Blocked Hosts

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

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 (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	104.18.3.89	CSGO content found -- 2022-06-13 16:39:30	×
	Q		

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

5. VPN

Demonstrar as configurações, a subnet usada e os utilizadores criados.

As configurações da minha OpenVPN na PfSense foram realizadas com base no guia que o professor deu na aula.

A subnet usada foi 10.120.59.8.0/24

Criei um utilizador chamado francisco e a password também francisco e a configuração deste User também foi em base do guia dado na aula.

Criar acesso do host para o servidor de FTP.

Para usar o utilizador dirigimo-nos a aba VPN → OpenVPN → Client Export Utility e fazer download do client.

O host instala o cliente e configura a vpn na usa máquina.

The screenshot shows the 'pfSense-UDP4-1194-francisco-config VPN' configuration page in pfSense. The 'Identity' tab is selected. The 'Name' field is 'pfSense-UDP4-1194-francisco-config'. Under the 'General' section, the 'Gateway' is '192.168.1.117:1194:udp4'. Under the 'Authentication' section, the 'Type' is 'Password with Certificates (TLS)'. The 'User name' is 'francisco'. The 'Password' is masked with dots. The 'CA certificate' is 'pfSense-UDP4-1194-francisco-config-ca.pem'. The 'User certificate' is 'pfSense-UDP4-1194-francisco-config-cert.pem'. The 'User private key' is 'pfSense-UDP4-1194-francisco-config-key.pem'. The 'User key password' field is empty. There is a 'Show passwords' checkbox and an 'Advanced...' button.

Ao ligar ira receber um ip na interface tun0 por exemplo:

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.120.58.2 netmask 255.255.255.0 destination 10.120.58.2
    inet6 fe80::a556:288c:b16a:d940 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500
```

Altere as regras da firewall de modo a permitir tráfego. Demonstrar.




Tive de criar uma regra na interface OpenVPN para permitir o tráfego com origem da rede da vpn (10.120.58.0) e destino ao FTP Server (10.120.59.9) na porta 21 (FTP).

Firewall / Rules / OpenVPN


The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
ALLOW RULES											
<input type="checkbox"/>	✓	0 / 1 KiB	IPv4 TCP	10.120.58.0/24	*	10.120.59.9	21 (FTP)	*	none	Allow OpenVPN FTP Server	  

Como podemos ver nas logs a regra está a funcionar bem:

✓ Jun 13 17:17:54 ovpsn1  Allow OpenVPN FTP Server (1654887001)  10.120.58.2:51962  10.120.59.9:21 TCP:S