Servidores Privados Manual Firewall Palo Alto





IIIEO empresas

1.	In	ntrodução	3
2.	F/	AQ	3
	2.1.	Como faço para aceder à Interface de gestão da Firewall Palo Alto?	3
	2.2.	Como está configurada a rede na minha Firewall?	5
	2.3.	O que são as "Zonas" configuradas na minha Firewall?	7
	2.4. Ades	Como faço para publicar na Internet um WEB SITE alojado num Servidor Privado da minha são?	8
	2.	.4.1. Publicação pelo IP público de IPv4 (só nas adesões onde este foi adquirido)	8
	2.	.4.2. Publicação pelo IP de IPv6	. 19
	2.5. remo	Como faço para estabelecer um Túnel VPN IPSEC entre a minha Firewall e uma Firewall ota?	.26
	2.	.5.1. Túnel VPN IPSec pelo IP público de IPv4 (só nas adesões onde este foi adquirido)	.26
	2.	.5.2. Túnel VPN IPSec pelo IP de IPv6	. 35
	2.6.	Como faço para me ligar com um cliente VPN aos Servidores Privados da minha Adesão?	.45
	2.	VPN GlobalProtect pelo IP público de IPv4 (só nas adesões onde este foi adquirido)	.45
	2.	.6.2. VPN GlobalProtect pelo IP de IPv6	. 61
	2.7.	Que configurações devo alterar antes de remover um IP da minha Firewall?	. 61
	2.8.	Onde posso encontrar mais informação soobre como configurar a minha Firewall?	.63
	2.9.	Como posso saber as Características Técnicas/ Funcionalidades da minha Firewall?	.63





1. Introdução

Este documento pretende responder às perguntas mais frequentes – FAQ – sobre a configuração da firewall Palo Alto do serviço Servidores Privados da Cloud MEO Empresas.

2. FAQ

2.1. **Como faço para aceder à Interface de gestão da Firewall Palo Alto?**

O acesso à interface de gestão da firewall Palo Alto é feito pelo Portal de Configuração IAAS – Internet as a Service – da sua adesão de Servidores Privados da Cloud MEO Empresas.

Faça Login no portal <u>cloud.meoempresas.pt</u> com as suas credenciais de cliente MEO, procure a sua adesão de servidores privados na lista e clique em "Configurar":

Selecione uma Conta	A Minh	a Conta Utiliza	dores Relatóri	os e <mark>Docu</mark>	mentação	Fluxos de a	provação	
PT PRIME-SOLUÇÕES EMPR₩						Incluir adv	esões canceladas	Q
Associar nova conta	0				1 . 193		0	
Os Meus Serviços	Nº adesão	Designação	Designação Data de adesão Es			stado		- Acão
	400100732	My VDC 2	11-05-	2022	Ø		Gerir Confi	gurar
Vouchers			LEGEN					6
Dados da Conta	A aguardar ativação	V Ativa	Falha na ativação) Susp) Densa	Cancelada	A agua aprova	v Irdar Ição
Podemos ajudar? 🕢	A iniciar	A ativar	A cancelar	A aguar	dar nova	₽ S Falha na criação	5	





Na aba "Redes" e clique em "Gerir":

	Servideres / Appliances Crupes Dodos	Recurrent	Tomplator	ISOs Athuldada	
	Servidores / Appnances Grupos (1878)	Recursos	remplates	ISOS Atividades	. 3
DETALHES DA RE	EDE				
Firewall	nativa Ilgado	Gerir]		
IP Público	215.13.132.96 2802.818.2101=c0				
Largura de Banda	Download 100Mbps / Upload 100Mbps	Gerir			
Criar rede				Ver detailhes do(s)	servidor(es) Mostrar grupos vazios
FE Rede Inicial de FrontEnd				Rede privada 🏔	Eliminar Renomear +
Rede Inicial de FrontEnd					

Clique no Link "Use Single Sign-On" e, de seguida, clique em "Continue":

	INEO EMPRESAS	
	Username	
	Password	
	Log In <u>Use Single Sign-On</u>	
ESTE SI CONTINU AUTORIZ REGISTA PORTUGA	ESTEMA APENAS DEVERA SER USADO POR UTILIZADORES AUTORIZADOS. AO JARA A USAR ESTE SISTEMA O UTILIZADOR RECONHECE QUE E UM UTILIZA ZADO. O UTILIZADOR RECONHECE QUE AS UTILIZACOS DESTE SISTEMA S JADAS E COMPREENDE QUE AS VIDLACOES A POLITICA DE SEGURANCA DA A AL A NIVEL DOS SISTEMAS E TECNOLOGIAS DE INFORMACAO E COMUNICACI	DOR AO LTICE DES





Volte a introduzir as suas credenciais de cliente MEO caso lhe seja solicitado e, passados alguns instantes, irá visualizar a interface de gestão da firewall:

	Layout 3 Columns 🗸	Widge	ets 🛩 🛛 Last upda	ated 11:07:0	8					5 mins	~ G		
Seneral Information		$\mathbb{G} \times$	Logged In Adm	nins			G×	Config Logs			G×		
Device Name	100003202-paloalto		Admin	From	Client	Session Start	Idle For	Command	Path	Admin	Time		
MGT IP Address	10.16.64.29		luisfrodrigues	169.254.1.1	Web	05/19 10:27:53	00:00:00s	commit		luisfrodrigues	05/19		
MGT Netmask	255.255.248.0		panorama	Console	Panorama	05/18 22:07:53	00:15:53s			Later Free stations and	10:50:35		
MGT Default Gateway	10.16.64.1							edit	Network virtual-router VRouter1	luistrodrigues	10:50:31		
MGT IPvő Address	unknown		Data Logs	Data Logs			G×	commit	luisfrodrigues	05/19			
MGT IPv6 Link Local Address	fe80::250:56ff:feb5:5e95/64		No data available	No data available.							10:36:48		
MGT IPv6 Default Gateway			System Logs					edit network interface tunnel units tunnel 10	luisfrodrigues	05/19 10:34:38			
MGT MAC Address	00:50:56:b5:5e:95						G X		annes connectao		2010 1100		
Model	PA-VM		Description				Time	Locks			5		
Serial #	015351000079188		NTP sync to server 10.16.4.133 05/19				05/19	All dealer front d			0,		
CPU ID	ESX:50060500FFFB8B0F				11:06:46	NO IOCKS TOUND							
UUID	4235B0AB-41F5-5D05-42EC- 0A9BF2C319B5		Connection to Update server: updates.paloaltonetworks.com completed successfully. initiated by 10 16 64 29			05/19 11:05:32	ACC Risk Facto	r (Last 60 minutes)		G			
VM Cores	2		IKEv2 IKE SA ne	gotiation is succ	eeded as initia	ator, non-	05/19		3.2				
VM Memory	5580644		rekey. Established SA:			1001	10:51:29						
VM License	VM-50		SPI:88a21503b4	4b52e38:672c4t	074c6e742ee	lifetime							
VM Capacity Tier	5.5 GB		28800 Sec.										
VM Mode	VMware ESXi		IKEv2 child SA n rekey Establishe	regotiation is suc	ceeded as init	iator, non-	05/19						
Software Version	1013		2a02:818:2101:	:c0[500]-2a02:8	18:2101::40[5	i00] message							
GlobalProtect Agent	5.2.8		18:0x00000001.	SPI:UXA020E34	E/UXEBF2/3B	sD.	05/10						
Application Version	8494-7079 (12/01/21)		2a02:818:2101:	ed. installed SA: :c0[500]-2a02:8	18:2101::40[5	600)	10:51:29						
Device Dictionary Version	49-327 (05/13/22)		SPI:0xA020E34	E/0xEBF273BD	lifetime 3600	Sec lifesize							
URL Filtering Version	0000.00.00.000		IKE protocol pot	ification messas	e received rec	reived potify	05/19						
GlobalProtect Clientless VPN	0		type ESP_TFC_F	ADDING_NOT	SUPPORTED	correct monthly	10:51:29						
Version			received notify t	ype	received notify type			05/19					

2.2. Como está configurada a rede na minha Firewall?

A firewall Palo Alto da sua adesão de servidores privados vem configurada com as seguintes interfaces de rede:



Interface management: para uso interno da MEO, necessária para assegurar o serviço de firewall à adesão;

Interfaces ethernet:

- 1. ethernet1/1: para uso interno da MEO, necessária para assegurar o serviço de firewall à adesão;
- 2. ethernet1/2: interface WAN (pública) da firewall;
- 3. ethernet1/3 a 1/9: interfaces privadas da firewall.

Interfaces tunnel

- **4.** tunnel.10: faz parte da pré-configuração básica *ready to use* de um túnel IPSec VPN para ligação a uma firewall remota (VPN Site to Site);
- 5. tunnel.20 a tunnel.50: disponíveis para serem usadas na criação de túneis IPSec VPN adicionais;

Na provisão da adesão, a firewall vem com uma interface privada disponível. Na Loja podem ser adicionadas mais interfaces privadas até um total de três.

A firewall vem sempre com endereçamento IPv6 atribuído, tanto na interface WAN como nas interfaces privadas. Para a atribuição de informação de rede IPv6 aos servidores privados a firewall Palo Alto implementa "IPv6 Stateless Address Autoconfiguration" (RFC 4862) e "IPv6 Router Advertisement Options for DNS Configuration" (RFC 8106). Os endereços IPv6 do DNS primário e secundário são os endereços IPv6 dos servidores de DNS rs.webside.pt e rs2.webside.pt, do serviço de clientes empresariais da MEO.

O endereçamento público IPv4 é opcional. Se for pretendido, pode ser adquirido um IP público de IPv4 na Loja.

Nas adesões em que foi adquirido um IP público de IPv4, a firewall vem com as seguintes configurações adicionais:

- DHCP ativado nas interfaces privadas para a atribuição de informação de rede IPv4 aos servidores privados. A informação de DHCP é a seguinte:
 - 6. IP address pool: 172.16.X.2 172.16.X.128
 - 7. Network mask: 255.255.255.0
 - 8. Default gateway: 172.16.X.1
 - 9. DNS primário: 62.28.116.41 (rs.webside.pt)
 - 10. DNS secundário: 62.28.40.173 (rs2.webside.pt)

O terceiro octeto X é igual a 2 para a primeira interface privada ethernet1/3, igual a 3 para a ethernet1/4 e assim sucessivamente até X igual a 8 para a última interface privada ethernet1/9.



Após a configuração inicial, quando um servidor privado for posto a dar serviço, é vivamente aconselhável configurar o servidor com um IP fixo ao invés de um IP da pool de DHCP. Na configuração da placa de rede do servidor deverá colocar um IP da gama 172.16.X.129 – 172.16.X.254 e fixar também os IPs do DNS primário e secundário.

- Uma interface tunnel.200, fazendo parte de uma pré-configuração básica *ready to use* da VPN GlobalProtect para ligação de clientes remotos às redes internas do VDC (VPN Client to Site).

Esta interface está configurada com a rede 172.16.50.0/24. Os clientes remotos ligados pela VPN GlobalProtect ficam com um IP nesta rede (pool).

- Uma interface loopback.1, também fazendo parte da pré-configuração da VPN
 GlobalProtect. Está configurada com o IP 172.16.60.1 e é utilizada exclusivamente na tradução do acesso ao portal GlobalProtect, através de regra NAT, do IP público de IPv4 da firewall e porto 4443 para o IP privado 172.16.60.1 e porto 443.

2.3. O que são as "Zonas" configuradas na minha Firewall?

A firewall Palo Alto controla o tráfego de pacotes de rede entre interfaces através de uma política de segurança, decidindo como atuar num pacote consoante este vá de encontro a uma regra de segurança dessa política. No mínimo, a regra de segurança deve identificar de onde vem o tráfego e para onde vai. Na firewall Palo Alto as regras de segurança são aplicadas entre Zonas. Uma Zona é um agrupamento de interfaces que representa um segmento da sua rede que está ligado e que é controlado pela firewall.

A firewall Palo Alto vem configurada com as seguintes Zonas:

MGMT (ethernet1/1) - Para uso interno da MEO;

Untrust (interface WAN ethernet1/2) - Tráfego externo, tipicamente não confiável;

Trust (interfaces privadas ethernet1/3 a 1/9) - Tráfego interno, tipicamente confiável;

- S2S (interface tunnel.10) Tráfego do túnel VPN IPSec. Zona usada na regra de segurança "S2S_Allow" para permitir o tráfego da VPN Site to Site básica *ready to use* pré-configurada na firewall;
- S2S2 a S2S5 (interfaces tunnel.20 a tunnel.50, respetivamente) Zonas disponíveis para serem usadas em regras de segurança para permitir o tráfego de VPNs Site to Site adicionais.

Nas adesões em que foi adquirido um IP público de IPv4, a firewall vem com a seguinte zona adicional:

14.04.2025



- VPN (interface tunnel.200) - Tráfego da VPN GlobalProtect. Zona usada pela VPN Client to Site básica *ready to use* pré-configurada na firewall.

2.4. Como faço para publicar na Internet um WEB SITE alojado num Servidor Privado da minha Adesão?

2.4.1. Publicação pelo IP público de IPv4 (só nas adesões onde este foi adquirido)

No exemplo se segue o site está alojado num servidor privado da adesão com sistema operativo Windows Server 2019 e hostname web001. O servidor tem o role Web Server instalado, tem o IP 172.16.2.130 e a firewall do Windows está desligada:

Adesão: 400100732 - My VDC 2						Monitorização e Reporting
	Servidores / Appliances G	rupos Redes	Recursos Temp	lates ISOs	Atividades 3	
Web-Server Servidor ligado com avisor 172.16.2.130	Ð.					Operações 🔻
Servidor / Appliance	Designação 🚯	We	b-Server			Alterar
Armazenamento	Hostname	web	b001			
	Template	Wir	ndows Server 2019 Star	ndard Edition (L	icensed)	
Alertas	Grupo	De	fault		~	Alterar
Estatísticas	Rede	FE			~	
Histórico	Descrição	[]]]				Alterar

A nossa firewall Palo Alto tem o IP público de IPv4 213.13.132.96:

		10		Monitorização e Rep
DE	Recursos	emplates is	Os Atividades 3	
nativa ligado	Gerir			
215.13.132.96 2a02.818:2101.c0				
Download 100Mbps / Upload 100Mbps	Gerir			
			Ver detailhes do(s) servidor(es)	Mostrar grupos vazios
			Rede privada 🔒 Elimir	nar Renomear +
	Servidores / Appliances Grupos Redes	Servidores / Appliances Crupos Redes Recursos Crupos Crupo	Servidores / Appliances Grupos Redes Recursos Templates IS IDE native ligado Gerir	Servidores / Appliances Crupos Redes Templates ISOs Atividades S DE native leade Gerir Gerir ISOS <



Primeiro vamos criar dois objetos na firewall para serem utilizados posteriormente, o IP público do site web e o IP privado do mesmo site.

Faça login na firewall. Selecione a aba "OBJECTS" e no menu à esquerda selecione a opção "Addresses". Clique em "Add" para adicionar um objeto novo:



Preencha a informação do objeto e clique em "OK":

									S ()
🖨 Addresses 👘 🚊									$_{2 \text{ items}} \rightarrow \times$
Address Groups		NAME	LOCATION	TYPE		ADDRESS		TAGS	
C Regions		gp-private		IP Netm	ask	172.16.60.1			
Dynamic User Groups				IP Netm	ack	213 13 132 96			
Ca Application Groups									
Application Filters		_							
X Services •		Address					0		
Service Groups		Name unbe	nor nublic						
Devices		Description Public	IPu4 address of web site o	n web001					
V 🧟 GlobalProtect		Type IP Ne	mack	2	3 13 132 96		Devites		
HIP Objects		Type In the		Ent	er an IP address or a net	work using the slash notation (Ex. 192.168.80	150 or		
HIP Profiles				192 (Ex	2001:db8:123:1-1 or 2	also enter an IPv6 address or an IPv6 address 001-db8-123-1-/64)	with its prefix		
External Dynamic Lists Custom Objects		Tags 4		120					
Data Patterns									
Spyware									
Unerability						OK	Cancel		
W URL Category									
Antivirus									
D Anti-Spyware									
Unerability Protection									
URL Filtering									
File Blocking									
A Data Filtering									
TRA AND			OF/CSV						
luisfredrigues Logout Last Logi	n Time	: 05/18/2022 22:27:52 Session	Expire Time: 06/17/2022	22:27:52				∃ Tasks Languej	👳 🥠 paloalto

O IP público de IPv4 adquirido também pode ser consultado na firewall, para isso selecione a aba "NETWORK" e no menu à esquerda selecione a opção "Interfaces". Clique na interface "ethernet1/2":

											0
7 interfaces	Ethernet VLAN	Loopback Tunne	I SD-WAN								
VLANs	0										
Virtual Wires	Q	10				121	10			9 items	$) \rightarrow$
Virtual Routers e										SD-WAN	
IPSec Tunnels *	INTERFACE	INTERFACE TYPE	PROFILE	STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-	SECURITY ZONE	PROFILE	
GRE Tunnels	athemat4 /4	Laver3	HTTPS-ICMP-		169 254 245 197/16	VRouter1	Untagend	0000	MGMT		-
DHCP .	ethernet1/1	V Layers	SSH-MGMT		107.254.245.177/10	VROBIETI	Ontagged	none	MGMT		
DNS Proxy	ethernet1/2	Layer3	ICMP		213.13.132.96/24	VRouter1	Untagged	none	Untrust		
GlobalProtect					2a02:818:2101::c0/64						
🚳 Portals 🔹 🔹	Cathornet1/2	Laver3	ICMP	-	172 16 2 1/24	VRouter1	Untagged	none	Trust		
Gateways •	mercence 75	89		الك	2-02-010-2101-0-774						
MDM					2802:616:2101:00::/64						
Clientless Apps	ethernet1/4	Layer3	ICMP		172.16.3.1/24	VRouter1	Untagged	none	Trust		
Clientless App Groups	4				2a02:818:2101:c1::/64						
Qo5	ethernet1/5	Layer3	ICMP		172.16.4.1/24	VRouter1	Untagged	none	Trust		
LLDP					2a02:818:2101:c2::/64						
A GlobalProtect IPSec Go	GR ethemet1/6	Layer3	ICMP		172 16 5 1/24	VRouter1	Untagged	none	Trust		
H IKE Gateways					2-02-010-21012/44						
A IPSec Crypto a	and a state of the state	1.000.000	10110		2802:010:2101:03::/04						
A IKE Crypto e	ethernet1/7	Layer3	ICMP		1/2.16.6.1/24	VRouter1	Untagged	none	Irust		
A Monitor					2a02:818:2101:c4::/64						
🐻 Interface Mgmt 🔹	cthemet1/8	Layer3	ICMP		172.16.7.1/24	VRouter1	Untagged	none	Trust		
Zone Protection					2a02:818:2101:c5::/64						
🚴 QoS Profile 🔹 🔹	ethernet1/9	Layer3	ICMP	100	172.16.8.1/24	VRouter1	Untagged	none	Trust		
Study Profile					2-02-818-2101-6/64						
🕪 BFD Profile 🔹 🔹	4										

Clique na aba "IPv4" para consultar o IP:

			Commit ~		٠Q						
				ŧ	3 🕐						
Interfaces	Ethernet VLAN Loopback Tunnel SD-WAN										
G VLANs		9 items) ->									
Virtual Routers	Intual Works Ethernet Interface										
GRE Tunnels	Bethemet1 Interface Name ethemet1/2 Comment WAN		MGMT								
© DNS Proxy ✓ ④ GlobalProtect	Bethermet Linterface Type Layer3		Untrust								
Gateways	Config IPv6 SD-WAN Advanced		Trust								
Clientless Apps	Contraction Cont		Trust								
🎄 QoS	ethemet1 2131313296/24		Trust								
Lie Network Profiles GlobalProtect IPSec (in) K KE Galeways	The address of the second se		Trust								
හි IPSec Crypto ම හි IKE Crypto ම	athematik		Trust								
Monitor Monitor Monitor Monitor	athemati Paddress/hetmask. Ex. 192.168.2:294/24	1	Trust								
S QoS Profile •	Bethemet1/)	Trust								
BFD Profile											
luisfrodrigues Logout Last Login Time	ier 05/18/2022 22:27:52 Session Expire Time: 06/17/2022 22:27:52		j≘ Tasks Lang	palo	oalto						

Vamos também criar o objeto referente ao IP privado do web site. Na firewall, volte a selecionar a aba "OBJECTS" e no menu à esquerda selecione a opção "Addresses". Clique em "Add", preencha a informação do objeto e clique em "OK":



	_	DIGHEOARD ACL	MUNITOR POLICIES	UNITED NETWORK	EVILE	
Addresses						S Ø Jitems)→ X
Address Groups		NAME	LOCATION	TYPE	ADDRESS	TAGS
Concern Unit Forem		gp-private		IP Notmask	172.16.60.1	
Applications		gi public		IP Netmask	213.13.132.96	
Application Groups		webocyver-public		IP Netmask	213.13.132.96	
Appreciation reliefs		Address			(
Service Groups Taps		Name	ebserver-private			1
CE Devices		Description F	rivate IPv4 address of web site on v	web001		
Goberrotect HIP Objects		Type 1	Netmask	√ 172.16.2.130	Resolve	20 - 10 - 10 - 10 - 10 - 10 - 10 - 10 -
HIP Profess				Enter an IP address or a 192.168.80.0/241. You (Ex. 2001.458.123.1.1	i network using the slash notation (Ex. 192.168).80.150 or can also anter an IPv6 address or an IPv6 address with its perfe- or 2001tbil:122:1::/64)	
G Custom Objects		Tags		AND BOX OR STRANTIN		
Data Patierra						
Spyware Shidwardality					OK Caroel	
URL Cutegory		-				
 Security Protest 						
Antivitus						
Volverability Protection						
URL Filtering						
File Blocking						
Cuta Ethnore						
Contract -						

O IP privado do site corresponde ao servidor IPv4 privado do servidor web001, o IP 172.16.1.130.

De seguida iremos configurar uma regra de NAT para traduzir o IP público do site para o IP privado. Para isso selecione a aba "POLICIES" e no menu à esquerda selecione a opção "NAT". Clique em "Add" para adicionar uma regra de NAT nova:

		DA	SHBOARD AC	C MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE			🛓 Commit 🗸 🛛 🕴 🕶 🗸	Q
											G	?
📾 Security	= (QC									3 items) -	→×
⇒ NAT							c	Original Packet			Tra	inslated
🍰 QoS 🚯 Policy Based Forwarding		N	AME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	c
Decryption		1 0	ilobalProtect Inbou	none	2 Untrust	Market Untrust	any	any	gp-public	🗶 service-gp-h	none	c
Application Override												
Authentication												F
SD-WAN		2 0	ilobalProtect Inbou	none	Martinet	Market Untrust	any	any	gp-public	💥 service-gp-ip	none	c
												F
		3 N	IAT_Trust_to_UnTrust	none	FZA Trust	Martine Untrust	ethernet1/2	any	any	any	dynamic-ip-and-port	зr
Policy Optimizer	- 4										ethemet1/2	
											213.13.132.96/24	
K Unused in 30 days	1											
🚯 Unused in 90 days	1											
		4										
Object : Addresses	+	(+) Ade		one 🕢 Enable (Disabie Move	PDF/CSV	Highlight Unus	ed Rules 🗌 View Rulebase	as Groups Rese	et Rule Hit Counter 🜱	Group ~ Test Policy Match	>>
The second se		Dana C	E (10 /0000 00.07.61								The Inclusion	lto

Preencha a informação da regra de NAT nova e no final clique em "OK":





	a	DASHBOARD ACC	MONITOR POLICIES	OBJECTS	NETWORK DE	VICE			<u>t</u> Commit ∽ 'tr ♥ir ♥
									9 Ø
Security	. Q(3 items → ×
⇒ NAT					Origi	nal Packet			Translated
QoS				DESTINATION	DESTINATION		DESTINATION		
Decryption		NAT Policy Rule						2	SOURCE TRANSLATION
Tunnel Inspection	1	Glot						-go-h	none
Application Override		General Origina	I Packet Translated Pack	et					-
Authentication		- Any	Destination Zone		Any		- Anv	1	
G SD-WAN	2		Untrust	~	SOURCE ADDR	E55 ^	DESTINATION ADDRESS	-gp+ip.	_ none
		Vintrust					webserver-public		
	2	NAT	Destination Interfa	ace					
Policy Ontimizer		- Contraction of the Contraction	any	~					by mixe ip mix port
so (= 0.de lineer									ethemet1/2
Unused in 30 days	1		Service						213.13.132.96/24
Unused in 90 days	1		any	~					
R Unused	1	🕂 Add 🕞 Delete			🕀 Add 🕞 Delete		🕀 Add \ominus Delete		
							OK Cancel		
								- I.	
Object - Addresses	1 0	AN ONLY DOWN	Contraction Marine	× Buncicov	The state to be a second of the		Delahara ar Canana - Davat Dela III		Provide and Track Deliver Matches
Uniferentiatures Larout Lart		105/18/2022 22/27-52 Seed	ion Evoire Time: 06/17/2022.2	00752	La Againgat Ondsed F	unes [] view	nuicuase as taroups Reset Rule Hi	e counter *	Take Descrote Match >>





Agora é necessário criar uma regra de segurança para permitir o acesso da Internet ao web site. Para isso selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Clique em "Add" para adicionar uma regra de segurança nova:

												G (?)
🖽 Security	Q											$_{6 \text{ items}} \rightarrow \times$
⇒ NAT							Source			Destination		
& QoS Policy Based Forwarding		NAME	TAGS	ТҮРЕ	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIO
 Decryption Tunnel Inspection Application Override 	1	S2S_Allow	none	Interzone	122 525	any	any	any	100 525 100 Trust	any	any	any
Authentication	2	VPN_Allow	none	universal	PPR VPN	any	any	any	Trust	any	any	any .
SD-WAN	3	GlobalProtect Portal	none	universal	M Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_AlL	none	universal	🎮 Trust	any	any	any	M Untrust	any	any	any
Policy Optimizer -	5	intrazone-default ®	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1	6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
C noise virtuoda app controls a C Unused Apps (Rule Usage												
	4											+

Preencha a informação da regra de segurança nova e no final clique em "OK":

) empresas

III



and Security							
⇒ NAT				Source		Destination	
Policy Based P	Convitu Della	Pula					APPLICATIO
Decryption	Security Policy	/ Rule				U	j any
Application O	General Sou	rce Destination Application Se	ervice/URL Category Acti	ons			
Dos Protectio	Name	Webserver access					any
🕞 SD-WAN	Rule Type	universal (default)				~	any
	Description	Access from Internet to web site on web001					
							any
	Tags	×				•	any
Policy Optimizer	Group Rules By Tag	None				~	j l
New App View	Audit Comment						antiy
Unused Apps							
V 🚝 Rule Usage		Audit Comment Archive					
No Unused in						Carl Carl	5
Noused						Cancel	2
	1						•
Object : Addresses	+ ⊕A	Add S Delete S Clone S Override 1	Revert' @ Enable S Disa	Move * PDF/CSV] Highlight Unused Rules 🗌 ۱	/iew Rulebase as Groups Reset Rule Hit (Counter * Groon

Security	DASHBOARD A	CC MONITOR POLICIES OBJE	CTS NETWORK DEVICE	ts Commit v	ি চি≺ Q হ ়ে 6 items → X
→ NAT QoS Policy Based P Decryption	Security Policy Rule		Source	Destination	APPLICATIO
Tunnel Inspect	General Source Destination	Application Service/URL Category	Actions		any
CE DoS Protectio		SOURCE ADDRESS			any .
Policy Optimizer	Vintrust				any Sny any
∼ /Ξ Rule Usage	⊕Add ⊖Delete	Add Delete	() Add () Delete	🕀 Add 🕞 Delete	
K Unused in B Unused in Unused	G	Negate		Ort Cance	
Object : Addresses		kane 🕲 Override 🔿 Revert 🖉 Enable 🚫	Disable Move 🖌 🔞 PDF/CSV 🗌 Highlight U	nused Rules 🗌 View Rulebase as Groups 👘 Reset Rule H	it Counter * Group * »
luisfrodrigues Log	zout Last Login Time: 05/18/2022 22:27:5	2 Session Expire Time: 06/17/2022 22:27:52		\$⊟ Tasks Lar	guage и paloalto



+ NAT		Course			
QoS				Cestmanon	
 Policy Based F Decryption 	Security Policy Rule			0	APPLICATIO
Tunnel Inspeci Application O	General Source Destination Applicatio	n Service/URL Category Actions			
Authentication	select	Any	anv		
SD-WAN	DESTINATION ZONE	DESTINATION ADDRESS	DESTINATION DEVICE		any
	Trust	V c webserver-public			
					any
					any
y Optimizer					any
Rules Without Unused Apps Rule Usage	⊕ Add ⊖ Delete	(+) Add (-) Delete	+ Add O Delete		
B Unused in		Negate			
Concern in					
				OK Cancel	

DASHBOARD ACC MONITOR POLICIES		
📾 Security 💿 🔍 🤇		$\begin{array}{c} & \textcircled{\begin{tabular}{lllllllllllllllllllllllllllllllllll$
ANT ■ CoS Dorog Read Proceeding	Source	Destination
Security Policy Rule Security Policy Rule Application General Source Destination Application Service/URL Cate	egory Actions	
Authenticatie Any Any Any Any Any		$0 \text{ items} \rightarrow \times$
V to mini		
Policy Optimizer		any.
Rew App View		ativ)
Visued Apps ✓ ∰ Rule Usage → Add → Delete	Add To Current Rule Add To Existing Rule	
40、Unused in 昭 Unused in 形 Unused in		Cancel
Object : Addresses + OAdd ODclete OCone Override: @ Revent @ End	able 🚫 Disable Move Y 🐵 PDF/CSV 🗌 Highlight Unused Rüles 🗌 Vie	* Rulebase as Groups Reset Rule Hit Counter * Group * *
luisfrodrigues Logout Last Login Time: 05/18/2022.22:27:52 Session Expire Time: 06/17/2022.22	2:27:52	🗧 Tasks Language - 🥠 paloaito



			Commit ~	
Security	Q		6 ii	G ⑦ tems)→×
→ NAT	*	Source	Destination	
 Decryption Tunnel Inspect Application O 	Security Policy Rule General Source Destination Application Service/URL Category Actions	ŝ	0	any
Authentication	application-default v	Any		
🥵 SD-WAN	SERVICE A	URL CATEGORY A		any
				any
Policy Optimizer				any
Roles Without			_	апү
Unused Apps	③Add ⊖Delete	⊕ Add ⊝ Delete		
IN Unused in No Unused in No Unused			Ск Canirel	
			_	
	4			•
Object : Addresses	+ OAdd Obelete OCone O Overlide Revent O Englide O Dealle	Move Y PDF/CSV Highlight Unused Rules	View Rulebase as Groups Reset Rule Hit Counter *	naloalto
impluoningnes i roß				paroallo

DASHBOARD	D ACC MONITOR POLICIES OBJECTS	NETWORK DE	VICE	(En Contril y	ା ଲ ଲେ• ସ୍ ତ ଡ
Security					$_{6 \text{ items}} \rightarrow \times$
∃+ NAT ●		Source		Destination	
QoS					
B Decryption Security Policy Rule				0	APPLICATIO
Tunnel Inspec Application O General Source Dest Application C General Source Dest	tination Application Service/URL Category Actio	ns			unity .
DoS Protectio Action Setting		Log Setting			any
SD-WAN Action Allow	we	×	Log at Session Start		any
5		Log Forwarding	default	~	
		Other Settlers			any
Profile Setting		Schedule	None	6	any
Policy Optimizer Profile Type Non	ne	 QoS Marking 	None	~	any
Rules Without			Disable Server Response Inspection	i	
C Unused Apps				OK Cancel	
Object : Addresses + + Add Obele	ete 🛞 Cone 🕲 Overlide 🕫 Revert 🥥 Erable 🚫 Disabl	- Move Y DF/C	SV 🗌 Highlight Unused Rules 🗌 Vi	ew Rulebase as Groups Reset Rule Hit C	ounter Y Group Y
luis-f-rodrigues@telecom.pt Logout Last Login Tim	ne: 05/19/2022 11:21:28 Session Expire Time: 06/18/2022 17:	15:52		≶⊟ Tasks Langua	🚌 🥠 paloalto

Para tornar as alterações efetivas, clique no botão "Commit" e na caixa de diálogo clique em "Commit":



102 Security	Q											6 items → ×
B NAT			1				Source			Destination		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICAT
 Decryption Tunnel Inspection Application Override 	1	S25_Allow	none	Anterzone	MAI S25	arbi	any -	aniy	Trant	any	ary.	any.
Authentication	2	VPN_Allow	mone	universal	(mag V29V	any	any .	lary .	(PR) Trust	any .	any	any
SD-WAN	3	GlobalProtect Portal	none	universal	Pa Untrust	any	any	any	P Untrust	🔁 go-public	any	any
	4	Trust_to_Untrust_All_	none	universal	M Trust	any	ану	any	M Untrust	any	any	any
	5	Webserver access	none	universal	179 Untrust	any	arriy	any	PA Tost	🕞 webserver-pu	any	I web-t
licy Optimizer -	6	Intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
Rules Without App Controls	7	Interzone-default	none	interzone	any	any	any	any	any	any	any	any
Ender Unage Unused in 30 days Unused in 90 days Unused												

-									Aitems > >
⇒ NAT •	4		Commit		08		Destination		
 QoS Policy Based Forwarding 		NAME	Doing a commit will overwrite the running configuration with	the commit scope.			ADDRESS	DEVICE	APPLICATI
Decryption	1	525 Allow	O Commit All Changes Commit Changes Made By:(1	luisfrodrigues					
Application Override				LOCATION TYPE		et:			
Authentication	2		policy-and-objects			si.			
C SD-WAN	3	GlobalProtect Portal				trust	gp-public	any	any
	4	Trust_to_Untrust_All				trust	any	any	any
	5	Webserver access				st	webserver-pu	any	web-br
New App Viewer	ó	intrazone-default				one)	any	any	auv
Rules Without App Controls 2	7	interzone-default					any	any	any
Consect Apps			Preview Changes DE Change Summary	date Commit	Group By Location Type				
Unused in 30 days 1			Note: This shows all the changes in login admin's accessible domain						
Unused in 90 days 1			Description						
					Commit Cancel				

Quando o Commit estiver concluído, clique em "Close":



	0							G ①
B Security =	Q	1	Commit Status	0	-	Dertination		→ X
🚴 QoS By Policy Based Forwarding		NAME	Operation Commit		E	ADDRESS	DEVICE	APPLICATIO
 Decryption Tunnel Inspection Application Override 	1	525_Allow	Status Completed Result Successful Details Performine panorama connectivity check (attempt 1 of 1)		725 Tust	any	any	any
Authentication	2	VPN_Allow 🗸	Panorama connectivity check was successful for 10.16.41.194 Configuration committed successfully	- 1	nust	any	any	any
SD-WAN	3	GlobalProtect Portal	Commit		Jntrust	gp-public	any	any
	4	Trust_to_Untrust_All		- 1	Intrust	any	any	any
*	5	Webserver access			frust	🖕 webserver-pu	any	web-brow
Policy Optimizer	ő	intrazone-default.			izone)	апу	апу	any
Rules Without App Controls 2	7	interzone-default				any	any	any
S Faule Usage S Unused in 30 days 2 S Unused in 90 days 2 D Unused in 90 days 2 D Unused 2 S D D S	4			ose				•

Para testar o acesso ao web site use um PC ligado à Internet e coloque o URL <u>http://213.13.132.96</u> num browser. Irá aparecer a página default do IIS:





2.4.2. Publicação pelo IP de IPv6

Para publicar o web site por IPv6 não é necessário configurar NATs na firewall porque, by design, todo o IPv6 é público. Não quer isto dizer que o web site está imediatamente exposto na Internet se tiver um IP de IPv6, tal como no exemplo do IPv4, é sempre necessário que exista uma regra de segurança configurada na ACL a permitir o acesso.

Vamos continuar a usar o exemplo de um servidor privado na adesão com hostname web001 e role Web Server instalado, onde se encontra alojado o web site a publicar. Para verificar qual é o IP de IPv6 do servidor, execute o comando **ipconfig** numa janela de comandos do Windows:



Primeiro vamos criar um objeto na firewall para ser utilizado posteriormente, o IP de IPv6 do site web.

Faça login na firewall. Selecione a aba "OBJECTS" e no menu à esquerda selecione a opção "Addresses". Clique em "Add" para adicionar um objeto novo:



	D	ASHBOARD ACC	MONITOR POLICIES	OBJECTS NETWORK D	EVICE	🛓 Commit 🗸 🛛 🕞 🏎
						8
Addresses	QC					2 items
Address Groups	N	IAME	LOCATION	TYPE	ADDRESS	TAGS
Regions		p-private		IP Netmask	172.16.60.1	
Dynamic User Groups	-	and and a set of the		20100151/40185	STOCK CONTRACTO	
Applications		p-public		IP Netmask	213.13.132.96	
Application Groups						
Application Filters						
Services •						
Service Groups						
Devices						
GlobalProtect						
HIP Objects						
HIP Profiles						
External Dynamic Lists						
Custom Objects	1					
Data Patterns						
Spyware						
😟 Vulnerability						
URL Category						
Security Profiles						
👔 Antivirus						
Anti-Spyware						
Vulnerability Protection						
O URL Filtering						
File Blocking						
WildFire Analysis						
🙆 Data Filtering						
197 0 5 0 1 0	(+) Ac	id 🕞 Delete 🔞 Clor	e DF/CSV			
		05/10/0000 00.07.50	C	0.07.50		Ketter in de nele

Preencha a informação do objeto e clique em "OK":

					NETWORK	DEVICE			
		UASHDOARD ALL	MONITOR POLICIES	Objects	MEHWORK	DEVICE.			
									S ()
📮 Addresses 👘 👘	Q								$_{2 \text{ items}} \rightarrow \times$
Address Groups		NAME	LOCATION		TYPE	ADDRESS		TAGS	
Regions		gp-private			IP Netmask	172.16.60.1			
Applications	Ĩ.				IP Netmask	213.13.132.96			
Ca Application Groups									
Application Filters		_		_	_				
Services •		Address					0		
Trans		Nama	bronuer public lauf						
Devices		Description IP	6 address of web site on web0	01					
V 🧟 GlobalProtect		Time IP	Values of web site on web	01	2.02.010.2101.0	0.28/h 9/hf 208/c 285/c			
HIP Objects		type II	4C0103K		Enter an IP address	or a network using the slash notation (Ex.	. 192.168.80.150 or		
HIP Profiles					192.168.80.0/24), Y (Ex. 2001-db8-123-1	ou can also enter an IPv6 address or an II -1 or 2001 db8:123:1-/64)	Pv6 address with its prefix		
Custom Objects		Tags 4							
Data Patterns									
Spyware									
Vulnerability							OK Cancel		
URL Category		-							
Security Profiles Antivinis									
Anti-Spyware									
Ulnerability Protection									
G URL Filtering									
File Blocking									
High WildFire Analysis									
The second secon	æ.		PDF/CSV						
Internetioner Linguit Lasting	ri Time	= 05/18/2022 22:27:52 Servi	n Exoire Time: 06/17/2022	22:27:52				Z= Tasks Languag	- Maloalto

De seguida vamos criar uma regra de segurança na firewall. Selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Clique em "Add" para adicionar uma regra de segurança nova:



📾 Security 🔹	Q											$_{\rm 6items}$ \rightarrow $>$
⇒ NAT							Source			Destination		
Policy Based Forwarding		NAME	TAGS	туре	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
 Decryption Tunnel Inspection Application Override 	1	525_Allow	none	interzone	FEA S2S	any	any	any	🛤 525 🎮 Trust	any	any	any
Authentication	2	VPN_Allow	none	universal	jezaj VPN	any	any	any	122) Trust	any	any	any
🚱 SD-WAN	3	GlobalProtect Portal	none	universal	Manust 🔤	any	any	any	🚝 Untrust	gp-public	any	any
	4	Trust_to_Untrust_All	none	universal	P Trust	any	any	any	Muntrust	any	any	any
icy Optimizer —	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1+	6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
Ander Ymholia App Canada Ander Ymholia App Canada Conada C												

Preencha a informação da regra de segurança nova e no final clique em "OK":

							G ()
→ NAT					Source	Destination	
Policy Based F Decryption	Security Policy	Rule	ication Service/URL Cate	egory Actions		٢	any
Authentication	Name Rule Type Description	Webserver access universal (default) Access from Internet to web sit	e on web001				any any
Policy Optimizer	Tags Group Rules By Tag	∢ None					any
New App View Rules Without Unused Apps See Rule Usage	Audit Comment	Audit Comment Archive					
K Unused in K Unused in K Unused						 OK Cancel	
	1 01			and the second second			•





	DASHBOARD ACC MOI	NITOR POLICIES OBJECTS NETWORK DE	VICE	Commit ~ 🗗 🖣 v 🗘	2
📾 Security				G (6 items) →	ð ×
→ NAT QoS	*	Source		Destination	
Policy Based P-	Security Policy Rule			() APPLICA	TIO
Tunnel Inspect	General Source Destination Application	on Service/URL Category Actions		UTY.	
Authentication	select v	Any	any	any	
G SD-WAN		DESTINATION ADDRESS		any.	
	in a must	Webserver-public-ipvo		any	
D.B. O.B. Inc.				any	
Policy Optimizer				any	
Roles Without					
✓ ₩ Rule Usage	Add Delete	(+) Add Oelete	🕀 Add 😑 Delete		
的 Unused in 民 Unused in 民 Unused		☐ Negate		OK Cancel	
Object - Addresses		His Brack Ottobe Ottobe Marry Ottobe	SV 🗆 Michight Linger Dular 🗆 May Bulabara a	- Crowner - Breact Build Life Countries M. Country M.	
luisfrodrigues Logo	ut Last Login Time: 05/18/2022 22:27:52 Session E	xpire Time: 06/17/2022:22:27:52	an El rabalha outrara Atres El view Atricates a	SE Tasks Language W paloalt	0



Security	<u>a</u> (6	$\rightarrow \times$
Qo5				
Policy Based P	Security Policy Rule		0	APPLICATIC
🐣 Tunnel Inspec	General Source Destination Application Servic	ce/URL Category Actions		
Authentication	Any	Q	0 items) \rightarrow X	
G SD-WAN		DEPENDS ON		any
	web-browsing			any
				any
Policy Optimizer				any
Rules Without				
Unused Apps Rule Usage	🕀 Add \ominus Delete	Add To Current Rule Add To Existing Rule		
Unused in				
K Unused			OK Cancel	

THE NAT		2.274		
A QoS				
Policy Based P-	Security Policy Rule		0	APPLICAT
Tunnel Inspect				
Application O	General Source Destination Application Service/URL Category Ac	tions		
Dos Protectio	application-default 🗸	Any		
G SD-WAN	SERVICE A	URL CATEGORY A		апү
				any
alicy Optimizor				any
				any
Rules Without				
Unused Apps	(Dati Object			
Contraction Contraction	Cana Constant	O HOR O DOCKE		
B Unused in				
10 Unused			OK Cancel	



		DASHBO	DARD ACC MONITOR POLICIES OBJECTS	NETWORK DE	VICE	Conmit	। ि मि• Q उ 0
security	. 0	20					$_{6 \text{ items}} \rightarrow \times$
B NAT				Source		Destination	
Policy Based F							APPLICATIO
Decryption	Security Poli	icy Rule				0	mty
Application O	General S	ource	Destination Application Service/URL Category Actions				
Authentication	Action Setting			Log Setting			any
SD-WAN		Action	Allow 🗢		Log at Session Start		any
			Send ICMP Unreachable		Log at Session End		
				Log Forwarding	default	<u> </u>	any
	- Profile Setting			Other Settings	(3)		any
Policy Optimizer	P	Profile Type	None	Schedule OoS Marking	None	×	
New App View					Disable Server Response Inspection		anny
Unused Apps							
S Unused in						Cancel	
C Unused	1						
	1						٠
Object : Addresses	+ @	E) Add 😑	Delete (2) Clone (3) Override (2) Revert (2) Enable (3) Disable	Move Y DF/C	SV 🔝 Highlight Unused Rules 🗌 View Ruleb	ase as Groups Reset Rule Hit Col	unter * Group *

Para tornar as alterações efetivas, clique no botão "Commit" e na caixa de diálogo clique em "Commit":

	0											GO
Security =	Q				1				1			o items → X
A QoS							Source			Destination	1	
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATI
 Decryption Tunnel Inspection Application Override 	1	S25_Allow	none	Interzone	FER 525	any	any	any	929 S2S	any	any	any
Authentication	2	VPN_Allow	none	universal	PZA VPN	any	any	any	Trust	any	any	any
C SD-WAN	3	GlobalProtect Portal	none	universal	M Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_All	none	universal	Mag Trust	any	any	any	M Untrust	any	any	any
	5	Webserver access	none	universal		any	any	any	Trust	webserver-pu	any	III web-bro
Policy Optimizer	6	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
Rules Without App Controls 3	7	interzone-default	none	interzone	any	any	any	any	any	any	any	any
V ERule Usage Ku Unused in 30 days 1 Ku Unused in 90 days 1 Ku Unused 1												





Quando o Commit estiver concluído, clique em "Close":

📾 Security 🔹	Q						7 items \rightarrow >
→ NAT •			Commit Status (1)		Destination		
A QoS Policy Based Forwarding		NAME	Operation Commit	E	ADDRESS	DEVICE	APPLICA
Decryption Tunnel Inspection Decryption Tunnel Inspection Decryption Application Override Authentication Z VPN_Allow VPN_Allow Decryption CiabalDiseted British	S2S_Allow	Status Completed Result Successful Details Performing panorama connectivity check (attempt 1 of 1)	i25 Tust	any	any	any	
	VPN_Allow	Panorama connectivity check was successful for 10.16.41.194 Configuration committed successfully	Tust	any	any	any .	
SD-WAN	3	GlobalProtect Portal	Commit	Jntrust	🖕 gp-public	any	any
	4	Trust_to_Untrust_AlL		Jntrust	any	any	any
*	5 Webserver acce	Webserver access		Inust	🖕 webserver-pu	any	II web-t
icy Optimizer –	6	intrazone-default		izone)	any	any	any
Rules Without App Controls ³ Unused Apps 0	7	interzone-default			any	any	any
Rule Usage Unused in 30 days 2 Unused in 90 days 2 Unused in 90 days 2 Unused 2			<				

Para testar o acesso ao web site use um PC ligado à Internet e coloque o URL <u>http://[2a02:818:2101:c0:386b:9cbf:ae86:a856]</u> num browser. Irá aparecer a página default do IIS:



2.5. Como faço para estabelecer um Túnel VPN IPSEC entre a minha Firewall e uma Firewall remota?

A firewall Palo Alto vem com uma pré-configuração básica *ready to use* de uma VPN Site to Site.

2.5.1. Túnel VPN IPSec pelo IP público de IPv4 (só nas adesões onde este foi adquirido)

No exemplo que se segue vamos utilizar a pré-configuração do túnel VPN IPSec existente na firewall Palo Alto para ligar a nossa rede privada 172.16.2.0/24 a uma rede remota **10.50.1.0/24** ligada noutra firewall. Na nossa rede privada encontra-se um servidor com sistema operativo Windows Server 2019 e hostname web001. O servidor tem o IP 172.16.2.130 e a firewall do Windows está desligada:



400100732 - My VDC 2							Monitorização e Reporting
Web-Server Servidor ligado com aviso	Servidores / Appliances Gr	upos Re	des Recursos	Templates	ISOs	Atividades 3	Operações 🕶
Servidor / Appliance	Designação O	[Web-Server				Alterar
Armazenamento	Hostname		web001				
	Template		Windows Server 2	201 <mark>9 Standa</mark> rd E	Edition (Li	censed)	
Alertas	Grupo		Default			~	Alterar
Estatísticas	Rede		FE			~	
Histórico	Descrição	0					

A firewall remota tem o IPv4 público **194.65.28.163**. A Pre-shared Key escolhida para a configuração do túnel VPN IPSec foi **QQtC^9AbZs**. Na rede remota encontra-se um servidor Windows semelhante ao nosso, com o IP 10.50.1.130. No final iremos verificar que conseguimos pingar o servidor remoto a partir do nosso e vice-versa.

Faça login na firewall. Selecione a aba "NETWORK" e no menu à esquerda selecione a opção "Network Profiles » IKE Gateways". Clique no gateway de nome "GW-VDC1":

												60
loterfacer.	0											1 item
Zones a	4		P			1	2 12		100000			
WANS				Loc	cal Address	-	Peer ID	2753	Local ID			1
Pa Virtual Wires		NAME	PEER ADDRESS	INTERFACE	IP	ID	TYPE	ID	TYPE	VERSION	MODE	PASSIVE MC
Virtual Routers e		GW-VDC1	240.88.120.10	ethernet1/2	213.13.132.96/24					ikev2	auto	
PSec Tunnels 🔹 🔹			8									
GRE Tunnels												
g DHCP .												
DNS Proxy												
GlobalProtect												
Portals •												
Portals •												
Portals • Cateways • Cateways • Cateways •												
Portals Acceleration Content of the second												
 Portals Gateways MDM Clientless Apps Clientless App Groups 												
Portals Gateways MDM Clientless Apps Clientless App Groups QoS												
Constants Constants	•											
Ortals Ortals	•											
Portals Portals Construction Constructio												
A Portals Portals Caleways Caleways Control Control Control Contr	•											
A portals Portals A cateways A cateways MDM Clientless Apps Clientless App Groups Clientless App Groups LLDP Network Profiles A GlobalProtect IPSec Gny HKE Getways PSec Crypto PSec Crypto Network	•											
A portais Portais A portais A portais A portais A portais A portain Clientless Apps Clientless App Groups Clientless App Groups LOP LOP ClichalProtect IPSec 6n HEE Gateways A portain IPSec Crypto A IKE Crypto A IKE Crypto	•											
Apricals Apricals Apricals Apricals Apricals Apricals Apps Control Apps	•											
Contais Control Contro Control Control Control Control Control Co												
Clientless Apps Clientless Apps Clientless App Groups												
Constant Constant												
Constants Constants												



Introduza o endereço público IPv4 da firewall remota no campo "Peer Address" e a Pre-shared Key no campo respetivo. Clique em "OK":

								5 O
🕮 Interfaces 🔹 🍵	Q							1 item \rightarrow \times
Zones •		IKE Gateway			0			
Q Virtual Wires	NAME I	PEER	d Oulfare			VERSION	MODE	PASSIVE MOD
🛞 Virtual Routers 🔹 🔹	GW-VDC1	240.1 General Advance	d Options			ikev2	auto	
IPSec Tunnels *		Name	GW-VDC1					
GRE Tunnels		Version	IKEv2 only mode		~			
CHCP *		Address Type						
DNS Proxy		Interface	ethernet1/2					
Partals		Level ID Address	040 40 400 07/04					
Gateways		Local IP Address	213.13.132.90/24					
MDM		Peer IP Address Type	O IF ○ FQDN ○ Dynamic					
Sclientless Apps		Peer Address	194.65.28.163		~			
Glientless App Groups		Authentication	Pre-Shared Key Certificate					
a QoS		Pre-shared Key			1			
LLDP		Confirm Pre-shared Key						
Network Profiles		Level I de atilitation						
GlobalProtect IPSec Gr		Local Identification	None					
A IPSec Comio		Peer Identification	None					
A IKE Crypto		Comment						
Monitor .								
interface Mgmt 🔹				C ov	Canad			
R Zone Protection				OK	Cancer			
🔒 QoS Profile 🔹 🔹								
LLDP Profile								
BFD Profile								

Na firewall remota também devem ser configurados o "Peer Address" com o IP público de IPv4 da nossa firewall Palo Alto e a Pre-shared Key.

No menu da esquerda, selecione a opção "IPSec Tunnels" e clique no túnel de nome "S2S-VDC1":

		DASHBOAR	D ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE				the Co	ommit ~	ि ि ि • • • •
														G
Interfaces		Q												1 item
Zones						IKE Gatev	/av/Satellite		-		Tunnel Interfa	300		
VLANs	- 1						DEED			VIDTUAL	VIDTUAL	SECUDITY		-
Virtual Wires	- 1	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	ADDRESS	STATUS	INTERFACE	ROUTER	SYSTEM	ZONE	STATUS	COMMEN
Virtual Routers		S25-VDC1	Tunnal	Auto Key	ethernet1/2	213 13 132	194.65.28.163	A IVE Info	tunnel 10	VRouter1	vsvs1	\$25		-
IPSec Tunnels	(4)	323 7002	Info	Autoricy	concluster 2	210.10.102	174.03.20.100	INE INIO	Connectado	(Show Routes)	*3932	525		
GRE Tunnels														
DHCP	•													
DNS Proxy	- 1													
GlobalProtect	- 1													
Contrals														
Gateways														
MDM	- 1													
Clientless Apps	. 1													
Clientless Apps	oups	4												
Clientless Apps Clientless App Gro QoS	oups	4												
Clientless Apps Clientless App Gro Clientless App Gro QoS	oups	4												
MDM Clientless Apps Clientless App Gro QoS LLDP Network Profiles	oups	*												
MDM Clientless Apps Clientless App Gro QoS LDP Network Profiles GlobalProtect IPSe	oups iec Gŋ													
MDM Clientless Apps Clientless App Gro QoS LLDP Network Profiles GlobalProtect IPSo HKE Gateways	oups ec Gry e													
IMDM Image: Clientless Apps Clientless App Gree QoS LLDP Network Profiles GlobalProtect IPS Tike Gateways PISec Crypto	oups ec Gn o	4												
Clientless Apps Clientless Apps Clientless App Gro Clientless App Gro ClobalProtect IPS Hotwork Profiles GlobalProtect IPS HIE Gateways M IPSec Crypto KE Crypto	oups ec Gŋ o o	4												
(ID) MDM Clientless Apps Clientless App Gro Clientless App Gro	oups ec @ŋ e e													
Clientless Apps Clientless Apps Clientless Apps Clientless Apps Clientless Apps ClobalProtect IPs ClobalProtect IPs IKE Gateways FISec Crypto Mick Crypto Mick Crypto Mick Crypto Mick Crypto Mick Crypto Mick Crypto	oups iec Gry o o o													
Gentless Apps Clientless Apps Clientless App Gre Cos Clientless App Gre Cos Clobal Horork Profiles ClobalProfiles GlobalProfiles GlobalProfiles PiSec Crypto Monitor Monitor Zone Protection	oups iec Gry o o o	•												
Genetics Apps Clientless Apps Clientless Apps Clientless App Gre Comment Comm	oups ec Gry e e													
MDM Interfers Apps Interfers App Grid Construction Interfers	oups ec tin o o o													
Important Interface Important Important	oups ec Gry e e													



Selecione a aba "Proxy IDs", selecione a aba "IPv4" e clique em "Add" para adicionar um Proxy ID novo:

										Con	umit ~	しょう
												G ()
interfaces .	- a											1 item $\rightarrow \times$
Zones 0		IPSec Tunnel							0			
₽ VLANs										SECUPITY		
Carl Virtual Wires		General Prox	ty IDs							ZONE	STATUS	COMMENT
Virtual Routers	S25-	IPv4 IPv6								\$25		
GRE Tunnels												
E DHCP		PROXY ID		LOCAL	1	REMOTE	P	ROTOCOL	ſ			
DNS Proxy												
V GlobalProtect												
Portals •												
C MDM												
Clientless Apps												
Clientless App Groups	4											
des QoS												
LLDP												
ChalastDestart IDEes 6a												
H IKE Gateways		O Art O Dulu										
PSec Crypto e		HADD Subject										
🔒 IKE Crypto 🔹												
Monitor *								ок	Cancel			
interface Mgmt												
OoS Profession												
LLDP Profile												
BFD Profile .												
4	⊕ Add (🖯 Delete 🕜 Enable	e 🚫 Disable 🕼	PDF/CSV								
Tuisfrodrigues Logout Last Log	gin Time: 05/1	8/2022 22:27:52 5	ession Expire Time	06/17/2022 22:27:52						j⊟ Tasks	Language	и paloalto

Preencha o campo "Proxy ID" com "SA1", o campo "Local" com a nossa rede privada 172.16.2.0/24, o campo "Remote" com a rede remota 10.50.1.0/24 e clique em "OK":

DASHBOARD				
				S ()
Mail Interfaces C. IPSec	Tunnel	0		$1 \text{ term} \rightarrow X$
Contract Wires	ral Proxy IDs			ATUS COMMENT
IPv4	IPv6			
€ DHCP +	Proxy ID	© cor		
DHS Provy Contain Contain Contain Contain Contain Contain Contains App Groups Contentses App Groups Contains App Groups	Proxy ID SA1 Local 172.16.2.0/24 IP Address or IP/netmask, only needed when peer requires Remote 1050.10/24 IP Address or IP/netmask, only needed when peer requires Protocol Any	sik.		
Control Profiles A GlobalProtect IPSec En.	ОК	Cancel		
IKE Gateways IPSex Crypto IKE Crypto Monitor Monitor Tone Protection Go Shofte ELEP Profe Intel Profe Intel Profe		CK Cancel		
∢ ⊕Add ⊝Delete	Enable Disable PDF/CSV		1- a.e.	

Na firewall remota também deve ser feita esta configuração do Proxy ID "SA1", mas colocando como "Remote" a nossa rede 172.16.2.0/24.



Caltice							Co	mmit ~	
									S ()
Interfaces							_		1 item → X
Zones			IPSec Tunnel				0		
្វាភ្លៃ VLANs							and the second se		
Virtual Wires			General Proxy IDs				ZONE	STATUS	COMMENT
Virtual Routers		5254	The second second				\$25	-	
0 IPSec Tunnels			IPv4 IPv6					10001	
GRE Tunnels			PROXY ID	LOCAL	REMOTE	PROTOCOL			
THE DIS DISK	181		SA1	172.16.2.0/24	10.50.1.0/24	any			
V GlobalProtect									
Portais									
Gateways									
MDM									
Clientiess Apps									
🖏 Clientless App Gr	oups	8							
A QoS									
LLDP									
V La Network Profiles									
GlobalProtect IPS	ec an						-		
A IDEac Comto			(+) Add (-) Delete						
A IKE Counto									
Monitor						OK Cance	4		
interface Mgmt						Contraction of the second			
Zone Protection									
& QoS Profile									
LLDP Profile									
- BFD Profile									
4 ((+) Add (😑 Delete 🕜 Enable 🚫 Dis	able 🔘 PDF/CSV					
histodringes Locout L	ast Lon	in Time: 05/1	18/2022 22:27:52 Session Ex	pire Time: 06/17/2022 22:27:52			g= Tasks	Language	Mpaloalto

Clique em "OK" para fechar o diálogo de configuração do túnel IPSec:

É necessária uma rota estática no Virtual Router para encaminhar o tráfego com destino à rede remota 10.50.1.0/24 pela interface do túnel IPSec.

Para este túnel IPSec "S2S-VDC1" já se encontram pré-configuradas rotas estáticas IPv4 no Virtual Router "VRouter1" da firewall de modo a encaminhar o tráfego com destino às gamas de endereçamento privado IPv4 10.0.0.0/8 e 192.168.0.0/16 pela interface "tunnel.10".

Podem ser consultadas selecionando na aba "NETWORK" » opção "Virtual Routers" do menu à esquerda » VRouter1 » Static Routes » IPv4:

										6 0
real interfaces a ≜ Q PR Zones a	Virtual Route	Virtual Router	Static Route	- IPv4 (Read	Only)			?	00	1 Hem → ×
VLATH: By Vraual Wreel Vraual Wreel Vraual Wreel Vraual Wreel Vraual Wreel Vraual Wreel Vraual Wreel Difference Difference Difference Difference Vraual ClobaliProtect Vraual ClobaliProtect Vraual ClobaliProtect Vraual ClobaliProtect (PBec Rp) T MC Cartways Vraual ClobaliProtect (PBec Rp) T MC Cartways Vraual Vraual ClobaliProtect (PBec Rp) T MC Cartways Vraual	View Router Settings Static Routes Redistribution F RIP OSPF- OSPF-3 BGP Multicast.	Name Destination Interface Next Hop Admin Distance BFD Profile BFD Profile Path Monitoring Failure NAME	Rede_Remota_S25 10.0.00/6 tunnel.10 None 10.240 10 Unicast Disable BFD Condition © Kong Kong ENABLE ENABLE	10000,8	Preemptive Hole DESTINATION IP	Time (min) 2 PING INTERVALISEC	PING COUNT		3 items) → X ROUTE TABLE unicast unicast unicast	More Panding Stats
luis-f-rodrimesietelecom.pt Logsut										



É também necessária uma regra de segurança a permitir o tráfego da VPN entre a nossa rede local e a rede remota. Já se encontra previamente configurada uma regra de segurança para este túnel IPSec "S2S-VDC1", sendo apenas necessário ativá-la.

Selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Selecione a regra de segurança pré-configurada de nome "S2S_Allow" clicando sobre o número dela (1). Clique em "Enable" para ativar a regra:

	0											(items)
Security	4	1	8	1	1				-			
QoS					-		Source			Destination	_	
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATI
Decryption	1	S2S_Allow	none	Interzone	122 S25	any	any	any	152 5	any	any	any
Application Override					Trust				Trust			
Authentication (王 DoS Protection G SD-WAN	2	VPN_Allow	none	universal	jezej VPN	any	any	any	Trust	any	any	any
	3	GlobalProtect Portal	none	universal	Mag Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_All	none	universal	Ma Trust	any	any	any	P2 Untrust	any	any	any
cy Optimizer —	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
icy Optimizer –	6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
Rules Without App Controls Mused Apps Rule Usage Sulfused in 30 days Mused in 90 days Unused												
												1

Na firewall remota também deve haver uma regra semelhante para permitir o tráfego do túnel VPN IPSec para a rede 10.50.1.0/24 e vice-versa.

Para tornar as alterações efetivas, clique no botão "Commit" e na caixa de diálogo clique em "Commit":



Security =	2											6 items → >
→ NAT •							Source			Destination		
 QoS Policy Based Forwarding 		NAME	TAGS	ТҮРЕ	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICA
Decryption Tunnel Inspection Application Override Authentication DoS Protection	1	S25_Allow	none	interzone	F29 525	any	any	any	1929 S2S	any	any	any
Authentication	2	VPN_Allow	none	universal	PER VPN	any	any	any	122 Trust	any	any	any
(E Das Pratection	3	GlobalProtect Portal	none	universal	🚧 Untrust	any	any	any	🚝 Untrust	🖕 gp-public	any	any
	4	Trust_to_Untrust_All	none	universal	PP Trust	any	any	any	M Untrust	any	any	any
olicy Optimizer —	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1+	6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
Window Window App Controls 5 Winsed Apps 0 Winsed in 30 days 1 Window 1 no 0 days 1 Window 1 no												

									iommit ~	
😂 Security	. 0	0					-11			$\begin{array}{c} & \textcircled{\bullet} \\ & \textcircled{\bullet} \\ & \textcircled{\bullet} \\ & & \textcircled{\bullet} \\ & & & \end{matrix}$
	=		Commit			0 🗖		Destination		
 QoS Policy Based Forwarding 		NAME	Doing a commit will overwrite the running	g configuration with the	e commit scope.			ADDRESS	DEVICE	APPLICATIO
Tunnel Inspection	1	S25_Allow	COMMIT SCOPE	langes made by (1) has	LOCATION TYPE		5	any	any	ату
Application Override			policy-and-objects				st			
Authentication	2	2 VPN_Allow	device-and-network				st.			
SD-WAN	c1.	GlobalProtect Portal					trușt	🔁 gp-public	any	arry
	Å	Trust_to_Untrust_All.,					trușt.	any	any	any
Policy Optimizer -		intrazone-default					Sinc)	any	any	any
Rules Without App Controls	+ 4	5 interzone-default						any	any	any
Unused Apps			Review Changes 🖉 Change Su	ummary 🛃 Validate	Commit	Group By Location Type				
✓ Ξ Rule Usage			Note: This shows all the changes in login admit	n's accessible domain.						
Chused in 90 days			Description							
						Commit Cancel				
	×									
Object : Addresses -	+ 0	Add ODelete OC	Clone 🙁 Override 🔍 Revert 🥥 Enat	ble 🚫 Disable M	ove * PDF/CSV	Highlight Unused Rules 🗌 Vi	ew Ruleba	se as Groups Rese	et Rule Hit Counte	r * Group * »
luisfrodrigues Logout Last Lo	gin Tir	me: 05/18/2022 22:27:5	52 Session Expire Time: 06/17/2022 22	:27:52				注 Tas		🊧 paloalto

Quando o Commit estiver concluído, clique em "Close":



Para testar o túnel VPN IPSec, fazemos login no servidor web001 da nossa adesão e verificamos que conseguimos pingar o servidor remoto com o IP 10.50.1.130:



Em sentido inverso, a partir do servidor remoto, verificamos que também conseguimos pingar o nosso servidor web001:

🥠 paloalto





Para verificar o estado do túnel VPN IPSec na firewall Palo Alto, selecione a aba "NETWORK" e no menu à esquerda selecione a opção "IPSec Tunnels". Um semáforo de estado na cor verde significa que o túnel está estabelecido corretamente entre os dois peers:

		DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE				Com	imit ~	b Er• Q
														G ()
Interfaces o	* C	2												1 item) $\rightarrow \times$
Zones 0			1			IKE Gatev	vav/Satellite				Tunnel Interf	ace		
VLANs							PEER	1		VIRTUAL	VIRTUAL	SECURITY	-	_
Virtual Wires	0	NAME	STATUS	TYPE	INTERFACE	LOCAL IP	ADDRESS	STATUS	INTERFACE	ROUTER	SYSTEM	ZONE	STATUS	COMMENT
Virtual Routers	C	S25-VDC1	Tunnel	Auto Key	ethernet1/2	213.13.132	194.65.28.163	IKE Info	tunnel.10	VRouter1	vsys1	\$25		
IPSec Tunnels =			Info							(Show Routes)				
GRE Tunnels														
DIS DIS Desire														
V GlobalProtect														
Portals														
Gateways .														
MDM														
Clientless Apps														
Clientless App Groups														
🐣 QoS														
👷 LLDP														
V 🕞 Network Profiles														
🙆 GlobalProtect IPSec @ry	5.C													
H IKE Gateways														
DiPSec Crypto 🔹														
🗄 IKE Crypto 🔹														
Monitor •														
Interface Mgmt •														
Zone Protection														
Cos Profile														
RED Profile														
	*			O Disable	PDF/CSV									
4)	0		Comple	C cronnie (91017034		2212231	_						And the second second
Construction	• (€ Add) Delet	e 🕜 Enable	S Disable (PDF/CSV	06/11/2022 23:	07:48					ž= Taske	5 Language	₩ paloalto



2.5.2. Túnel VPN IPSec pelo IP de IPv6

No exemplo que se segue vamos utilizar a pré-configuração do túnel VPN IPSec existente na firewall Palo Alto para ligar a nossa rede interna 2a02:818:2101:c0::/64 a uma rede remota **2a02:818:2101:40::/64** ligada noutra firewall. Na nossa rede interna encontra-se um servidor com o IP de IPv6 2a02:818:2101:c0:386b:9cbf:ae86:a856.

A firewall remota tem o IP de IPv6 **2a02:818:2101::40**. A Pre-shared Key escolhida para a configuração do túnel VPN IPSec foi **QQtC^9AbZs**. Na rede remota encontra-se um servidor Windows semelhante ao nosso, com o IP de IPv6 2a02:818:2101:40:9d1c:30f4:4dcc:13f1. No final iremos verificar que conseguimos pingar o servidor remoto a partir do nosso e vice-versa.

Faça login na firewall. Selecione a aba "NETWORK" e no menu à esquerda selecione a opção "Network Profiles » IKE Gateways". Clique no gateway de nome "GW-VDC1":

			DASHBOARD	ACC MON	ITOR POLI	CIES OBJECTS	NETWORK	DEVICE				Commit ×	৳ ₩- Q
													G (?)
Interfaces		Q											1 item) $\rightarrow \times$
Zones		-			Loci	al Address	Po	er ID		Local ID			
VLANs		m	NAME	PEER ADDRESS	INTERFACE	IP	ID	ТУРЕ	ID	TYPE	VERSION	MODE	PASSIVE MODE
Virtual Wires			GW-VDC1	240.88.120.10	ethernet1/2	213 13 132 96/24		10000			ikey2	auto	
Virtual Routers			GWYDCI	240.00.120.10	culemeta/2	213.13.132.70/24					INCV2	3010	
GPE Tunnels													
S DHCP													
TONS Proxy													
V 🚱 GlobalProtect	- 1												
🚯 Portals													
🚑 Gateways	•												
MDM [
Clientless Apps													
Clientless App Gro	oups	9											
S QoS	- 1												
ELLDP	- 1												
ClabelPosteet IDC													
E IKE Cotemans	ec on												
A IPSec Crypto													
A IKE Crypto													
Monitor													
🐼 Interface Mgmt													
Zone Protection	- 1												
🚴 QoS Profile													
5 LLDP Profile													
BFD Profile		4											۲
4	~ ×	()	Add 🕞 Delete (🧭 Enable 🚫 Dis	able	SV.							
luisfrodrigues Logout Li	ast Logi	n Time	:: 05/18/2022 22:	:27:52 Session Exp	nire Time: 06/17/	2022 22:27:52					śΞ	lasks Language	🥠 paloalto

Selecione o "Address Type" IPv6, selecione o "Local IP Address" IPv6 da ethernet1/2, introduza o endereço IP de IPv6 da firewall remota no campo "Peer Address" e a Pre-shared Key no campo respetivo. Clique em "OK":



Na firewall remota também devem ser configurados o "Peer Address" com o IP de IPv6 da nossa firewall Palo Alto e a Pre-shared Key.

No menu da esquerda, selecione a opção "IPSec Tunnels" e clique no túnel de nome "S2S-VDC1":

			DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE				🛔 Cor	nmit 🗸	৳ ᡛ∎◄ Q
	_														G (?
Interfaces		Q													1 item \rightarrow >
Zones						1	IKE Cotor	vov/Sotollito				Tunnel Interf	200		
VLANs								arra	1	-	10000000		an cumunu	1	
Q Virtual Wires			NAME	STATUS	TYPE	INTERFACE	LOCAL IP	ADDRESS	STATUS	INTERFACE	ROUTER	SYSTEM	ZONE	STATUS	COMMENT
Virtual Routers	•		\$25-VDC1	Tunnel	Auto Key	ethernet1/2	2:02:818:21	2=02-818-21	A IVE loto	tunnel 10	VRouter1	veve1	\$25		
1 IPSec Tunnels	0	-1	525 4001	Info	Auto Key	culcificiti'i	2802.010.21	2802.010.21	TKE INIO	connici. 10	(Show Routes)	*3931	525		
GRE Tunnels															
₫ DHCP	•														
DNS Proxy															
GlobalProtect															
Contrais Contrained Portains	•														
Gateways	0														
MDM															
Clientless Apps															
Clientless App Group	15														
🐣 QoS															
tldp 👷															
 Network Profiles 															
GlobalProtect IPSec	6ŋ														
Ħ IKE Gateways	•														
IPSec Crypto															
B IKE Crypto															
🖰 Monitor															
interface Mgmt															
R Zone Protection															
& QoS Profile															
LLDP Profile															
H BFD Profile	. 🗔														
	. *	(+)	Add Delet	e 🕢 Enable	O Disable	PDF/CSV									
	P	0	and a second	Contraction of the second	0										

Selecione o "Address Type" IPv6 e selecione a "IKE Gateway" GW-VDC1. A seguir selecione a aba "Proxy IDs":

empresas

//\=



Caltice				the Co	nmit ~	
						50
Interfaces	= 9	_				1 item $\rightarrow \times$
Zones II		IPSec Tunnel	(
ញ្ញិត្ត VLANs				SECURITY		
Pa Virtual Wires		General Prox	y IDs	ZONE	STATUS	COMMENT
Virtual Routers	525	Nama	\$25.VDC1	\$25		
CPC Tunnels		Tunnel Interface	tuninal 10	-		
- DHCP		Tunnel Interface				
DNS Proxy		Type	O Auto Key 🕧 Manual Key 💮 GlobalProtect Satellite			
V GlobalProtect		Address Type	IPv4 O IPv6			
Portals		IKE Gateway	GW-VDC1 v	1		
Gateways a		IPSec Crypto Profile	Sulte-B-GCM-256			
MDM			Show Advanced Ontions			
Clientless Apps		Comment		1		
Clientless App Group:						
S QOS						
V P Network Profiles			Cancel	2		
GlobalProtect (PSec @				-		
H IKE Gateways						
🔒 IPSec Crypto 🔹						
🔂 IKF Crypto 🔹						
Monitor ·						
interface Mgmt 4						
Zone Protection						
QoS Profile						
CLUP Profile						
	· DAdd	Dalata (2) Escible	O Deable @ PDF/CSV			
	CT MOD					
						🥢 paloalto

Selecione a aba "IPv6" e clique em "Add" para adicionar um Proxy ID novo:

							Comr	nit ~	
									50
Interfaces	10.2	- Q.							1 item) \rightarrow \times
Zones		1	PSec Tunnel			0			
ក្ខត្តិ VLANs							SECURITY		
Virtual Wires		NAM	General Proxy IDs				ZONE	STATUS	COMMENT
Virtual Routers	•	S25-	IPv4 IPv6				\$25		
CRF Tunnels		_							
€ DHCP			PROXY ID	LOCAL	REMOTE	PROTOCOL			
DNS Pressy									
V 🥵 GlobalProtect									
Portals	141								
Gateways									
Glientless Apps									
Clientless App Gro	oups	4							
🚴 QoS 🕎 LLDP									
V C Network Profiles									
GlobalProtect IP56	ec Gry								
H IKE Gateways			Add Delete						
PSec Crypto									
IKF Crypto									
Interface Mont						Cancel			
Zone Protection									
QoS Profile									
LLDP Profile									
De BED Profile									
4	-	⊕ Add ⊖	Delete 🕢 Enable 🚫 Disable 🔞 P	PDF/CSV					
luisfrodrigues Logout Li	ast Log	gin Time: 05/18/	2022 22:27:52 Session Expire Time: (06/17/2022 22:27:52			≸⊟ Tasks	Language	🊧 paloalto

Preencha o campo "Proxy ID" com "SA1", o campo "Local" com a nossa rede interna 2a02:818:2101:c0::/64, o campo "Remote" com a rede remota 2a02:818:2101:40::/64 e clique em "OK":



C altice								
🖼 interfaces 🔹 🖒								1 item) -> X
74 Zones ·		IPSec Tunnel				0		
VLANK.							SECTIONTY.	
Re Virtual Wires		General Proxy IDs					ZONE	
Virtual Routers	525-1	IPv4 IPv6					\$25	
A CET Tropple	_		_				_	
# DHCP		PROXY ID	Proxy ID V6		?	COL		
2 DNS Proxy								
V 🥵 GlobalProtect			Proxy ID	SA1				
Portals +			Local	2a02:818:2101:c0::/64				
Gateways =				IP Address or IP/netmask, only needed when peer require	is it.			
			Remote	2a02:818:2101:40::/64				
Clientless Apps				IP Address or IP/netmask, only needed when peer require	5 n.			
Clientess App Groups	4		Protocol	Any	~			
Co Libe				ок	Cancel			
C GlobalProtect IPSec 60								
H IKE Gateways *		Add Dalata						
🖨 IPSec Crypto 👘 🖷								
🙆 IKE Crypto 🔹								
Monitor +						OK Cancel		
interface Mgmt +								
Zone Protection								
Qo5 Profile								
ES LLDP Profile								
Te BFD Profile								
	(Add (🕘 Delete 🕑 Enable 🚫 Di	sable () PDF/CSV					
luistredvicues Logout List Ligin								2 paloalto

Na firewall remota também deve ser feita esta configuração do Proxy ID "SA1", mas colocando como "Remote" a nossa rede 2a02:818:2101:c0::/64.

				4					G (?)
interfaces									1 item) -> >
Pa Zones			IPSec Tunnel				0		
P VLANs									
C Virtual Wires			General Proxy IDs				ZONE	STATUS	COMMENT
Wirtual Routers		525	Construction				\$25	-	
IPSec Tunnels			IPv4 IPv6					The set	
GRE Tunnels			PROXY ID	LOCAL	REMOTE	PROTOCOL			
E DHCP	141		SA1	2a02:818:2101:c0:/64	2a02:818:2101:40::/64	any			
ClobalProtect									
A Portais	100								
Gateways									
MDM									
Clientless Apps									
Clientless App Gr	sups								
🚴 QoS									
S LLDP									
✓ C Network Profiles									
GlobalProtect IPS	ec Gin								
T IKE Gateways	181		(+) Add (-) Delete						
🖻 IPSec Crypto									
KE Crypto	141								
🔂 Monitor						ОК Са	icel		
interface Mgmt									
Zone Protection									
QoS Profile									
LLDP Profile									
WE BED Profile		0	Der Der Gener						
4	×.	(Add	🕞 Delete 🅑 Enable 🚫 Disab	le (PDF/CSV					

Clique em "OK" para fechar o diálogo de configuração do túnel IPSec:

Para que o tráfego com destino à rede remota 2a02:818:2101:40::/64 seja corretamente encaminhado pelo túnel IPSec é necessário adicionar uma rota estática no Virtual Router.

No menu da esquerda, selecione a opção "Virtual Routers" e clique no router de nome "VRouter1":



	DASHBOARD ACC	MONITOR POLICIES C	BJECTS NETWOR	K DEVICE			L Commit ∽	în ⊡r Q
								50
🚥 Interfaces 🔹 📥 🖸	2							1 item $\rightarrow \times$
Zones •		FACES CONFIGURATION	RIP	OSPF	OSPFV3	BGP	MULTICAST	RUNTIME STATS
WLANS Image: Second	VRouter1 ethem ethem ethem ethem ethem ethem ethem	et1/1 Static IPv6 Routes: 1 et1/2 Static Routes: 3 et1/3 ECMP status: bhadhed et1/4 et1/6 et1/6						More Runtime Stats
Gateways Gateways Gateways Clentless Apps Clentless App Groups Clentless App Groups Qos ClabalProtect IPSec En Fice Gateways GlabalProtect IPSec En Fice Gateways ClabalProtect IPSec En Fice Gateways Fice Ga	⊕ Add ⊝ Delete @ PDF/CS	/						

Selecione a opção "Static Routes", selecione a aba "IPv6" e clique em "Add" para adicionar uma rota nova:

Models Note Router Settings IPv4 IPv6 MultiCast Nove Ruitine Virtual Wires Virtual Routers Item -> × Item -> × Item -> × MultiCast MultiCast Nove Ruitine IPsc: Toranels Item -> × Item -> × Item -> × Item -> × MultiCast MultiCast MultiCast MultiCast MultiCast MultiCast Item -> × Item -> × MultiCast MultiCast MultiCast Item -> × MultiCast MultiCast MultiCast MultiCast MultiCast MultiCast MultiCast Item -> × MultiCast MultiCast MultiCast Item -> × MultiCast MultiCast Item -> × MultiCast MultiCast Item -> × MultiCast Item -> × MultiCast Item -> × MultiCast Item -> × Item -> ×	1000	· AC	Virtual Router - VR	oute	r1								0 🗆		1 item) →
Windlewiders Redistribution Profile Place Tounels RiP DISP Tounels RiP OSPF OSPF OSPF OSPF3 BGP Datatic Ospertates BGP Multicast BGP Multicast Multicast Olienties Apps Multicast Olienties Apps Multicast Model Protect Place (in) Multicast Milticast Multicast Milticast Multicast	VLANs		Router Settings Static Routes	IPv	14 IPv6									MULTICAST	RUNTIME STATS
Chicke OSFF CohadProtect BCP Multicast Multicast CheadProtect BCP Multicast CheadProtect Condemark Condemark <	Virtual Routers PSec Tunnels GRE Tunnels		Redistribution Profile	20				No	ext Hop				1 item $\rightarrow \times$		
QSPFV3 BCP Consultivation Multicast Citerations Appo	DHCP		OSPF		NAME	DESTINA	INTERFA	туре	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE		
	GlobalProtect		OSPFv3 BGP		Default- IPV6	::/0	ethernet1	ipv6- address	2a02:818	default	10	None	unicast		
Study ChaliProtect PSec 6in THKE Gateways ThKE Gateways ThKE Crypto ThKE Crypto ThKE Crypto ThKE Crypto	Clientless App Gr Clientless App Gr Clientless App Gr Clientless App Gr	sups	Multicast												
KECrypto Monitor															
OK Cancel	 LLDP Network Profiles 	c 6ŋ													

Dê um nome à rota, introduza a rede destino (2a02:818:2101:40::/64), a interface por onde deve ser encaminhado o tráfego (tunnel.10, a interface associada a este túnel IPSec), e como Next Hop coloque "None" (a interface tunnel.10 não tem um IP associado). Clique em "OK":



Clique em "OK" para fechar o diálogo de configuração do Virtual Router:

Interfaces		<u>a</u>	Virtual Router - VR	oute	er1	_	_	_	_	_	_	_	08		$(G \otimes I)$
VLANs VITual Wires Ortual Routers	8		Router Settings Static Routes Redictribution People	IP	v4 IPv6								2 items $\rightarrow \times$	MULTICAST	RUNTIME STATS
IPSec Tunnels OF Tunnels	141		Redistribution Frome		1	1		Ne	ext Hop				T		
DHCP	-		OSPF		NAME	DESTINA	INTERFA	түре	VALUE	ADMIN DISTANCE	METRIC	BFD	ROUTE TABLE		
✓ € GlobalProtect			OSPFv3		Default- IPV6	::/0	ethernet1	ipv6- address	2a02:818	default	10	None	unicast		
Portals Gateways Gateways MDM Clentless Apps Clentless App Gro Go Clentless App Gro Clentless A	e ups c Gry		BGP Multicast		\$25- VDC1_2a	2a02:818	tunnel.10			default	10	None	unicast		
IKE Gateways IPSec Crypto IKE Crypto IKE Crypto Monitor Monitor				(Add 🗇 Del	lete 🔞 Cloi	ne					ок	Cancel		
QoS Profile					-	-	-		-	-	-				

De seguida vamos ativar a regra de segurança que irá permitir o tráfego da VPN entre a nossa rede local e a rede remota.

Selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Selecione a regra de segurança pré-configurada de nome "S2S_Allow" clicando sobre o número dela (1). Clique em "Enable" para ativar a regra:



NAME 1 \$25_Allow 2 VPN_Allow 3 GlobalProtect Portal 4 Trust_to_Untrust_All 5 intrazone-default.	TAGS none none none none none none	TYPE Interzone universal universal universal universal	ZONE PPI 525 PPI Trust PPI VPN PPI Untrust PPI Trust	ADDRESS any any any	Source USER any any any	any any any	ZONE PPR S25 PPR Trust PPR Trust PPR Untrust	Destination ADDRESS any any Egg pp-public	DEVICE any any any	APPLICATIOn any any any any
NAME 1 S25_Allow 2 VPN_Allow 3 GlobalProtect Portal 4 Trust_to_Untrust_All 5 intrazone-default	TAGS none none none none none none	TYPE Interzone universal universal universal	ZONE PRR 525 PRR Trust PRR VPN PRR VPN PRR VPN PRR Trust	ADDRESS any any any	USER any any any	any any any	ZONE PERI 525 PERI Trust PERI Untrust	ADDRESS any any any gp-public	any any any	APPLICAT any any any
1 S25_Allow 2 VPN_Allow 3 GlobalProtect Portal 4 Trust_to_Untrust_All 5 Intrazone-default.	none none . none . none	Interzone universal universal universal	PER S25 PER Trust PER VPN PER Untrust PER Trust	any any any	any any any	any any any	PPA S25 PPA Trust PPA Trust PPA Trust PPA Untrust	any any Gruppepublic	any any any	any any any
2 VPN_Allow 3 GlobalProtect Portal 4 Trust_to_Untrust_All 5 intrazone-default	none none none none	universal universal universal	Pa Untrust	any any	any any	any any	🚝 Trust 🎮 Untrust	any C gp-public	any any	any any
GlobalProtect Portal Trust_to_Untrust_All intrazone-default	. none	universal	Ma Untrust	any	any	any	M Untrust	📮 gp-public	any	any
4 Trust_to_Untrust_AlL 5 intrazone-default	. none	universal	M Trust							
5 intrazone-default	none			any	any	any	M Untrust	any	any	any
		intrazone	any	any	any	any	(intrazone)	any	any	any
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any
*										

Na firewall remota também deve haver uma regra semelhante para permitir o tráfego do túnel VPN IPSec para a rede 2a02:818:2101:40::/64 e vice-versa.

Para tornar as alterações efetivas, clique no botão "Commit" e na caixa de diálogo clique em "Commit":

	0											GO
Security =	Q		r						1			o items → X
A QoS							Source			Destination	1	
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIO
Decryption	1	S2S_Allow	none	interzone	P24 S2S	any	any	any	22 525	any	any	any
Application Override					P24 Trust				🚧 Trust			
Authentication	2	VPN_Allow	none	universal	PER VPN	any	any	any	1929 Trust	any	any	any .
SD-WAN	3	GlobalProtect Portal	none	universal	M Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_AlL	none	universal	Ma Trust	any	any	any	Market Contrust	any	any	апу
icy Optimizer —	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1+	6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
Control of the second												



Security										6 items $\rightarrow X$
3+ NAT			Commit			08				
A QoS S Policy Based Forwarding		NAME	Doing a commit will over	write the running configur	ation with the commit scope.			ADDRESS	DEVICE	APPLICATIO
Decryption	1	\$25 Allow	COMMIT SCOPE		LOCATION TYPE	INCLUDE IN COMMIT				any
Tunnel Inspection			policy-and-objects				et.			
Authentication	2		device-and-network				ar.			
E DoS Protection	-	Circle Day of Day of Day								
SD-WAN	-3		1				trust	gp-public	any	any
	4	Trust_to_Untrust_All					trust	any	any	any
Policy Ontimizer	5	intrazone-default					sine)	any	any	any .
New App Viewer	1+ 6	Interzone-default						any	any:	any
Rules Without App Control	0		Preview Changes	E Change Summary	Validate Commit	Group By Location Type				
V ;= Rule Usage	1		Note: By default, this show commit	s all the changes by selected	admins in login admin's accessible	domain. Admins may choose some of them to				
Unused in 90 days	4		Description							
A CONTRACT										
						Commit Cancel				

Quando o Commit estiver concluído, clique em "Close":

Caltice		DASHBOARD ACC	C MONITOR POLICIES OBJECTS NETWORK DEVICE			Get Ge	mmit 🗸	। हि सि• Q
								G ()
Security *	Q							$_{6 \text{ items}} \rightarrow \times$
→ NAT •			Commit Status	1		Destination		
QoS Solicy Based Forwarding		NAME	Operation Commit	1	E	ADDRESS	DEVICE	APPLICATIO
Decryption Tunnel Inspection Application Override	1	S2S_Allow	Status Completed Result Successful Details Partial changes to commit: changes to configuration by administrators: kiis-f-rodrigues@telecom.pt		325 Trust	any	any	any
Authentication	2	VPN_Allow	Changes to configuration in device and network Changes to policy and objects configuration	. 1	Tust	any	any	any :
SD-WAN	3	GlobalProtect Portal	Performing pannama connectivity check lattermpt.1 of 1) Pannama connectivity check was successful for 10.16.41.194 Configuration committed successfully		Jntrust	👰 gp-public	any	any
	4	Trust_to_Untrust_AlL.	Commit	_	Jntrust	any	any	any
Policy Optimizer -	5	intrazone-default			izone)	any	any	any
New App Viewer 1+	6	interzone-default				any	any	any
Rules Without App Controls 3 Unused Apps 0 Rule Usage Nused in 90 days 1 Nused in 90 days 1 Nused in 90 days 1	- 0							•
Object : Addresses +	\oplus	Add 😑 Delete 🔞 Clo	ne 💿 Override 🐵 Revert 🥑 Enable 🚫 Disable 🛛 Move 🖌 🔞 PDF/CSV 🗌 Highlight Unused Rules	s 🗌 '	√iew Ruleb	ase as Groups Rese	t Rule Hit Cour	nter Y Group Y
luis-f-rodrigues@telecom.pt Log		Last Login Time: 05/12/2	022 18:59:50 Session Expire Time: 06/11/2022 23:07:48			≸≘ Tas	ks Language	🋷 paloalto

Para testar o túnel VPN IPSec, fazemos login no servidor web001 da nossa adesão e verificamos que conseguimos pingar o servidor remoto com o IP 2a02:818:2101:40:9d1c:30f4:4dcc:13f1:





Em sentido inverso, a partir do servidor remoto, verificamos que também conseguimos pingar o nosso servidor web001:

	connecteu (enci) preu) to				Cond Car abor
2	📧 Administrator: Command Prompt	-	×		
Recycle Bin			^		
	C:\>ipconfig				
	Windows IP Configuration				
	Ethernet adapter Ethernet0:				
	Connection-specific DNS Suffix .: TPU6 Address : 2a02:818:2101:40:0d1c:30f4:4dcc:13f1				
	Link-local IPv6 Address : fe80::9d1c:30f4:4dcc:13f1%11				
	Subnet Mask				
	Default Gateway : fe80::250:56ff:feb5:35f1%11 10.50.1.1			and the second sec	
	C. L. Noing 6 2002 949 2401 - 0 2066 - 0-6 - 0066 - 0066				
	C. () Jing -0 2802.010.2101.00.000.9001.800.8000				
	Pinging 2a02:818:2101:c0:386b:9cbf:ae86:a856 with 32 bytes of data: Reply from 2a02:818:2101:c0:386b:9cbf:ae86:a856: time=1ms			_	
	Reply from 2a02:818:2101:c0:386b:9cbf:ae86:a856: time<1ms Reply from 2a02:818:2101:c0:386b:9cbf:ae86:a856: time<1ms				
	Reply from 2a02:818:2101:c0:386b:9cbf:ae86:a856: time<1ms				
	Ping statistics for 2a02:818:2101:c0:386b:9cbf:ae86:a856:				
	Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:				
	Minimum = 0ms, Maximum = 1ms, Average = 0ms				
	C: \>		~		
H <i>X</i>				^ @ ₽ 4	10:55
					19/05/2022

Para verificar o estado do túnel VPN IPSec na firewall Palo Alto, selecione a aba "NETWORK" e no menu à esquerda selecione a opção "IPSec Tunnels". Um semáforo de estado na cor verde significa que o túnel está estabelecido corretamente entre os dois peers:



		DASHBOARD	ACC	MONITOR	POLICIES	OBJECTS	NETWORK	DEVICE				G Cor	nmit 🗸 🕴	ቬ ∰∗ ቢ
														G ()
Interfaces	0													1 item $\rightarrow \times$
Zones o			1			IVE Catou	um/Satellite				Tunnel Interf	200		
💑 VLANs						Ince Gates	nay/ satemice			10071101	initial interi	acc	-	_
Contract Vires		NAME	STATUS	TYPE	INTERFACE	LOCAL IP	ADDRESS	STATUS	INTERFACE	ROUTER	SYSTEM	ZONE	STATUS	COMMENT
Virtual Routers •		\$25-VDC1	Tunnel	Auto Key	ethernet1/2	2a02-818-21	2=02-818-21	A IVE Info	tunnel 10	VRouter1	vsvs1	\$25	(III)	
1 IPSec Tunnels =		525 4002	Info	Auto (kc)	contractara	2002.010.21	2002.010.21	INC INC	conner.20	(Show Routes)	13932	525		
GRE Tunnels														
E DHCP 0														
DNS Proxy														
V 🥵 GlobalProtect														
Portals e														
Gateways •														
C MDM														
Clientless Apps														
Clientless App Groups	4													
Cab Natural Deptiles														
ClobalProtect IPSec En														
HIE Cateway														
A IPSec Comto														
A IKE Comito														
A Monitor														
Interface Memt														
Zone Protection														
A QoS Profile #														
LLDP Profile														
BED Profile .														
	\oplus	Add 🕞 Delet	e 🕢 Enable	🚫 Disable 🕼	PDF/CSV									
luisfrodrigues Logout Last Logi	n Tim	e: 05/18/2022	22:27:52 Se	ssion Expire Tim	e: 06/18/2022 1	0:27:53						≸⊞ Task	s Language	и paloalto

NOTAS:

As definições relativas às Fases 1 e 2 de estabelecimento de um túnel IPSec podem ser consultadas na aba "NETWORK" e nas seguintes opções do menu à esquerda:

- 11. Fase 1
 - 1. "Network Profiles | IKE Gateways"
 - 2. "Network Profiles | IKE Crypto"
- 12. Fase 2
 - 1. "IPSec Tunnels"
 - 2. "Network Profiles | IPSec Crypto"

Os eventos relacionados com VPNs podem ser consultados na aba "MONITOR" » opção "Logs | System" do menu à esquerda.



2.6.1. VPN GlobalProtect pelo IP público de IPv4 (só nas adesões onde este foi adquirido)

empresas

Nas adesões em que foi adquirido um IP público de IPv4, a firewall Palo Alto vem com uma pré-configuração básica *ready to use* do portal e gateway GlobalProtect, que é a solução do fabricante Palo Alto para as VPNs Client to Site.

No exemplo que se segue a nossa firewall Palo Alto tem o IP público de IPv4 213.13.132.96 e vamos utilizar a pré-configuração existente na firewall para ligar um PC cliente com Internet, por VPN, à rede privada 172.16.2.0/24 da adesão. Nesta rede privada encontra-se um servidor privado com sistema operativo Windows Server 2019 e hostname web001. O servidor tem o IP 172.16.2.130 e a firewall do Windows está desligada. No final iremos estabelecer uma sessão de Remote Desktop Connection para este servidor:

Soluções Cloud			O			Olá, L	uis Manuel Filipe L Rodrigues 💄 Q
Adesão: 400100732 - My VDC 2			unite				Monitorização e Reporting
Servi	idores / Appliances G	rupos Red	les Recursos	Templates	ISOs	Atividades 3	
••• Web-Server •• Servidor ligado com avisos 172.16.2.130							Operações 🕶
Servidor / Appliance	Designação 🚯		Web-Server				Alterar
Armazenamento	Hostname		web001				
	Template		Windows Server	2019 Standard I	Edition (Li	censed)	
Alertas	Grupo		Default			~	Alterar
Estatísticas	Rede		FE			~	
Histórico	Descrição		ina.				Alterar

Vamos ativar a conta de VPN pré-configurada para fazer login no Portal e no agente GlobalProtect. Faça login na firewall. Selecione a aba "DEVICE" e no menu à esquerda selecione a opção "Local User Database » Users". Clique na conta "vpnuser":





Ative a conta ("Enable"), altere a password e clique em "OK":

			Contraction of the Contraction o	
				G ()
Setup • • C				1 item) $\rightarrow \times$
Config Audit	7 NAME		LOCATION	ENAB
Administrators	Vonser			
Authentication Profile	. Partment			
Authentication Sequences				
El User Identification =				
WM Information Sources				
Response Pages =	Local User		()	
Ci Log Settings			(c))	
V Le Server Profiles	Name	vpnuser		
U SNMP Trap	Mode	Password O Password Hash		
Systog •	Password			
	Confirm Password			
C Netflow		Z Enable		
RADIUS		Cardona Co.		
TACACS+ +				
LDAP			Cancel	
Rerberos			_	
SAML Identity Provider				
Multi Factor Authentica				
V III Local User Database				
Contraction of the Contraction o				
Scheduled Los Expert				
Co Software				
GlobalProtect Client				
Dynamic Updates				
•	PAdd Delete Clone PDF/CSV			
luis-f-rodrigues@telecom.nt Logout				🚝 Tasks 🗌 Language 🛛 🍪 paloaito'

Agora selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Selecione a regra de segurança pré-configurada de nome "VPN_Allow" clicando sobre o número dela (2). Clique em "Enable" para ativar a regra:

14.04.2025



🖽 Security	0											$6 \text{ items} \rightarrow \times$
⇒ NAT							Source			Destination		
QoS Policy Based Forwarding		NAME	TAGS	туре	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICAT
 Decryption Tunnel Inspection Application Override 	1	S25_Allow	none	Interzone	म्बन् S.25 म्बन् Trust	any	any	any	昭和 S2S 昭和 Trust	any	any	any
Authentication	2	VPN_Allow	none	universal	PZN VPN	any	any	any	Trust	any	any	any
C SD-WAN	3	GlobalProtect Portal	none	universal	Mag Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_Allow	none	universal	Ma Trust	any	any	any	🚝 Untrust	any	any	any
olicy Optimizer	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1	+ 6	interzone-default	none	interzone	any	any	any	any	any	any	any	any
La Rules virtifioù App Controls 元 Unused Apps ○ 元 Rule Usage 感 Unused in 30 days 感 Unused Unused	0											

Para tornar as alterações efetivas, clique no botão "Commit" e na caixa de diálogo clique em "Commit":

												G ()
🖾 Security	Q	<u></u>	-									6 items → X
DoS							Source			Destination		
Bolicy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIO
 Decryption Tunnel Inspection Application Override 	1	S25_Allow	none	Interzone	FER S2S	any	any	any	FEE S25	any	any	any
Authentication	2	VPN_Allow	none	universal	P2 VPN	any	any	any	Mar Trust	any	any	any
SD-WAN	3	GlobalProtect Portal	none	universal	M Untrust	any	any	any	M Untrust	gp-public	any	any
	4	Trust_to_Untrust_All	none	universal	M Trust	any	any	any	M Untrust	any	any	any
Policy Optimizer -	5	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any
New App Viewer 1	6	interzone-default	none	interzone	any.	any	any	any	any	any	any	any
Control of the set of the se												





Quando o Commit estiver concluído, clique em "Close":

🔛 Security 🔹	Q							$_{6 \text{ items}} \rightarrow \times$
→ NAT 0			Commit Status (0		Destination		
Policy Based Forwarding		NAME	Operation Commit	*	E	ADDRESS	DEVICE	APPLICAT
 Decryption Tunnel Inspection Application Override 	1	525_Allow	Status Completed Result Successful Pacific Durity learners to complete hances to configuration by administratory, bit if adding of the own at		i25 Tust	any	any	any
Authentication	2	VPN_Allow	Details Partial changes to commit changes to computation by administrators: hits-t-roongues@telecom.pt Changes to policy and objects configuration Performing ranormar connectivity, check (attempt 1 of 1)		īrust	any	any	any
SD-WAN	3	GlobalProtect Portal	Parrorama connectivity check was successful for 10.16.41.194 Configuration committed successfully		Jntrust	🔁 gp-public	any	any
	4	Trust_to_Untrust_AlL		-	Jntrust	any	any	any
licy Optimizer —	5	intrazone-default		1	izone)	any	any	any
New App Viewer 1+	6	interzone-default				any	any	any
Unused Apps 0 Rule Usage Unused in 30 days 1 Curved in 90 days 1 Curved in 90 days 1 Curved in 90 days 1			+ Close					

Abra uma janela de browser e introduza o URL com o seu IP Publico IPv4 da adesão no seguinte formato <u>https://IPv4PublicodaAdesao:4443</u> (exemplo:

<u>https://213.13.132.96:4443</u>). O browser irá indicar que a ligação não é privada. Isto deve-se ao certificado do portal ter sido emitido por uma Root CA self signed da própria firewall:







Para que os browsers deixem de apresentar este aviso e para o correto funcionamento posterior do agente GlobalProtect é necessário guardar o certificado da Root CA self signed

na pasta dos Trusted Root Certification Authorities do PC cliente. Clique no aviso **A** Inseguro que se encontra à esquerda do URL e de seguida clique em "O certificado não é válido":





Selecione a aba "Certification Path", selecione o certificado "4235B0AB-41F5-5D05-42EC-0A9BF2C319B5.cloudwall.local" e clique em "View Certificate":

General	Details	Certification Path	
Certif	ication pa	th	
	4235B0A	8-41F5-5D05-42EC-0A9BF2C319B 3.132.96	5.cloudwall.local
6		ſ	View Certificate
Certific This C/	ate <u>s</u> tatu A Root ce	s: rtificate is not trusted because it is thorities store	not in the Trusted Root

Selecione a aba "Details" e clique em "Copy to File...":

Show: All> Field Value Version V3 Serial number 00896ff995bd50 1bef Signature algorithm sha256RSA Signature hash algorithm 19 de maio de 2022 02:51:19 Valid from 19 de maio de 2023 02:51:19 Valid to 19 de maio de 2023 02:51:19 Subject 4235BDAB-41F5-5DD5-42EC-0 Valid to 19 de maio de 2023 02:51:19 Copy to File	cricical	Details	Certification Pat	1	
Field Value Version V3 Serial number 00896ff995bd501bef Signature algorithm sha256RSA Signature hash algorithm sha256 Issuer 4235B0AB-41F5-5D05-42EC-0 Valid from 19 de maio de 2022 02:51:19 Valid to 19 de maio de 2023 02:51:19 Subject 4235B0AB-41F5-5D05-42EC-0	how:	<all></all>		~	
Edit Properties Copy to File	Field Ve Se Sig Sig Iss Va Va	rsion rial numbe gnature al nature ha suer lid from hiect	er gorithm ash algorithm	Value V3 00896ff995bd501bef sha256RSA sha256 4235B0AB-41F5-5D05-42EC-0 19 de maio de 2022 02:51:19 19 de maio de 2023 02:51:19 4235B0AB-41E5-5D05-42EC-0	~
				Course Els	2





Irá ser executado o Certificate Export Wizard. Clique em "Next":

🗧 🐓 Certificate Export Wizard	~
Welcome to the Certificate Export Wizard	
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
To continue, dick Next.	
<u>N</u> ext Cance	el 👘

Selecione a opção "Base-64 encoded X.509 (.CER)" e clique em "Next":

xport File For Certifica	ormat tes can be exported in a variety of file formats.
Select t	ne format you want to use:
O	ER encoded binary X,509 (.CER)
• B	ase-64 encoded X.509 (.CER)
00	ryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
	Indude all certificates in the certification path if possible
OB	ersonal Information Exchange - PKCS #12 (.PFX)
I	Include all certificates in the certification path if possible
	Delete the private \underline{k} ey if the export is successful
	Export all extended properties
I	Enable certificate privacy
ON	licrosoft Serialized Certificate S <u>t</u> ore (.SST)



Escolha a pasta e o nome do ficheiro para onde será exportado o certificado e clique em "Next":

-	Certificate Export Wizard	
1	File to Export	
	Specify the name of the file you want to export	
-		
	File pame:	
	C:\//sers/vntc031\/Deskton\PA Boot CA self signed cer	Browse
	er pacia (picos) peakop (Artobi ex acit alginearter	browse
		Vext Cancel

Clique em "Finish" para exportar o certificado:

You have	successfully completed the Certificate	Export wizard.
File Nam	e	C:\Users\xptc031\Desktop\PA Root (
Export k	eys	No
Include	all certificates in the certification path	No
File Forn	lat	Daseon Encoded X.309 (",CEP)



Se o seu PC cliente fizer parte de um domínio, poderá dar-se a situação de não ter privilégios para executar os passos de importação do certificado indicados a seguir. Se assim for, fale com o administrador do domínio Windows em que o seu PC se insere para ultrapassar a situação.

Abra a pasta para onde foi exportado o certificado e clique duas vezes no mesmo para o abrir. De seguida, clique em "Install Certificate":

• n	te Information
This CA Root ce install this certi Authorities stor	rtificate is not trusted. To enable trust, ficate in the Trusted Root Certification 'e.
Issued to:	423580AB-41F5-5D05-42EC-0A9BF2C319B5.dou dwall.local
Issued by:	423580AB-41F5-5D05-42EC-0A9BF2C319B5.dou dwall.local
Valid from	19/05/2022 to 19/05/2023

Irá ser executado o Certificate Import Wizard. Escolha a certificate store que mais se adeque ao seu caso, neste exemplo foi escolhida a certificate store do "Current User". Clique em "Next":





Clique em "Browse" para escolher a store para onde vai ser importado o certificado:

Certificate Store				
Certificate	tores are system areas v	vhere certificates	are kept.	
Windows ca	n automatically select a c	ertificate store, o	r you can specif	y a location for
	ue. Natically select the certifi	cata atora bacad .	on the type of c	ortificato
Auto	all certificates in the follo	unios store	on the type of t	el uncate
Cert	ficate store:	wing store		
	neare store.			Browse
17				

Selecione a store "Trusted Root Certification Authorities" e clique em "OK":



1	Personal	~
	Trusted Root Certification Authorities	
	Enterprise Trust	
- 2	Intermediate Certification Authorities	
	Trusted Publishers	-
	Untrusted Certificates	×.

Clique em "Next":

INEO empresas

	differente Channe
G	Certificate stores are system areas where certificates are kept.
	Windows can automatically select a certificate store, or you can specify a location for the certificate. O Automatically select the certificate store based on the type of certificate Place all certificates in the following store
	Certificate store: Trusted Root Certification Authorities Browse

Clique em "Finish" para concluir o processo de importação:





Ser-Ihe-á apresentado um aviso de segurança. Clique em "Yes" para aceitar os riscos inerentes e importar o certificado:

ecurity	Warning
Δ	You are about to install a certificate from a certification authority (CA) claiming to represent:
	4235B0AB-41F5-5D05-42EC-0A9BF2C319B5.cloudwall.local
	Windows cannot validate that the certificate is actually from "4235B0AB-41F5-5D05-42EC-0A9BF2C319B5.cloudwall.local". You should confirm its origin by contacting "4235B0AB-41F5-5D05-42EC-0A9BF2C319B5.cloudwall.local". The following number will assist you in this process:
	Thumbprint (sha1): 07A0BE31 D2F94724 765A5A77 C8667C29 AF088181
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
	Do you want to install this certificate?
	Yes No

Clique em "OK" para fechar as caixas de diálogo que ainda se encontrem abertas.

Carregue no botão de refresh do browser. Agora já será apresentada a página do portal GlobalProtect sem o aviso A Inseguro, tendo este sido substituído por um cadeado (- indica que a ligação é segura):

14.04.2025



Introduza as credenciais da conta vpnuser e carregue em "LOG IN":

🍪 GlobalProtect Portal 🗙 🕂			V		-	đ	×
← → C ☆		@ ☆		*	2	J 🧒	:
	GlobalProtect Portal						
	vpnuser						
	LOG IN						

É apresentada uma lista de agentes GlobalProtect para descarregar e instalar. Descarregue o que corresponder à versão do sistema operativo instalado no seu PC cliente:

) empresas



Clique duas vezes no agente que acabou de descarregar para iniciar a instalação e prossiga pelos menus clicando em "Next" até ficar concluída.

Após o agente GlobalProtect ter sido instalado com sucesso no PC cliente irá aparecer o ícone

na taskbar do Windows juntamente com uma janela de diálogo do agente a pedir a introdução do endereço do portal. Preencha com o IP:porto **213.13.132.96:4443** e clique em "Connect":



De seguida introduza as credencias da conta vpnuser e clique em "Sign In":

empresas





O agente irá estabelecer a VPN e apresentará a seguinte mensagem de sucesso:



Agora vamos ligar-nos remotamente ao servidor virtual da adesão a partir do PC cliente. Abra a aplicação de Remote Desktop Connection e preencha os campos com o IP do servidor remoto – 172.16.2.130 – e o User name da conta pretendida para login. Clique em "Connect":



Introduza a password da conta que pretende usar para fazer login no servidor e clique em "OK":

Remote Decision Connection	- 1
S Remote Desktop Connection	
Remote Desktop	
Connection	
Windows Security	
Enter your credentials	
,	
These credentials will be used to conne	ect to 172.16.2.130.
Administrator	
More choices	
more enoices	
ОК	Cancel
	aline all and all all all all all all all all all al

Sessão RDC estabelecida entre o PC cliente e o servidor privado web001 através da VPN GlobalProtect:





2.6.2. VPN GlobalProtect pelo IP de IPv6

A firewall Palo Alto do serviço Servidores Privados da Cloud MEO só suporta VPNs Client to Site em IPv4 e só para clientes Windows e Mac. IPv6 e clientes Linux e Mobile (Android, iOS) não é suportado, nestas situações deverá contactar o seu agente comercial MEO para mais informações.

2.7. Que configurações devo alterar antes de remover um IP da minha Firewall?

A remoção de um IP público de IPv4 da firewall Palo Alto implica ter de remover previamente a menção a esse IP de todas as configurações onde ele esteja presente, sob risco de criar uma inconsistência na configuração global da firewall e não ser possível gravar a configuração e torná-la efetiva.

Sítios comuns na configuração da firewall (mas não exaustivos) onde são usados IPs públicos de IPv4 são os seguintes:





Regras de segurança (ACL) - aba "POLICIES", opção "Security";

Regras de NAT - aba "POLICIES", opção "NAT";

		DASHBOARD A		OR POLI	CIES OBJEC	CTS NETWOR	RK DEVICE			t c	ommit ~ C	. F∃ < Q
												G 🕐
Security 0	Q											7 items \rightarrow \times
→ NAT 0							Source			Destination		
Policy Based Forwarding		NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATIC
Decryption						(m)						000
Application Override Authentication	H											
DoS Protection	- 81				and the second s				(meneric			
	-31	-		1.000	-					-		
Policy Optimizer -			1.000	1000		in.						100
Rules Without App Controls	-101			-					-			
Kule Usage Unused in 30 days	I			and a								
Unused in 90 days 1												
								1 P. 1 P. 1 . 1 P		C D		•
Object : Addresses +			Jone - xo) Overrid	e ip Revert	Contactor of the second	Lasable Move *	WPDF/CSV	Hignlight Unused F	cules 🔄 view Ruleba	se as Groups Res	et kule Hit Counter	 Group * >>
luistrodrigues Logout Last Log	ini l'ini	e: 06/08/2022 15:31:4	45 Session Expire	: Time: 07/22/	2022 23:40:58					s≞ las	ts Language 🛷	paloalto

VPNs Site to Site - aba "NETWORK", opção "IKE Gateways";

									G 🕐
C Interfaces	100	Q(INC Colores						1 item \rightarrow \times
Zones			IKE Gateway			U			
VLANs Can Virtual Wires			General Advanced	Options			VERSION	MODE	PASSIVE MOD
S Virtual Routers	140	2	40. Nama				ikev2	auto	
(IPSec Tunnels			Warne	urs and much					
GRE Tunnels			version [REV2 only mode		×			
1 DHCP			Address Type	IPv4 () IPv6					
DNS Proxy			Interface e	ethernet1/2		<i>\u016</i>			
GlobalProtect			Local IP Address	213.13.132.96/24		~			
Gateway			Peer IP Address Type						
Cateways Cateways			Poor Address	240 89 1 20 10					
Clientless Apps			Peer Address	40.00.120.10		×			
Clientless App Gr	oups		Authentication	Pre-Shared Key () Certificate	20				
🚓 QoS			Pre-shared Key						
ELDP			Confirm Pre-shared Key						
			Local Identification	None	~				
尚 GlobalProtect IPS	ec Gry		Peer Identification	None	~				
H IKE Gateways									
D IPSec Crypto			Comment						
IKE Crypto									
Interface Memt					0	K Cancel			
Zone Protection									
QoS Profile									2
LLDP Profile		0.000							t.

Se o IP que estiver a ser removido for o último IP público de IPv4 da firewall esta passa a ter apenas endereçamento IPv6. As seguintes ações são executadas automaticamente:

Desativação do DHCP;

Remoção da regra NAT da zona Trust para a zona Untrust;





Alteração da pré-configuração básica *ready to use* da VPN Site to Site para usar IPv6 (IKE gateway "GW-VDC1" e IPSec Tunnel "S2S-VDC1").

2.8. Onde posso encontrar mais informação soobre como configurar a minha Firewall?

A firewall Palo Alto vem ela própria com páginas de ajuda bastante completas. Sempre que vir o símbolo (2) presente nas caixas de diálogo (tipicamente no canto superior direito) pode clicar para obter ajuda relevante para as configurações em causa.

O fabricante Palo Alto disponibiliza ainda online manuais completos de administração da firewall. Os manuais são atualizados à medida que a versão do software da firewall evolui, sendo sempre possível consultar o manual referente à versão de software específica da sua firewall:

PAN-OS® Administrator's Guide

PAN-OS® Networking Administrator's Guide

GlobalProtect Administrator's Guide

2.9. Como posso saber as Características Técnicas/ Funcionalidades da minha Firewall?

Na seguinte tabela estão enumeradas as caraterísticas técnicas / funcionalidades – disponíveis e não disponíveis – da firewall Palo Alto.

Características da Firewall PALO ALTO disponibilizada nos Servidores Privados						
Firewall	s	Nativa Palo Alto e como opção Firewall de Data Center				
Endereçamento IP	s	IPv4/IPv6 (IPv4 opcional) Endereçamento IPv4/IPv6 publico dos servidores privados, restrito à plataforma dos servidores privados.				
Interfaces de rede por servidor	s	Se for IPv4; um endereçamento privado Se for IPv6 deixam de existir redes privadas do cliente. Todas as redes e VMs passam a ter endereçamento público				
Firewall com planeamento de regras	s	É possível efetuar a calendarização de regras de firewall para alturas especificas e com duração pré-determinada.				



Diagnóstico	s	Estão acessíveis através da interface de administração web, diversas ferramentas que facilitam o diagnóstico de situações excecionais, e que apoiam no despiste da configuração dos diversos serviços que não estejam a produzir o efeito desejado.
DHCP Server and Relay	s	Servidor de DHCP para a(s) rede(s) interna(s) do Virtual Data Center (IPv4) SLAAC Stateless Address Auto-configuration (IPv6)
IPv4 VPN IPSec (Client to Site) C2S e (Site to Site) S2S	s	O tráfego ao ser cifrado na Palo Alto perde cerca de 25% da largura de banda contratada. Suporte IPv4 em VPN Client to Site apenas para SO Windows e MAC. Uso do cliente Palo Alto GlobalProtect. *GlobalProtect IPv6 não suportado. *Linux e Mobile não suportado. Implicam transição para serviço FW de Data Center
NAT	s	Sim em IPv4. Em IPv6 todos os endereçamentos são públicos
Largura de banda	s	Largura de banda partilhada com 20/50 ou 100 Mbps Largura de banda dedicada opcionalmente
Debito máximo	s	Da FW Palo Alto (nativa) para a Internet 100 Mbps
Acessos Remotos	s	Até 10 VPN (Client to Site) e 5 IPSec (Site to Site)
Interface de Administração	s	A interface de administração permite uma experiência de utilização facilitada
Dashboard	s	A Palo Alto disponibiliza um dashboard que permite de forma rápida perceber o seu estado de funcionamento.
IPv6	s	A Firewall Palo Alto suporta IPv6, estando desde já disponível a configuração na(s) rede(s) interna(s) do VDC
Relatórios e Monitorização	s	A firewall disponibiliza diversos mecanismos de reporting, com possibilidade de fazer drill down no detalhe dos gráficos e exportar a informação
Políticas com App Control	s	As políticas de segurança podem ser aplicadas às aplicações NOTA: a MEO só dá apoio nas policies L4 e não aplicacionais
Policies com GeoLocation	s	Políticas baseadas nos IPs/Localizações/País
		Encaminhar pedidos de DNS das redes internas para outro servidor de DNS. Suportado, mas não configurado. Os servidores Internos têm de ser configurados com os IPs dos DNS tipificados para a Palo Alto
DNS Forwarder	S	IPV4: "PublicIPv4PrimaryDNS": "62.28.116.41", "PublicIPv4SecondaryDNS": "62.28.40.173", IPV6: "PublicIPv6PrimaryDNS": "2a02:818:2010:5041:0:0:0:d001", "PublicIPv6SecondaryDNS": "2a02:818:2021:6041:0:0:0:d00"
OpenVPN	Ν	Acesso remoto com funcionalidade OPENVPN



Dynamic DNS	N	Serviço DNS dinâmico na Internet com publicação de um nome associado ao IP público da VFW (virtual firewall) do VDC
DNS Server	N	Funcionamento de DNS server para redes internas do VDC dado pela VFW
Load Balancing	N	O balanceamento de carga para servidores internos requer a contratação de serviços de balanceamento específicos
IPSec C2S- Linux + Android *	N	Suporte IPv4 em VPN Client to Site para Linux e Android. GlobalProtect IPv6. Requer licenciamento específico e subscrição de serviço FWDC.
IPS/IDS- Anti-Bot, Antivírus	N	IPS/IDS-Sistema de deteção e Proteção de Intrusão requer licenciamento específico e subscrição de serviço FWDC
URL Filtering	N	Filtragem ao URL ou categorias de URL
Content Filtering + SSL Inspection	N	Filtragem de conteúdos- Regras que conseguem filtrar o conteúdo de uma página Web SSL Inspection permite interpretar conteúdos cifrados em SSL
SSL VPN	Ν	Acesso remoto por SSL VPN https:// ao IP da VFW + porto
SD-WAN	Ν	Não está disponível embora apareça na VFW para configuração
DOS Protection	Ν	Não está disponível embora apareça na VFW para configuração
QOS	Ν	Não está disponível embora apareça na VFW para configuração
Policy Based Forwarding	Ν	Não está disponível embora apareça na VFW para configuração

Legenda:

S – Disponível

N - Indisponível ou requer licenciamento não suportado nesta versão da FW