Servidores Privados
Manual Firewall Palo Alto

MEO empresas

14.04.2025

Índice

1. Introdução

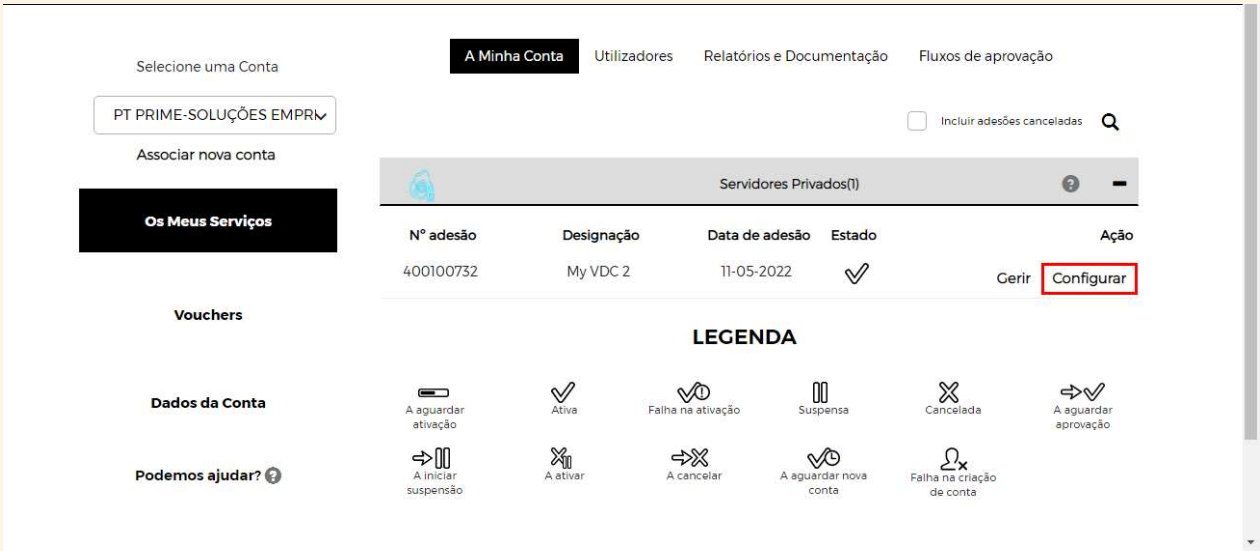
Este documento pretende responder às perguntas mais frequentes – FAQ – sobre a configuração da firewall Palo Alto do serviço Servidores Privados da Cloud MEO Empresas.

2. FAQ

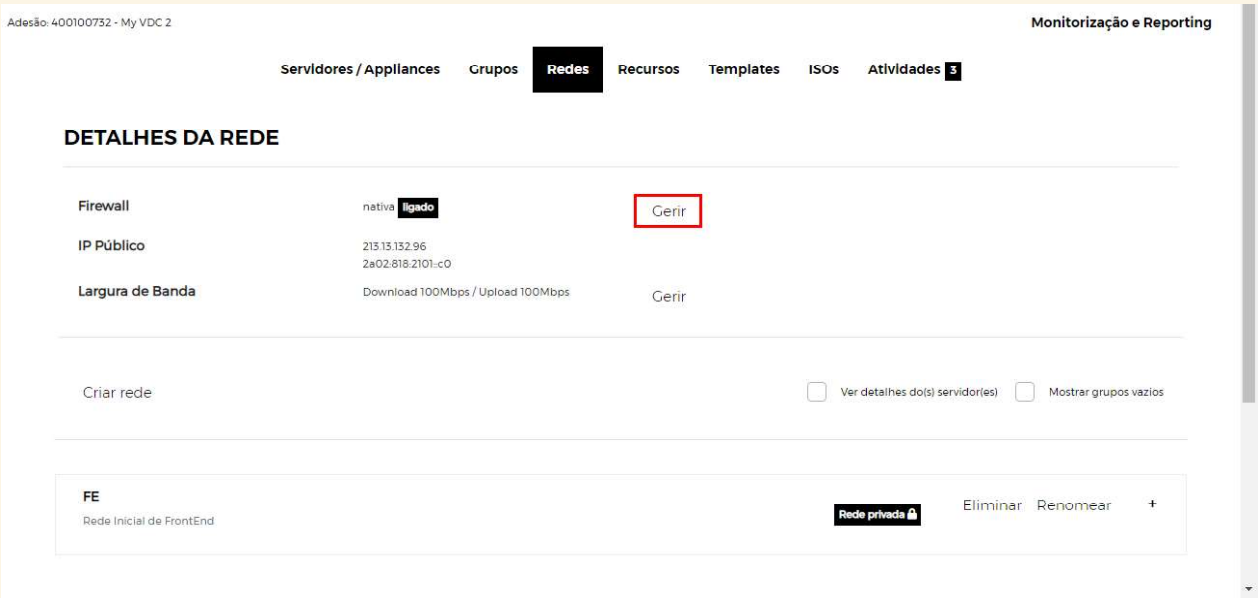
2.1. Como faço para aceder à Interface de gestão da Firewall Palo Alto?

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.

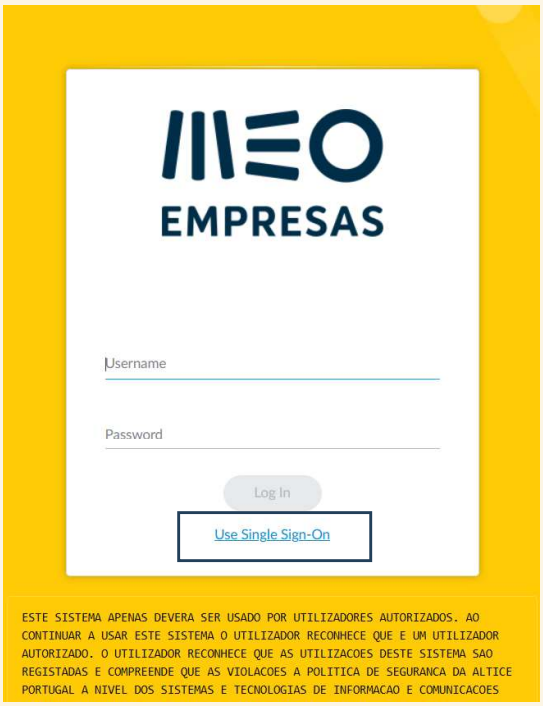
Faça Login no portal cloud.meoempresas.pt com as suas credenciais de cliente MEO, procure a sua adesão de servidores privados na lista e clique em "Configurar":

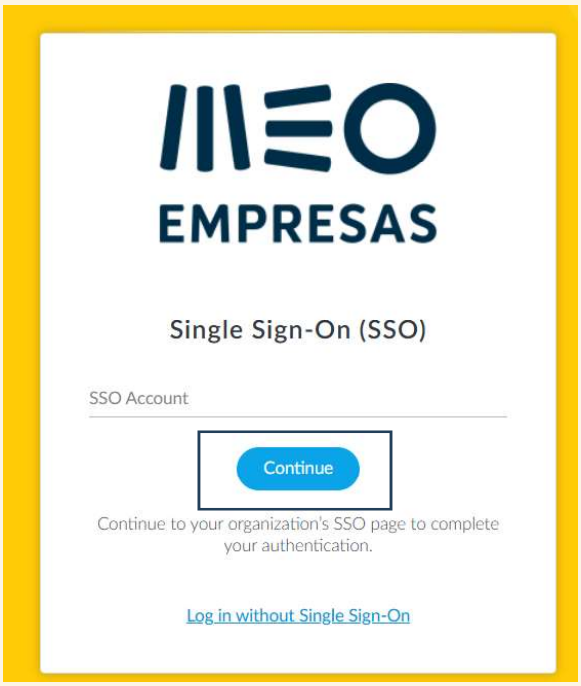


Na aba “Redes” e clique em “Gerir”:

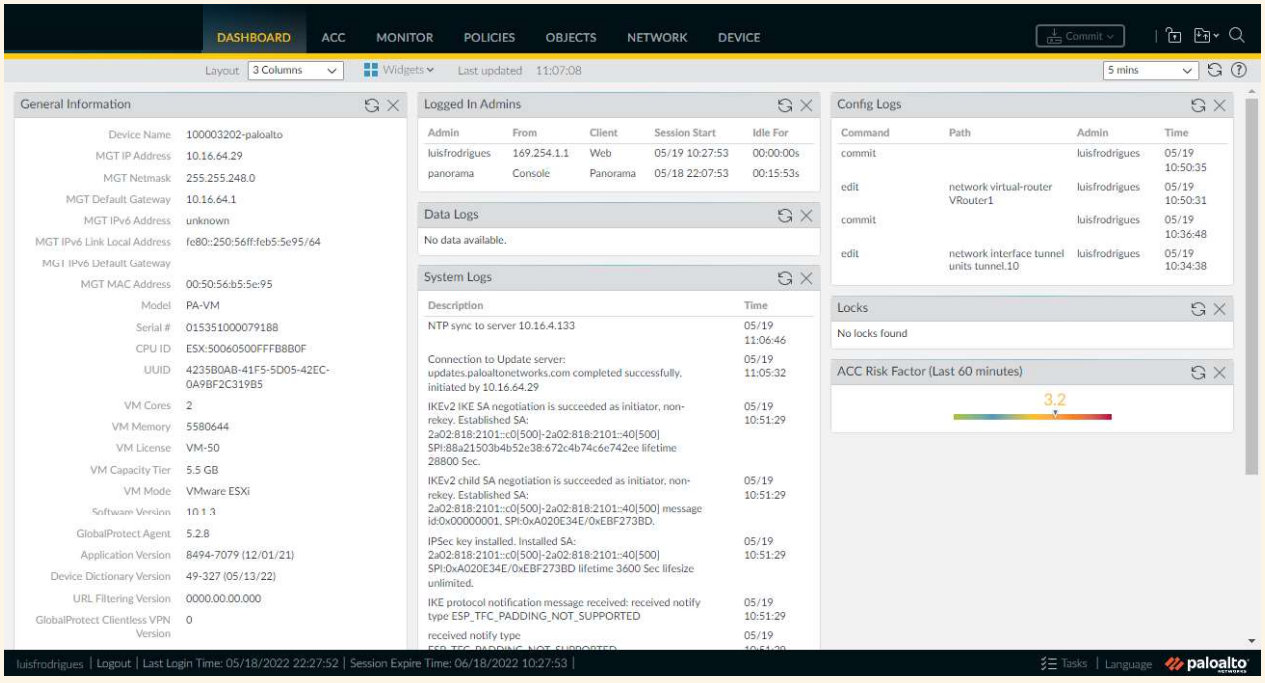


Clique no Link “Use Single Sign-On” e, de seguida, clique em “Continue”:





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:



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.

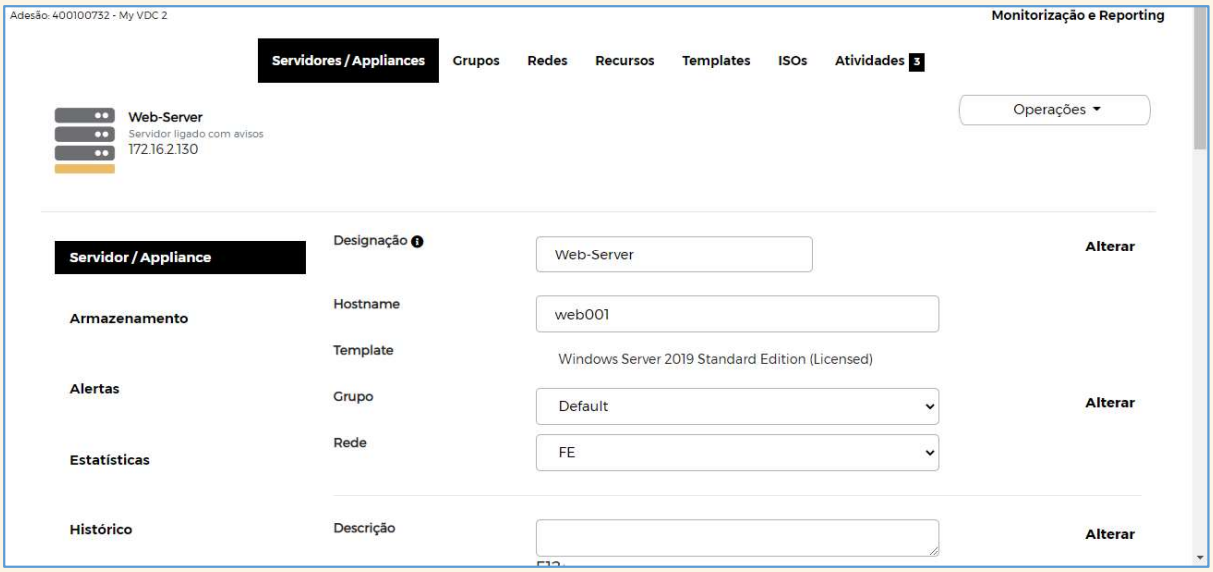
Nas adesões em que foi adquirido um IP público de IPv4, a firewall vem com a seguinte zona adicional:

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

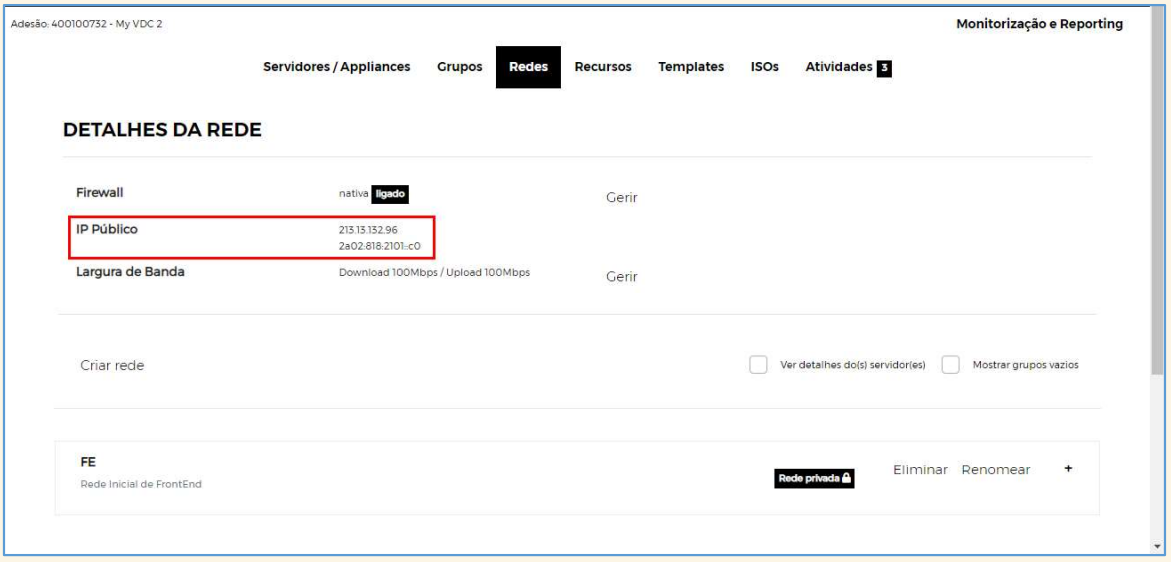
2.4. Como faço para publicar na Internet um WEB SITE alojado num Servidor Privado da minha Adesão?

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:

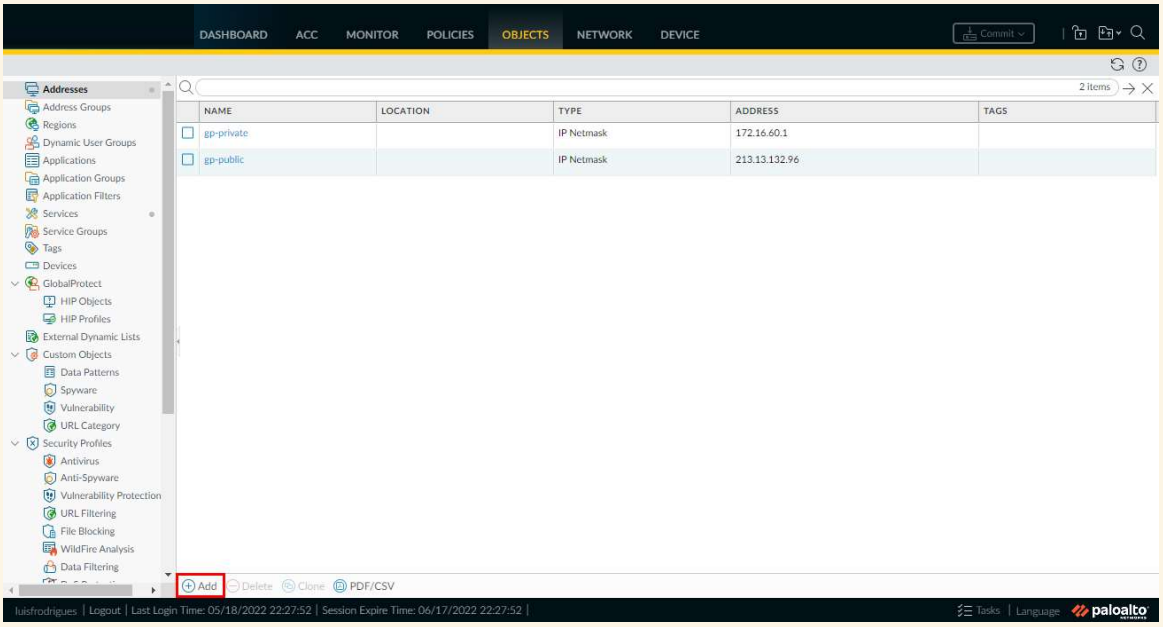


A nossa firewall Palo Alto tem o IP público de IPv4 213.13.132.96:

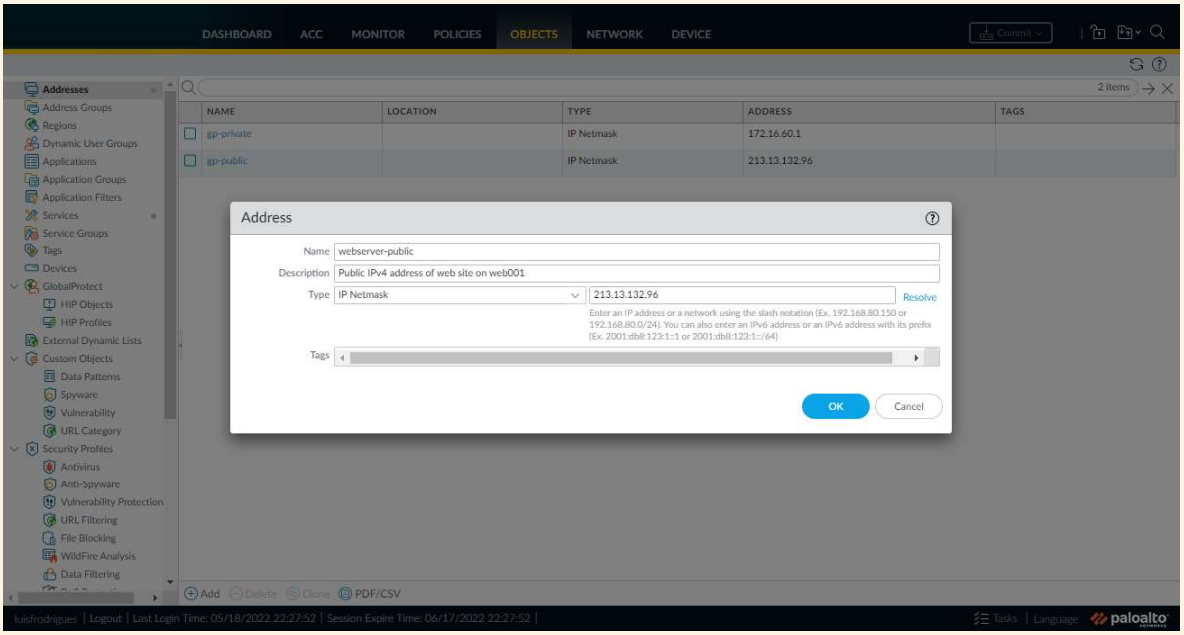


Primeiro vamos criar dois objetos na firewall para serem utilizados posteriormente, o IP público do site web e o IP privado do mesmo site.

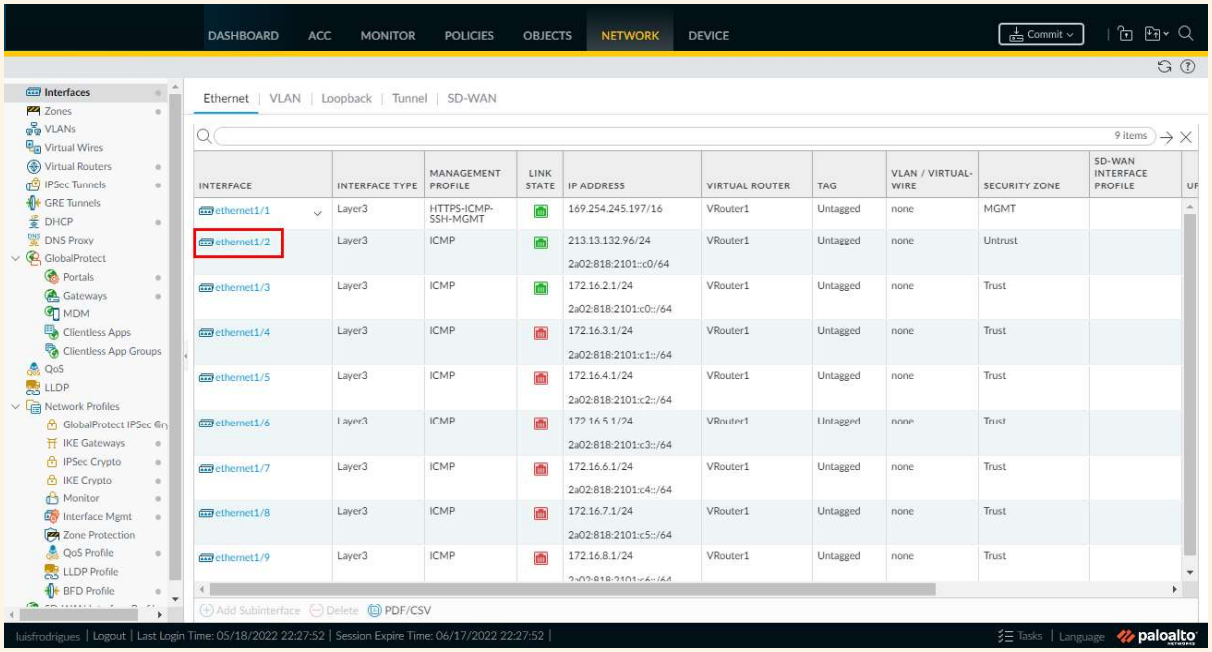
Faça login na firewall. Selecione a aba “OBJECTS” e no menu à esquerda selecione a opção “Addresses”. Clique em “Add” para adicionar um objeto novo:



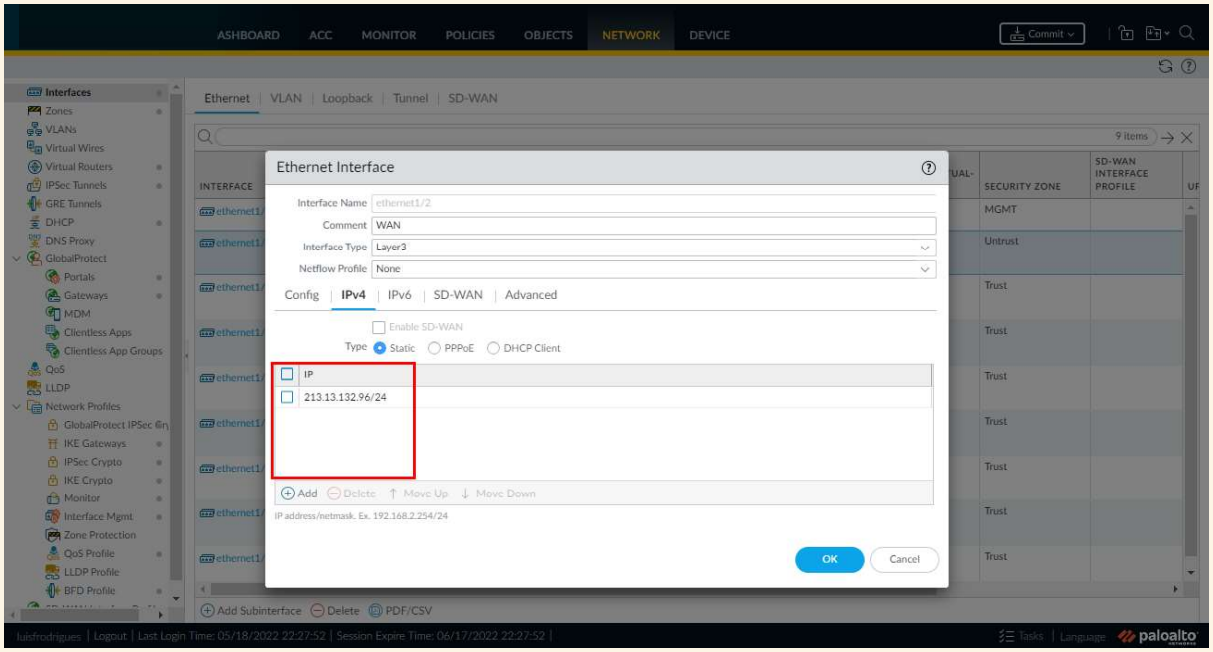
Preencha a informação do objeto e clique em “OK”:



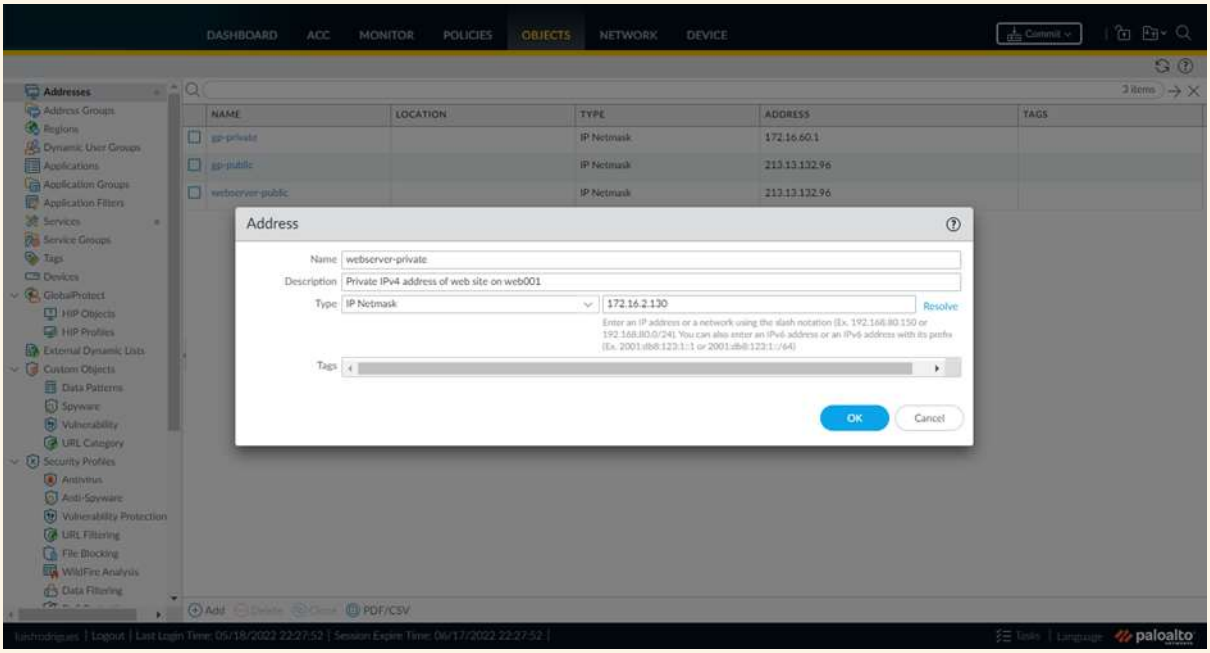
O IP público de IPv4 adquirido também pode ser consultado na firewall, para isso selecione a aba “NETWORK” e no menu à esquerda selecione a opção “Interfaces”. Clique na interface “ethernet1/2”:



Clique na aba “IPv4” para consultar o IP:

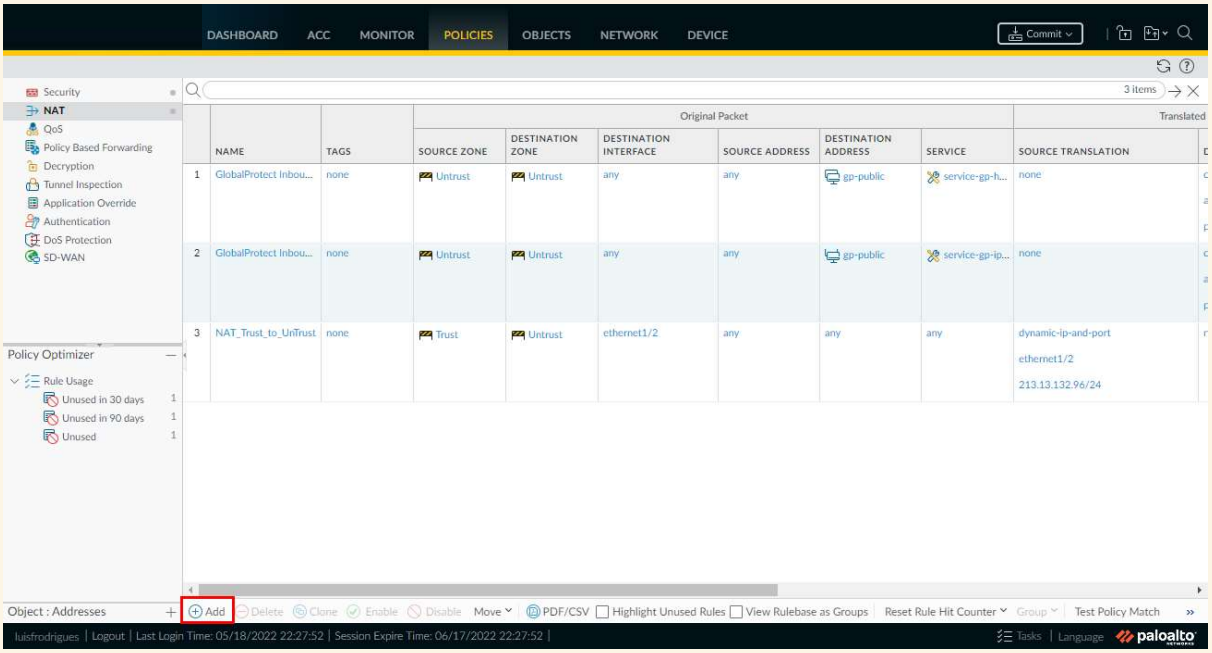


Vamos também criar o objeto referente ao IP privado do web site. Na firewall, volte a selecionar a aba “OBJECTS” e no menu à esquerda selecione a opção “Addresses”. Clique em “Add”, preencha a informação do objeto e clique em “OK”:

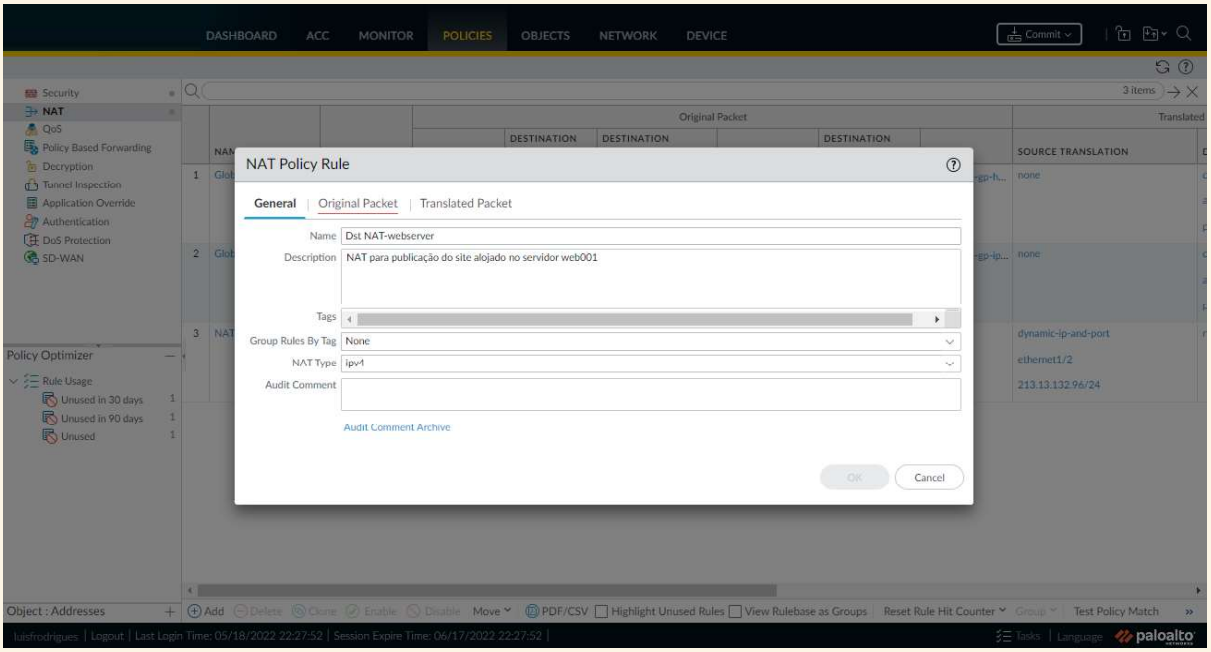


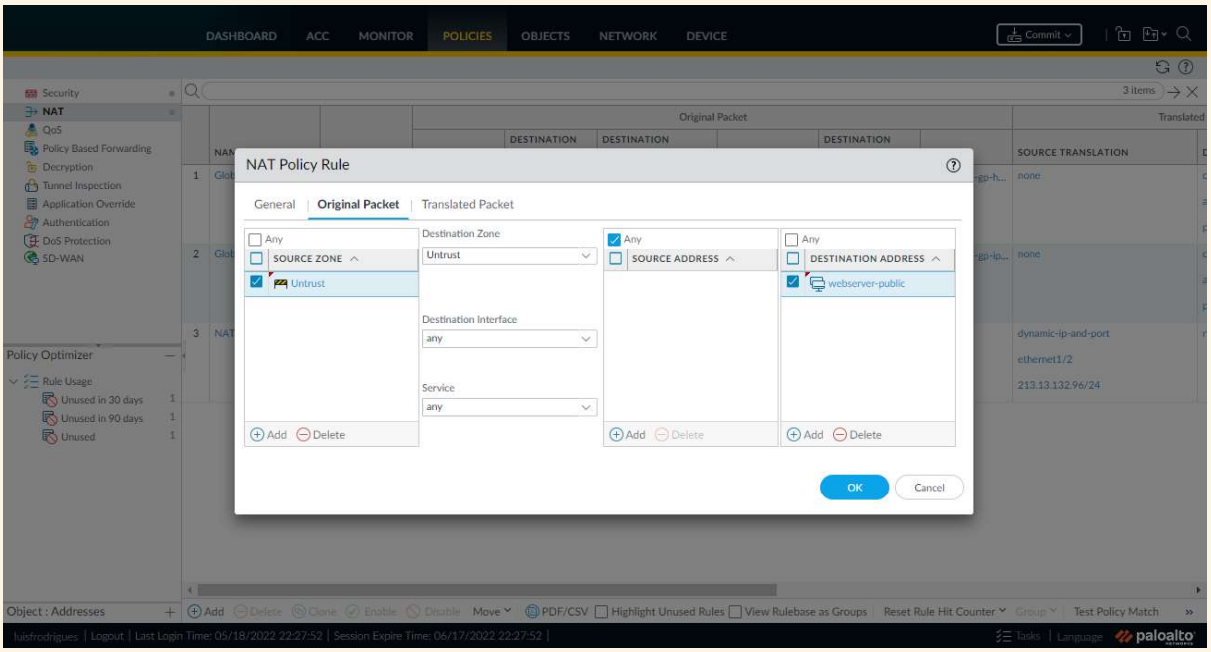
O IP privado do site corresponde ao servidor IPv4 privado do servidor web001, o IP 172.16.1.130.

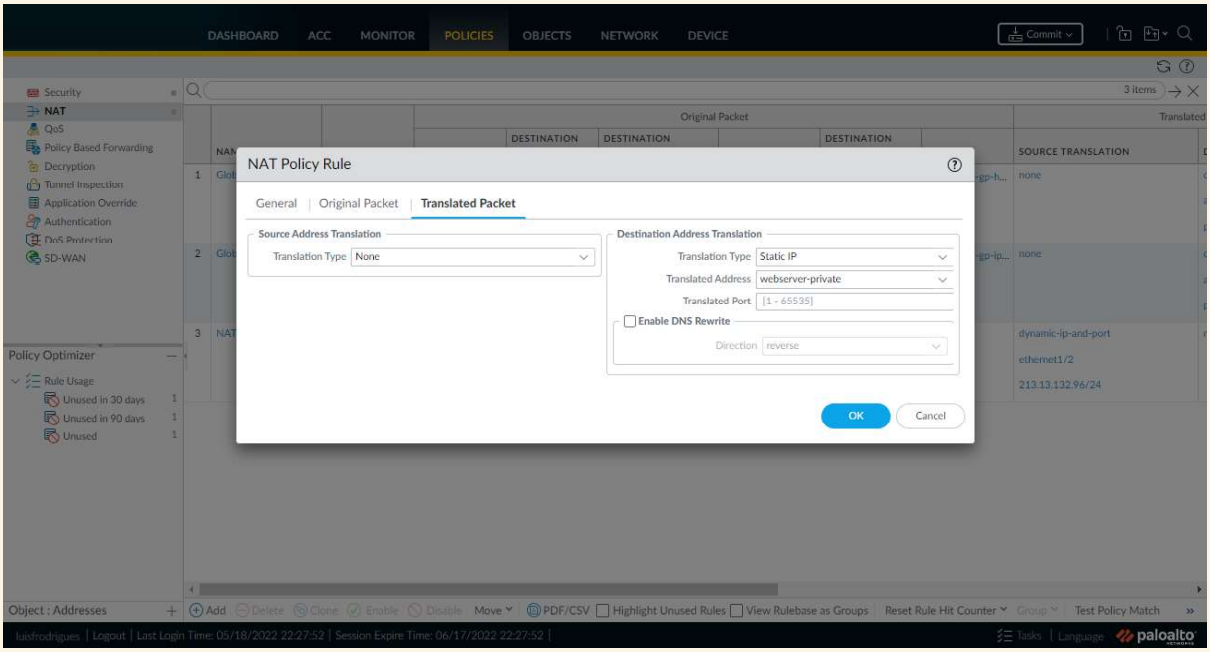
De seguida iremos configurar uma regra de NAT para traduzir o IP público do site para o IP privado. Para isso selecione a aba "POLICIES" e no menu à esquerda selecione a opção "NAT". Clique em "Add" para adicionar uma regra de NAT nova:



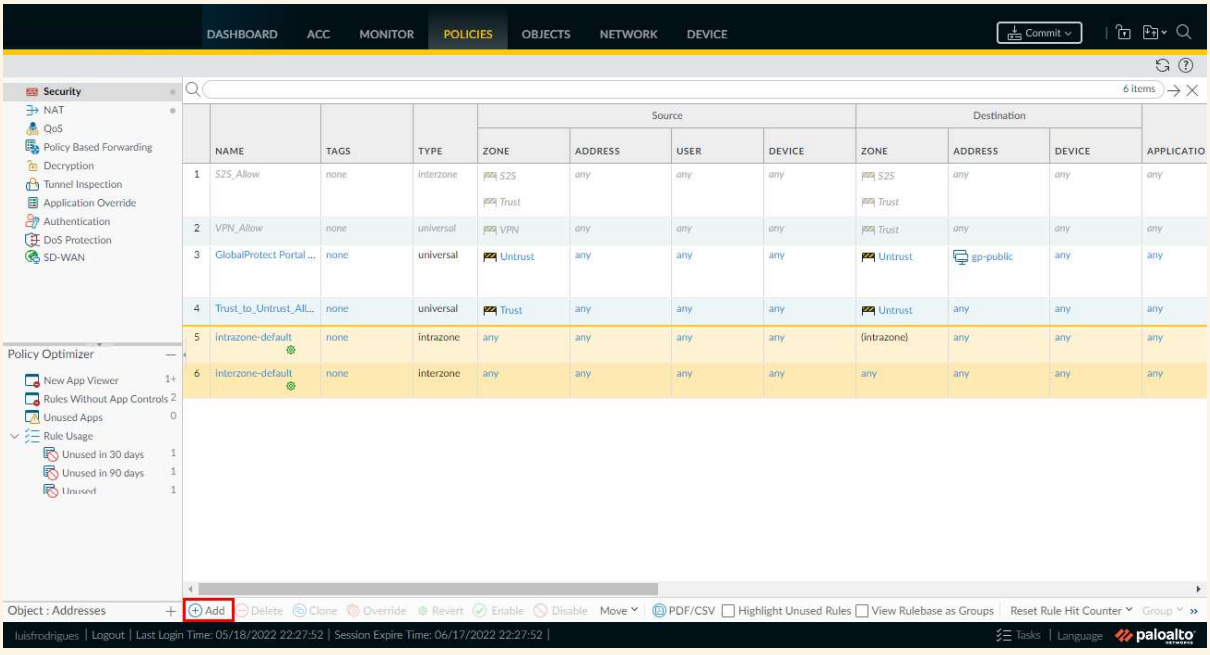
Preencha a informação da regra de NAT nova e no final clique em "OK":


DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
NAT Policy Rule
General
Original Packet
Translated Packet
Name
Dst NAT-webserver
Description
NAT para publicação do site alojado no servidor web001
Tags
Group Rules By Tag
None
NAT Type
ipv4
Audit Comment
Audit Comment Archive
OK
Cancel

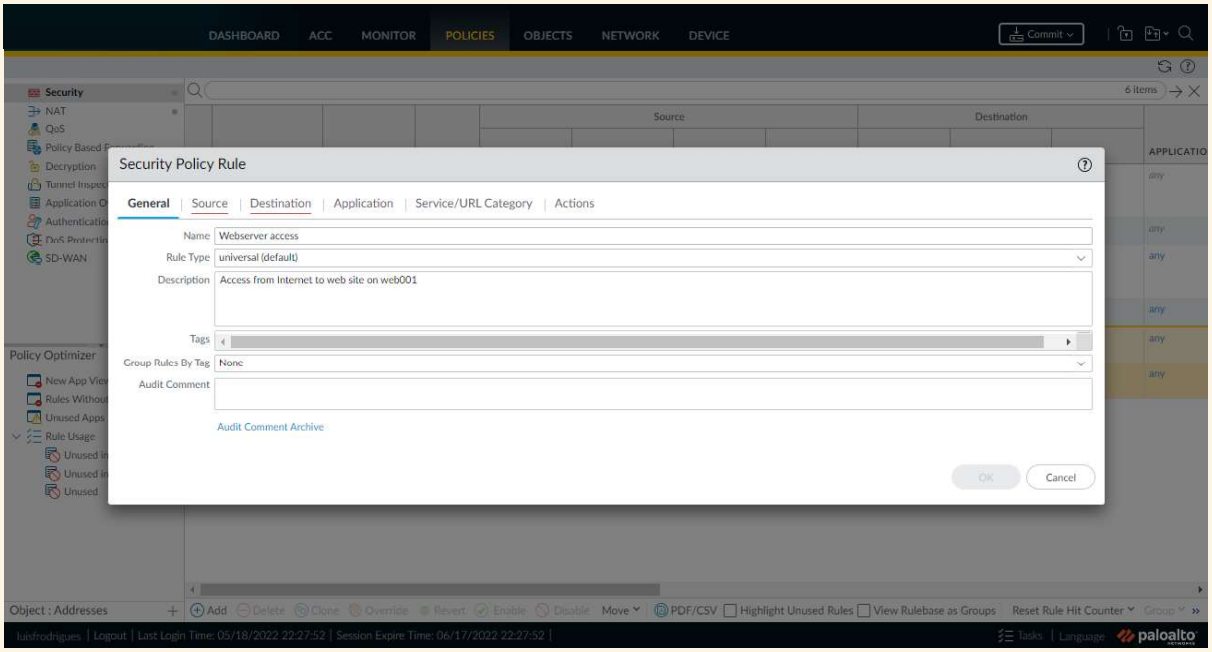

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
NAT Policy Rule
General
Original Packet
Translated Packet
Any
SOURCE ZONE
Untrust
Destination Zone
Untrust
Destination Interface
any
Service
any
Any
SOURCE ADDRESS
Any
DESTINATION ADDRESS
webserver-public
Add
Delete
OK
Cancel

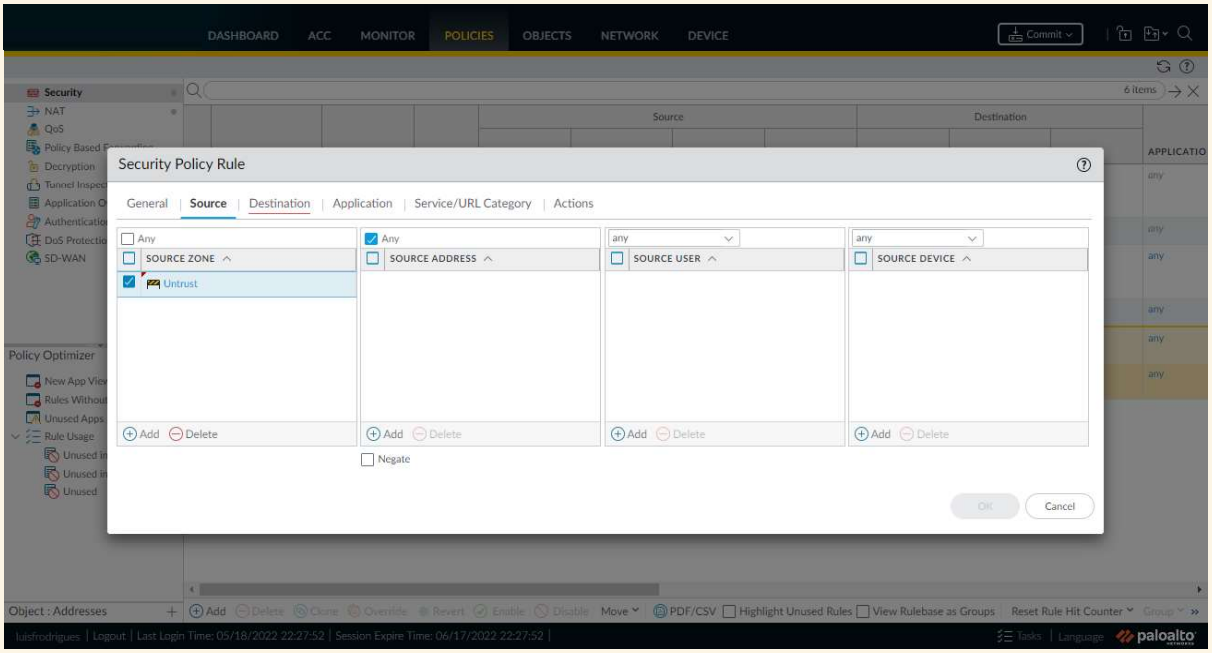


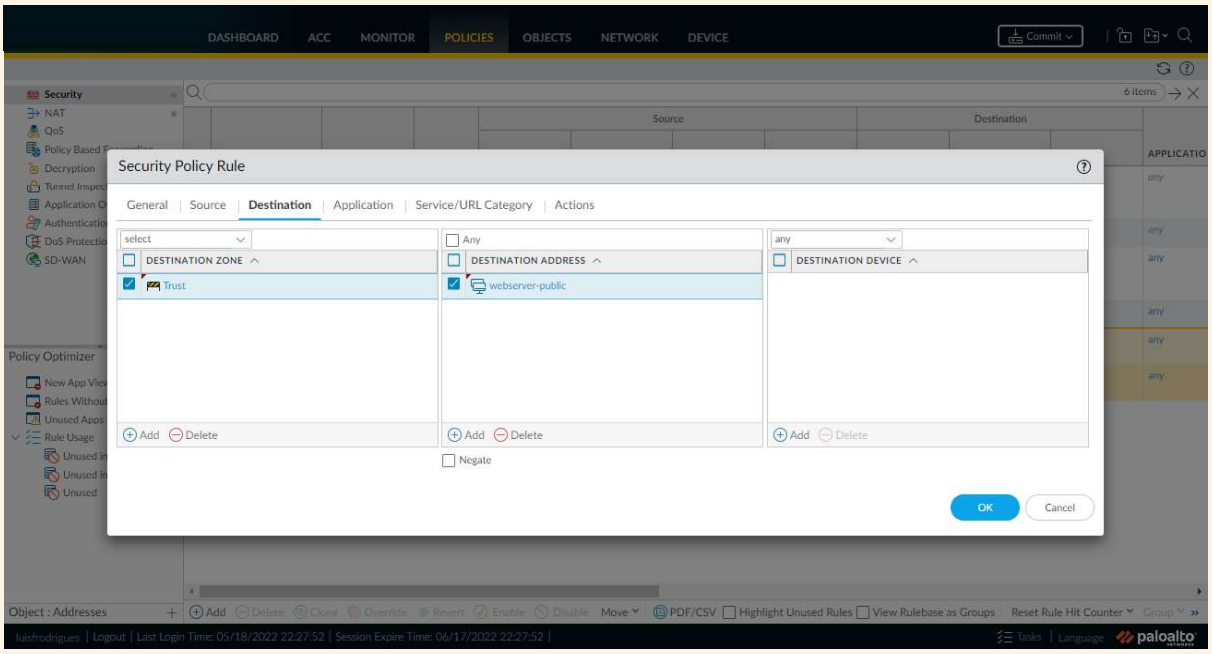
Agora é necessário criar uma regra de segurança para permitir o acesso da Internet ao web site. Para isso selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Clique em "Add" para adicionar uma regra de segurança nova:

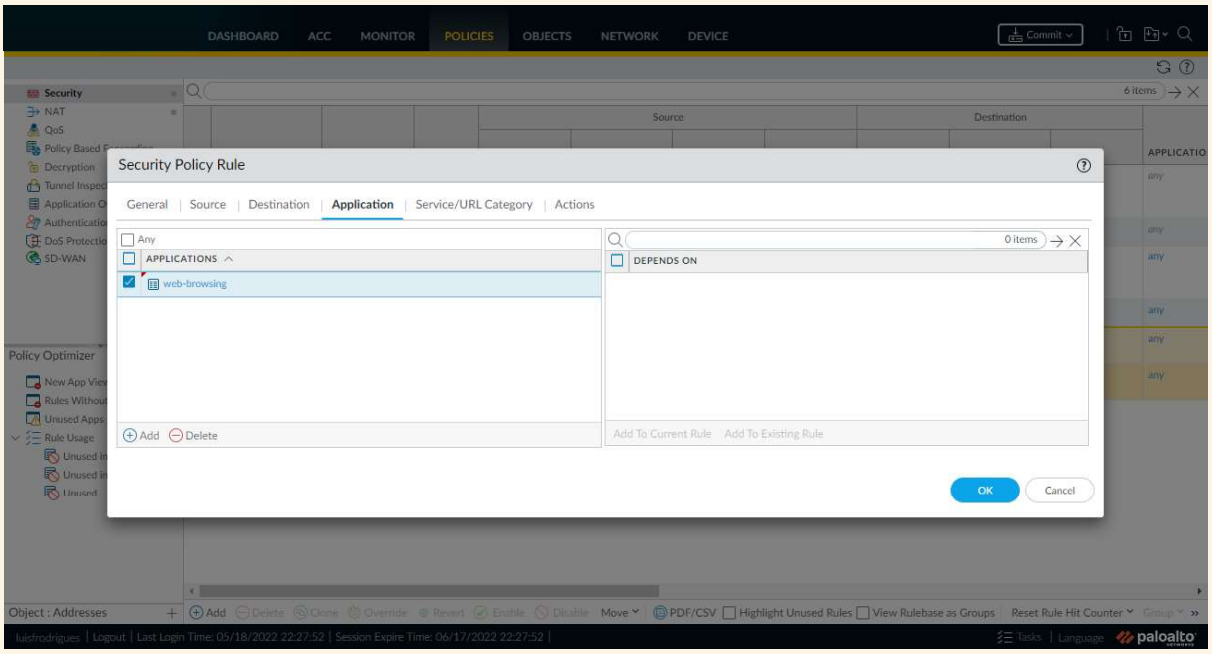


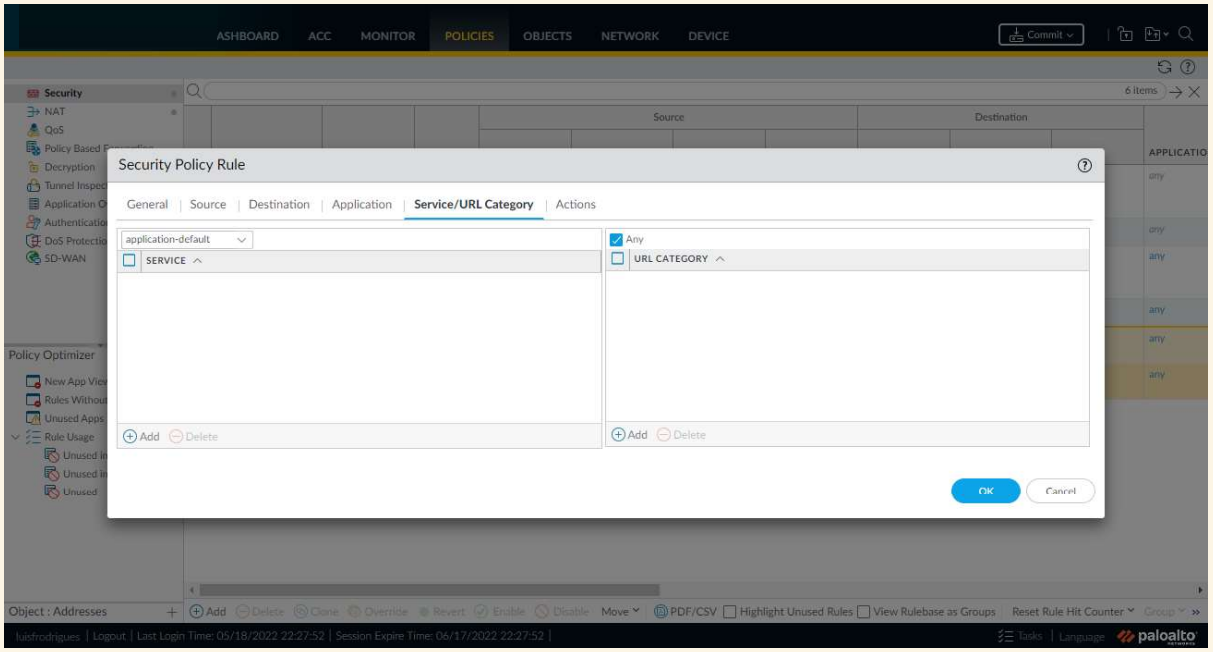
Preencha a informação da regra de segurança nova e no final clique em "OK":

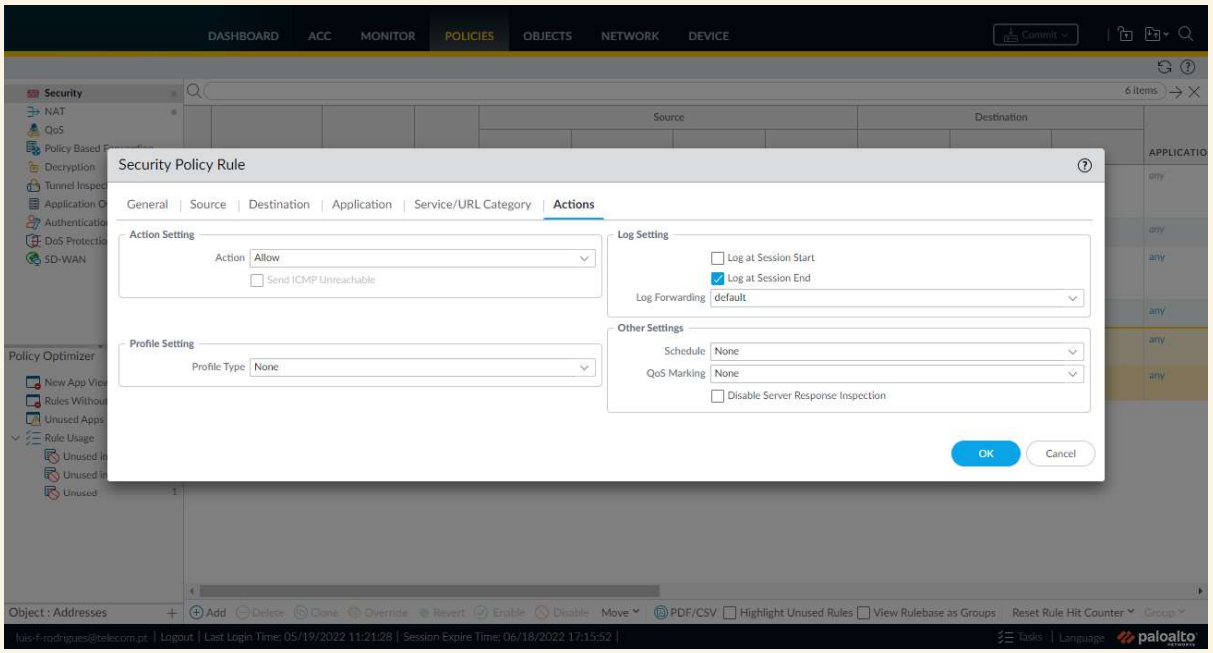

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based
Decryption
Tunnel Inspect
Application O
Authentication
DoS Protectio
SD-WAN
Policy Optimizer
New App View
Rules Without
Unused Apps
Rule Usage
Unused in
Unused in
Unused
Object : Addresses
Add
Delete
Clone
Override
Revert
Enable
Disable
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Group
6 items
Source
Destination
APPLICATIO
any
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Name
Webserver access
Rule Type
universal (default)
Description
Access from Internet to web site on web001
Tags
Group Rules By Tag
None
Audit Comment
Audit Comment Archive
OK
Cancel
luisfrodrigues | Logout | Last Login Time: 05/18/2022 22:27:52 | Session Expire Time: 06/17/2022 22:27:52 |
Tasks
Language
paloalto


DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based
Decryption
Tunnel Inspect
Application O
Authentication
DoS Protectio
SD-WAN
Policy Optimizer
New App View
Rules Without
Unused Apps
Rule Usage
Unused in
Unused in
Unused
Object : Addresses
Add
Delete
Clone
Override
Revert
Enable
Disable
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Group
6 items
Source
Destination
APPLICATIO
any
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
SOURCE ZONE
Untrust
Any
SOURCE ADDRESS
any
SOURCE USER
any
SOURCE DEVICE
Add
Delete
Negate
OK
Cancel
luisfrodrigues | Logout | Last Login Time: 05/18/2022 22:27:52 | Session Expire Time: 06/17/2022 22:27:52 |
Tasks
Language
paloalto

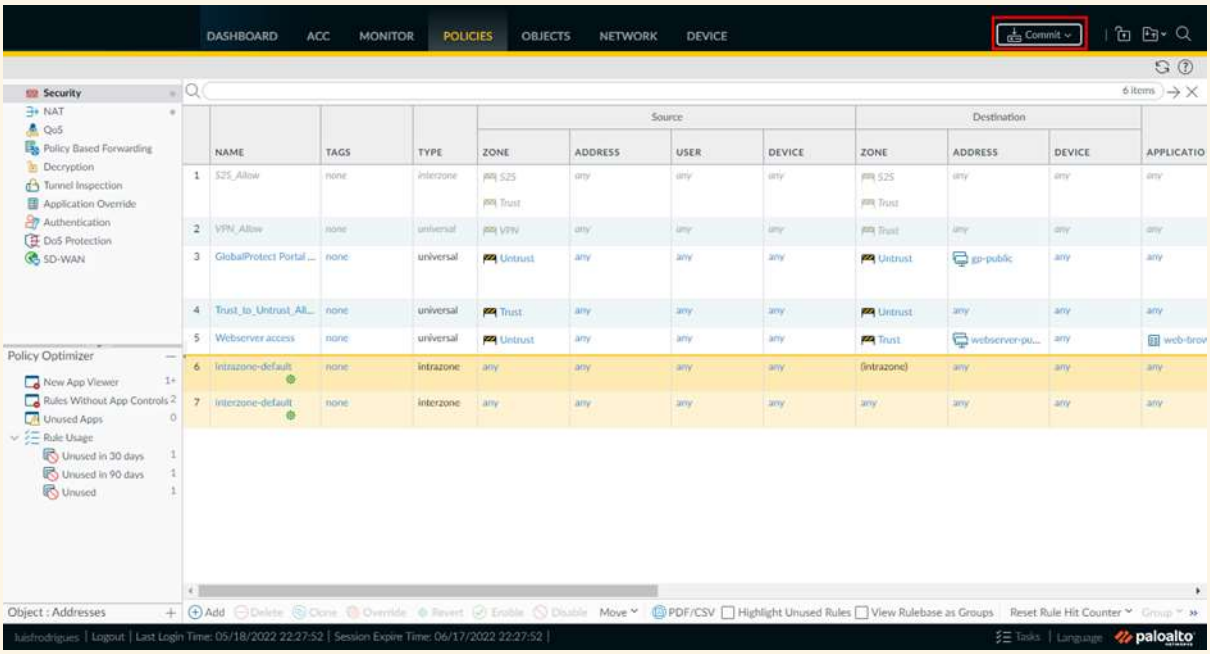

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App Viewer
Rules Without App Controls
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
Object : Addresses
Source
Destination
APPLICATIO
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
select
DESTINATION ZONE
Trust
Any
DESTINATION ADDRESS
webserver-public
any
DESTINATION DEVICE
Add
Delete
Negate
OK
Cancel
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
paloalto

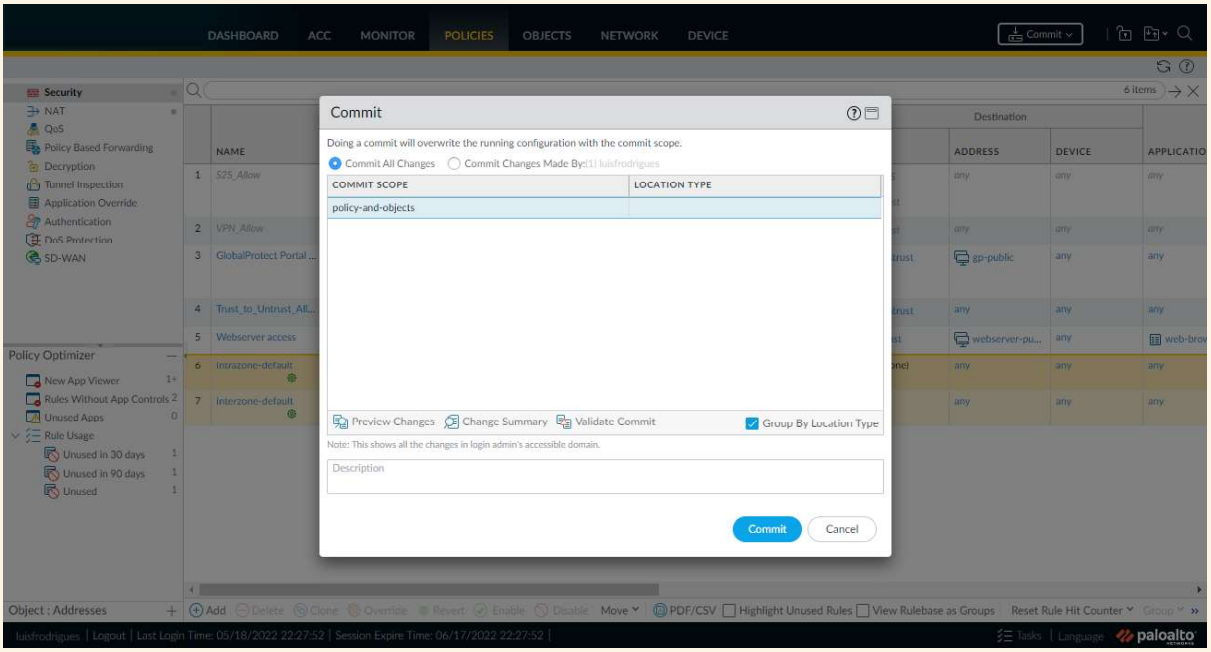

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based Forwarding
Decryption
Tunnel Inspection
Application Override
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App Viewer
Rules Without App Controls
Unused Apps
Rule Usage
Unused in 30 days
Unused in 90 days
Unused
Object : Addresses
Source
Destination
APPLICATIO
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
APPLICATIONS
web-browsing
0 items
DEPENDS ON
Add
Delete
Add To Current Rule
Add To Existing Rule
OK
Cancel
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
paloalto



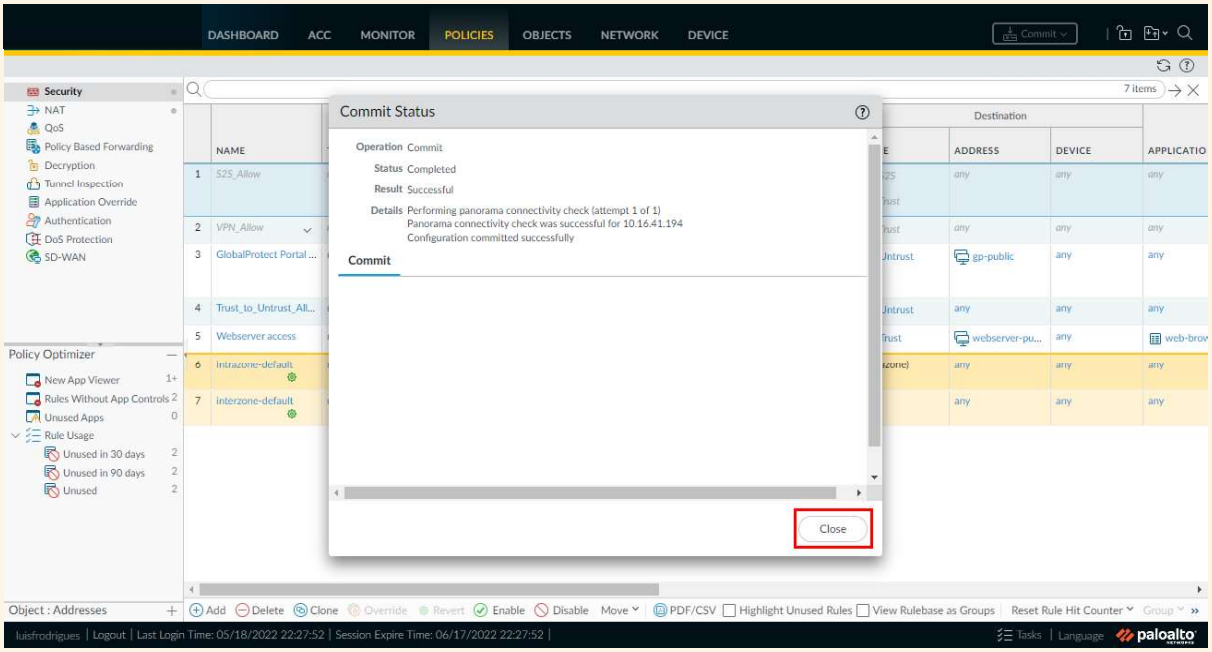


Para tornar as alterações efetivas, clique no botão “Commit” e na caixa de diálogo clique em “Commit”:

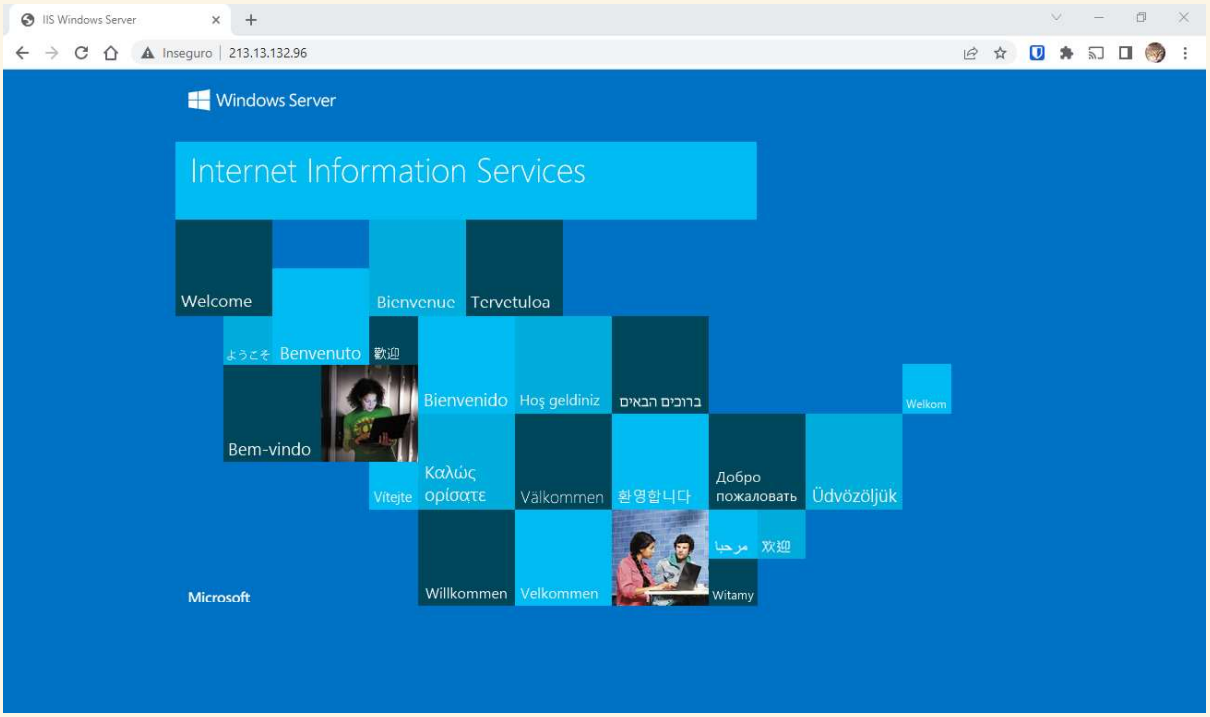




Quando o Commit estiver concluído, clique em “Close”:



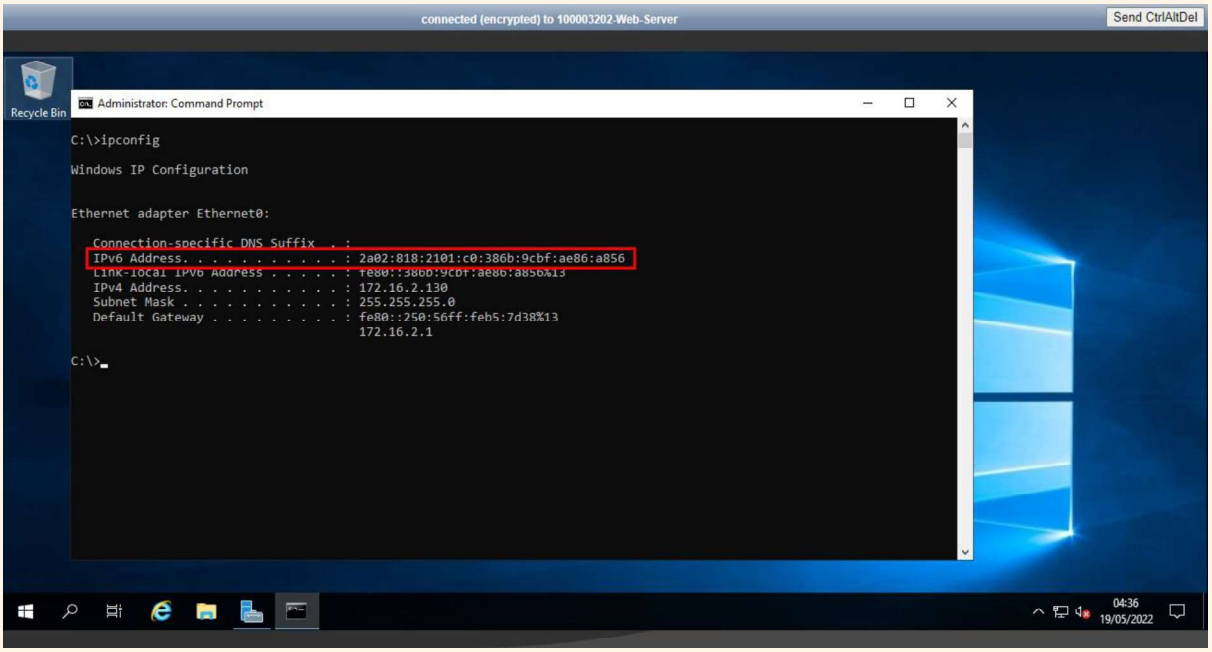
Para testar o acesso ao web site use um PC ligado à Internet e coloque o URL http://213.13.132.96 num browser. Irá aparecer a página default do IIS:



2.4.2. Publicação pelo IP de IPv6

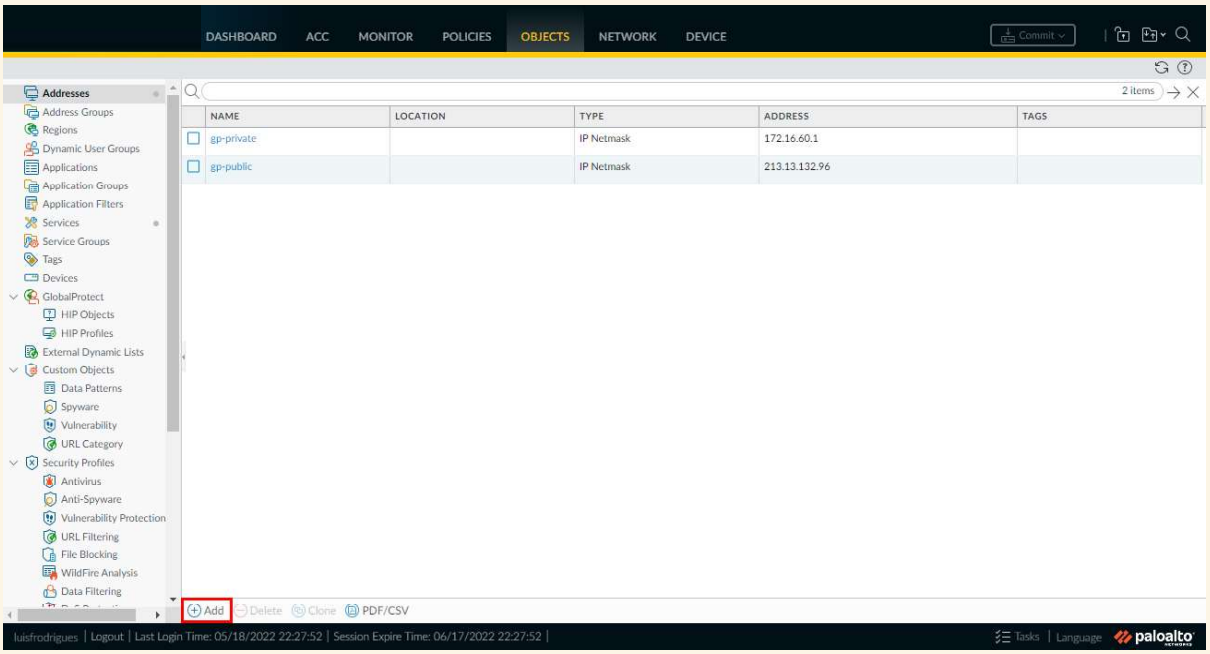
Para publicar o web site por IPv6 não é necessário configurar NATs na firewall porque, by design, todo o IPv6 é público. Não quer isto dizer que o web site está imediatamente exposto na Internet se tiver um IP de IPv6, tal como no exemplo do IPv4, é sempre necessário que exista uma regra de segurança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

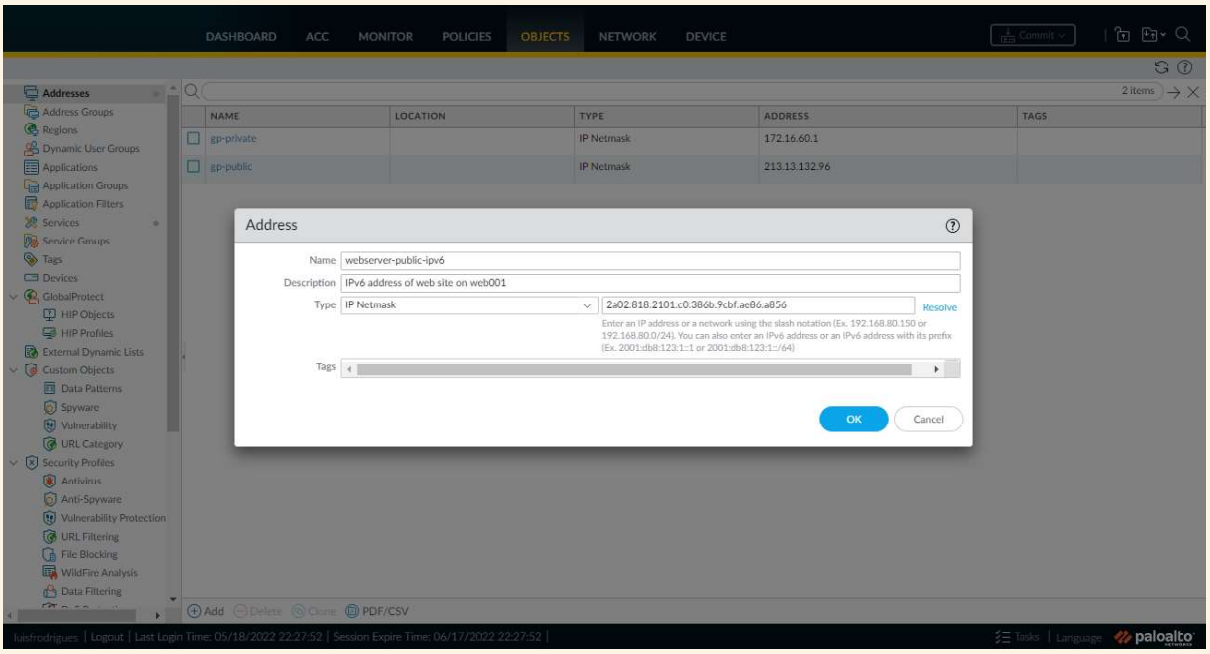


Primeiro vamos criar um objeto na firewall para ser utilizado posteriormente, o IP de IPv6 do site web.

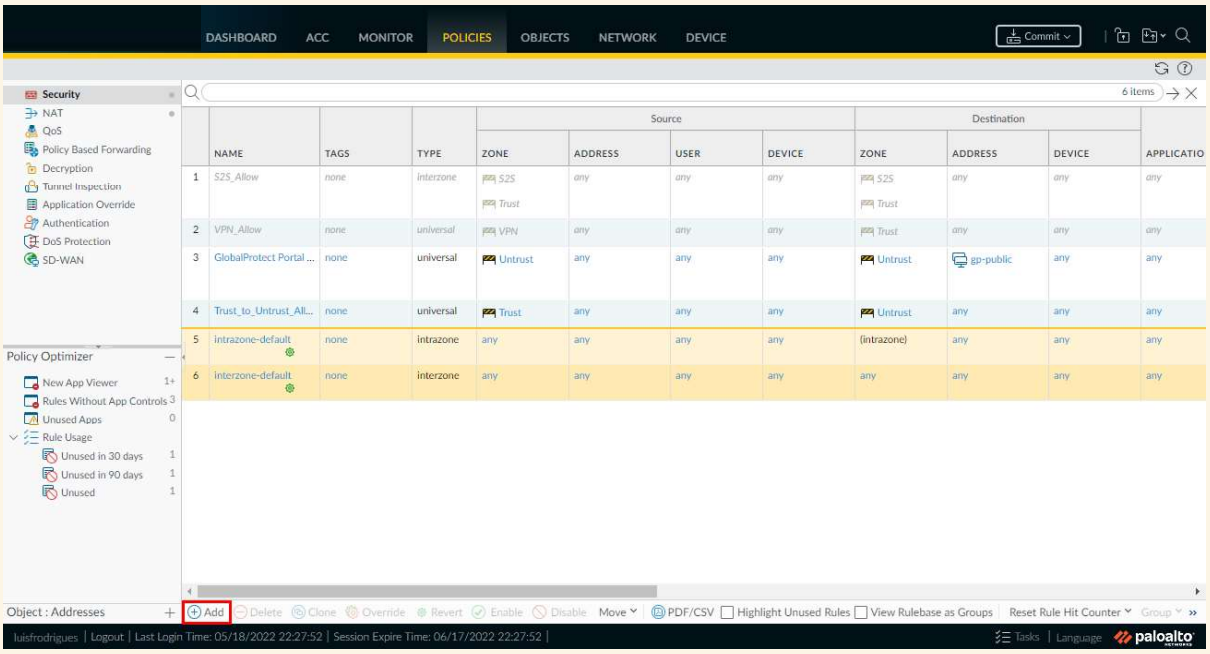
Faça login na firewall. Selecione a aba “OBJECTS” e no menu à esquerda selecione a opção “Addresses”. Clique em “Add” para adicionar um objeto novo:



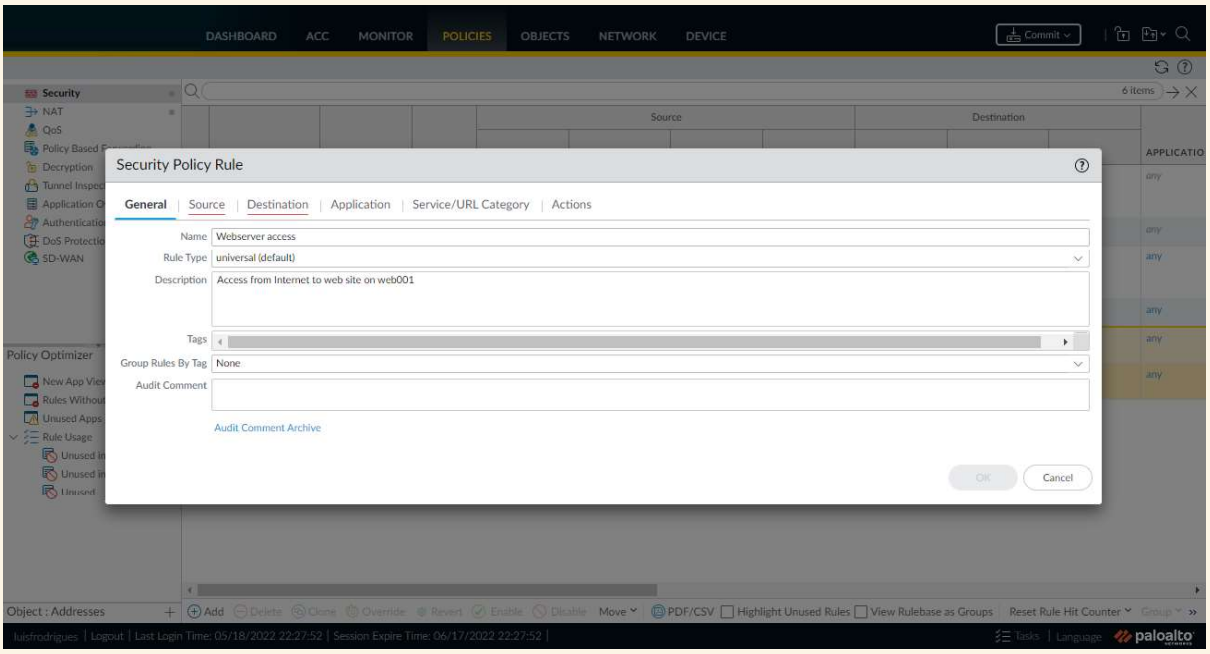
Preencha a informação do objeto e clique em “OK”:

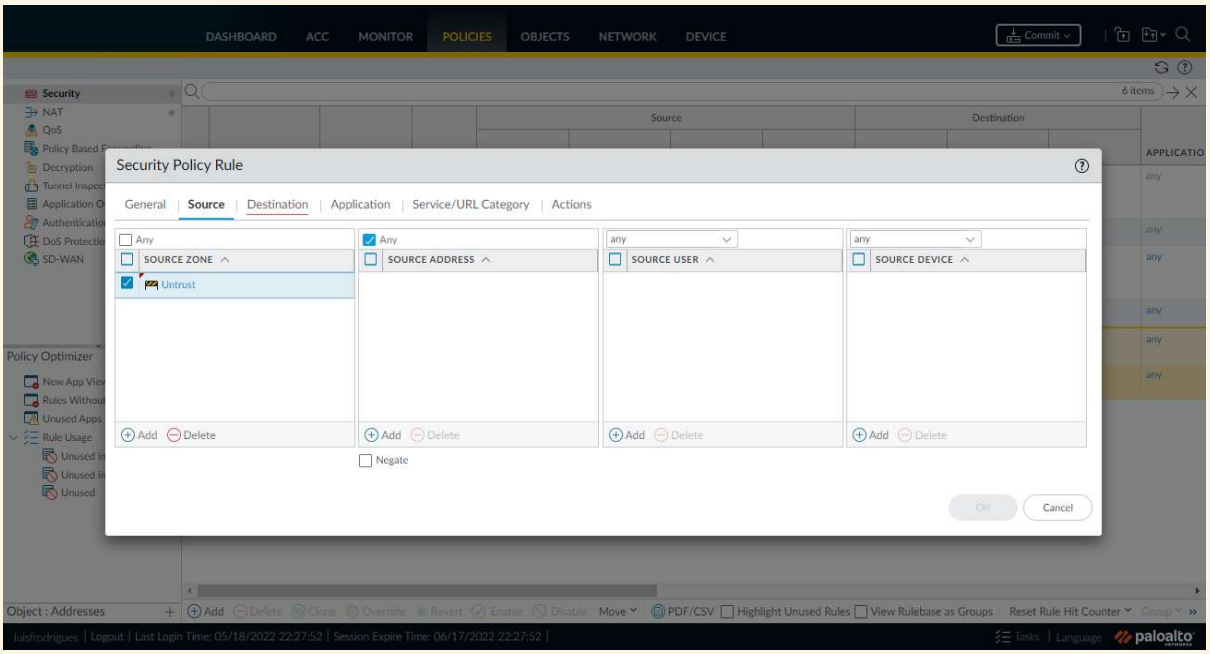


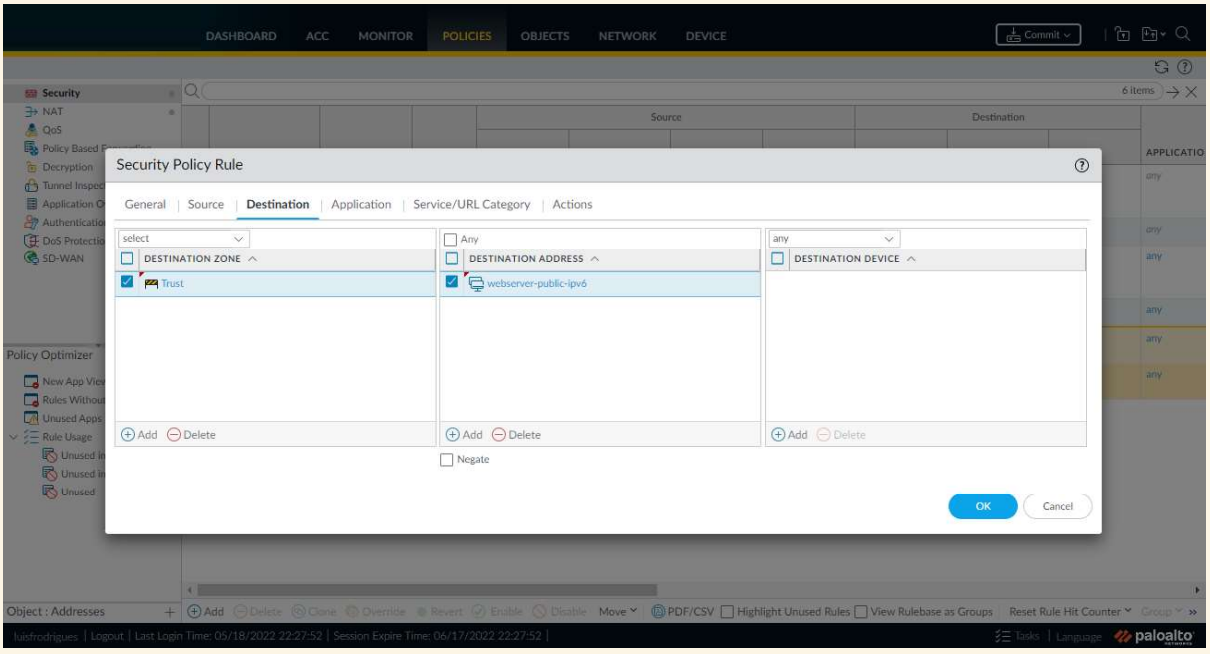
De seguida vamos criar uma regra de segurança na firewall. Selecione a aba “POLICIES” e no menu à esquerda selecione a opção “Security”. Clique em “Add” para adicionar uma regra de segurança nova:

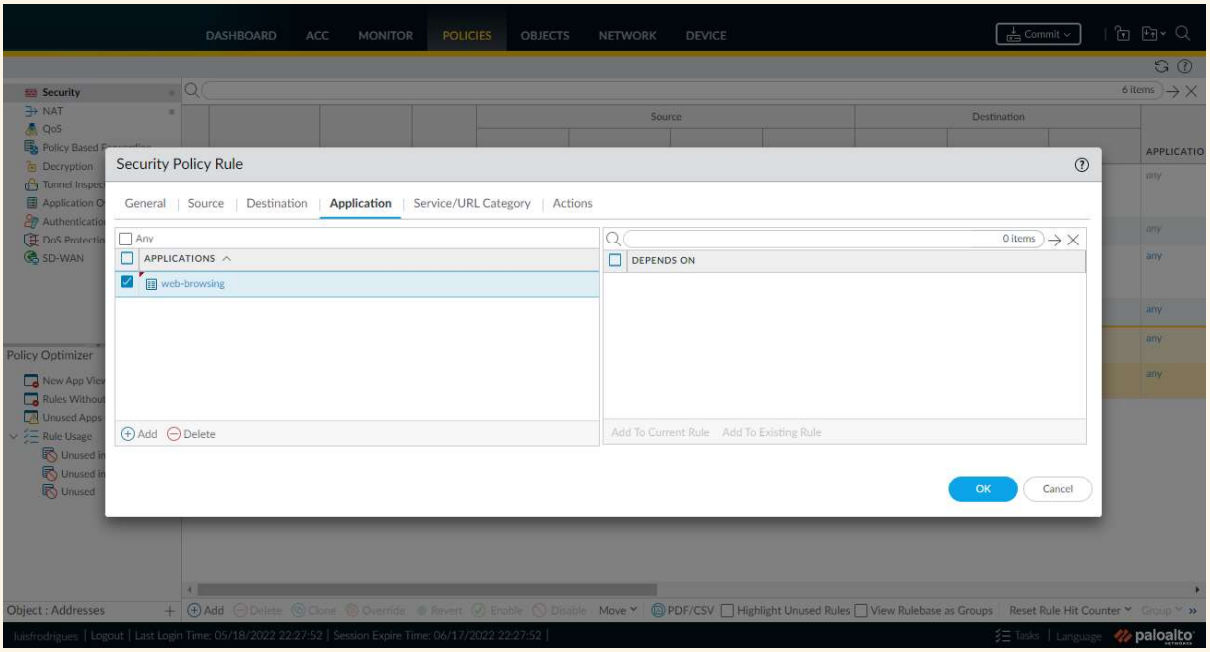


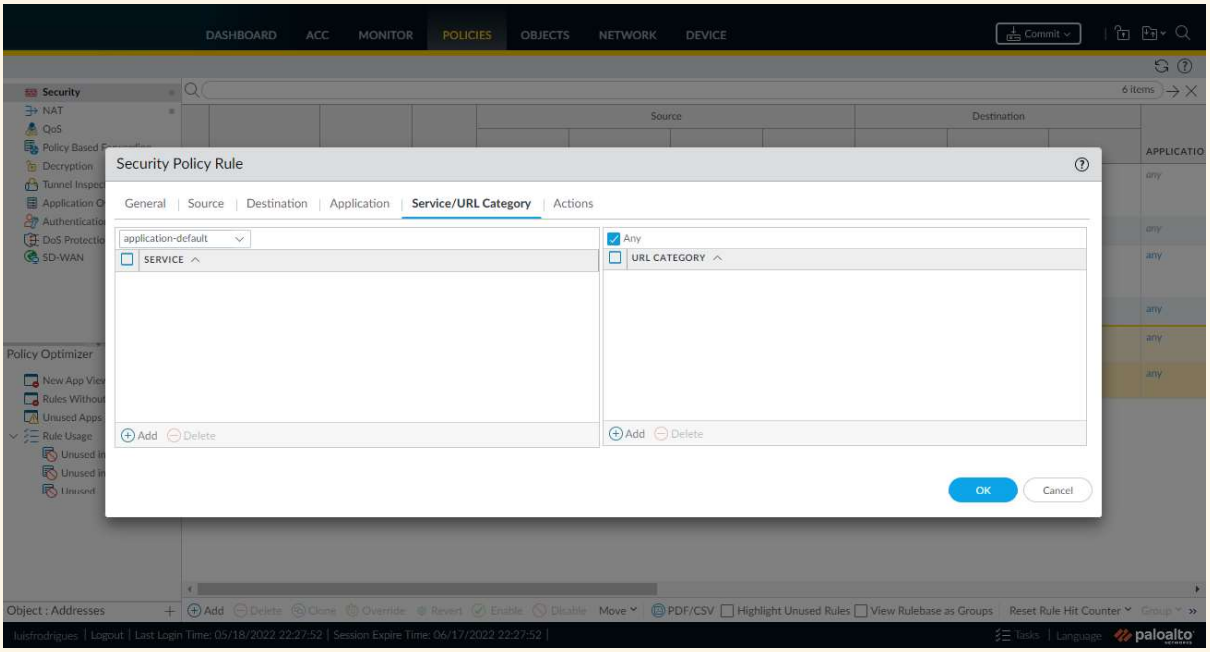
Preencha a informação da regra de segurança nova e no final clique em “OK”:

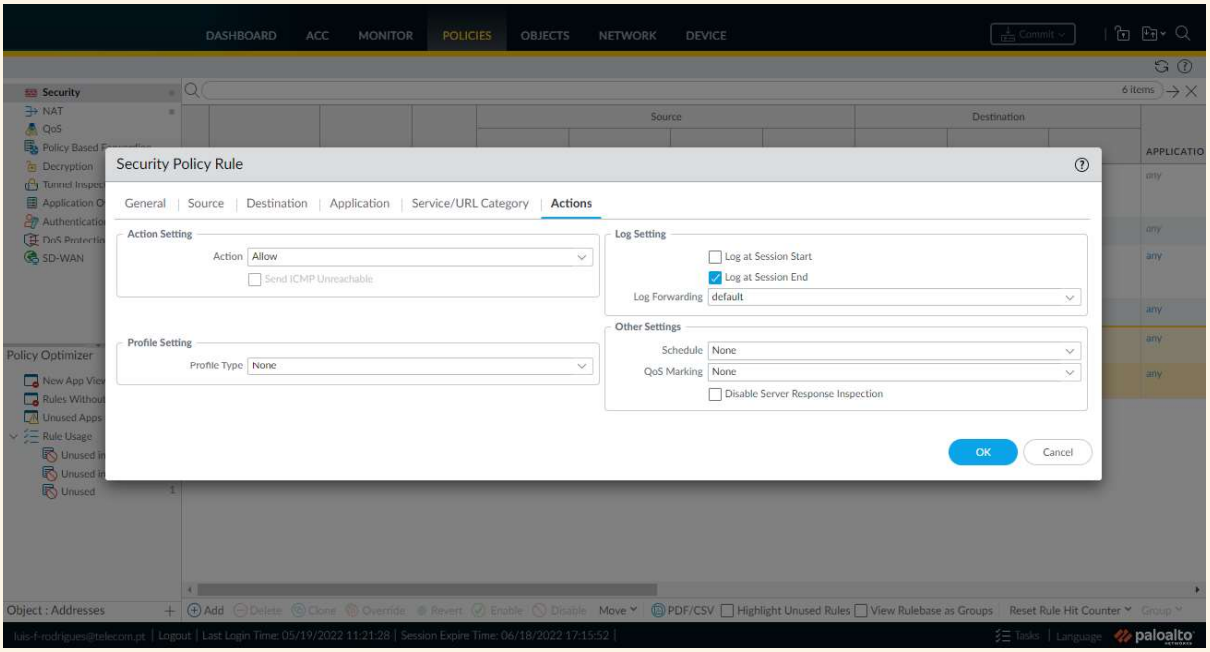



DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
SOURCE ZONE
Untrust
SOURCE ADDRESS
SOURCE USER
SOURCE DEVICE
Add
Delete
Negate
OK
Cancel
Source
Destination
Policy Optimizer
Object : Addresses
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
paloalto

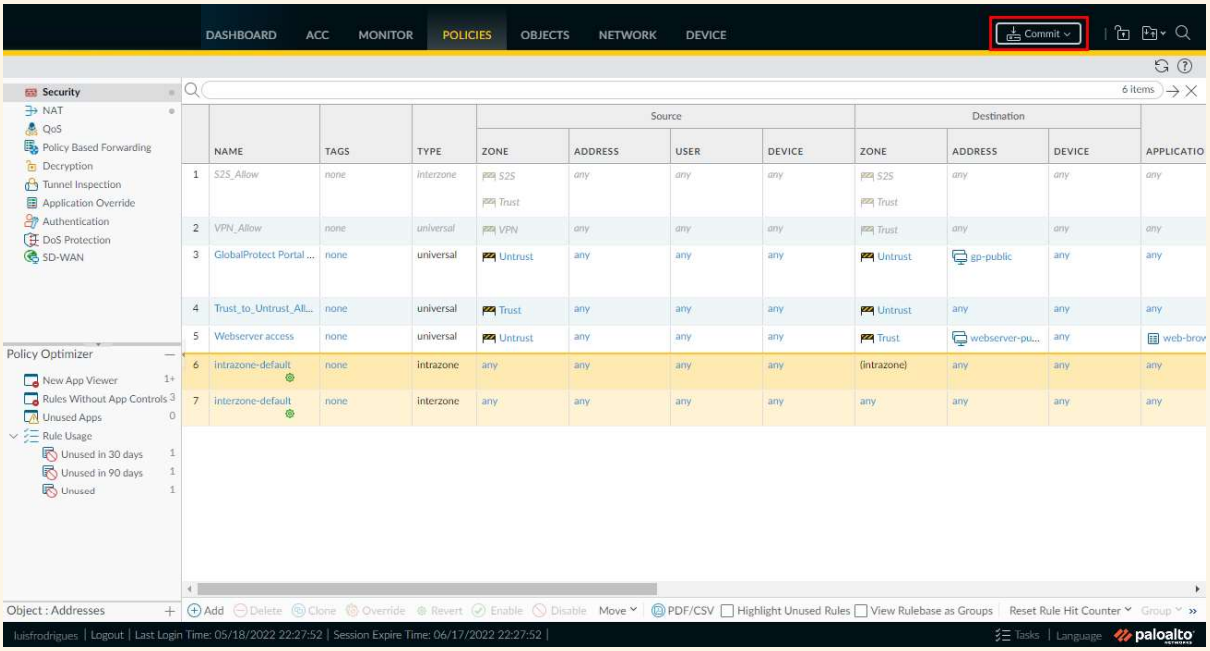

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
select
DESTINATION ZONE
Trust
Any
DESTINATION ADDRESS
webserver-public-ipv6
any
DESTINATION DEVICE
Add
Delete
Negate
OK
Cancel
Source
Destination
Policy Optimizer
Object : Addresses
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
paloalto

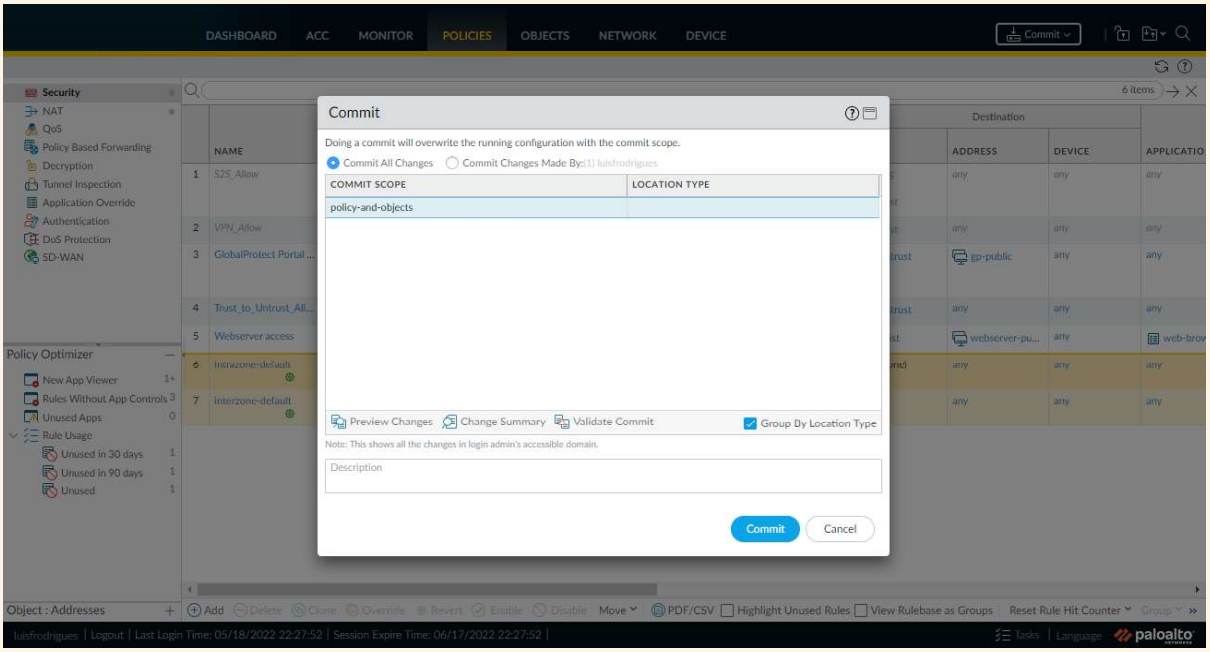

DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based
Decryption
Tunnel Inspect
Application O
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App View
Rules Without
Unused Apps
Rule Usage
Unused in
Unused in
Unused
Object : Addresses
Source
Destination
APPLICATIO
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
Any
APPLICATIONS
web-browsing
0 items
DEPENDS ON
Add
Delete
Add To Current Rule
Add To Existing Rule
OK
Cancel
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Tasks
Language
paloalto


DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
Security
NAT
QoS
Policy Based
Decryption
Tunnel Inspect
Application O
Authentication
DoS Protection
SD-WAN
Policy Optimizer
New App View
Rules Without
Unused Apps
Rule Usage
Unused in
Unused in
Unused
Object : Addresses
Source
Destination
APPLICATIO
Security Policy Rule
General
Source
Destination
Application
Service/URL Category
Actions
application-default
SERVICE
Any
URL CATEGORY
Add
Delete
OK
Cancel
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Tasks
Language
paloalto

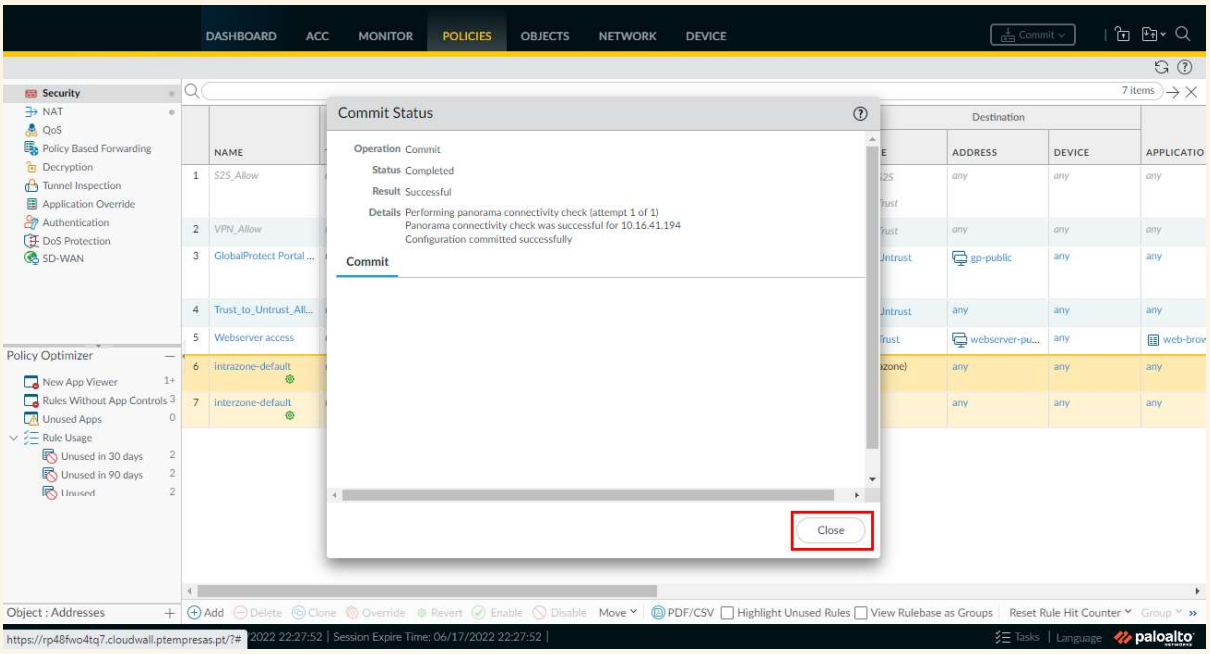


Para tornar as alterações efetivas, clique no botão “Commit” e na caixa de diálogo clique em “Commit”:

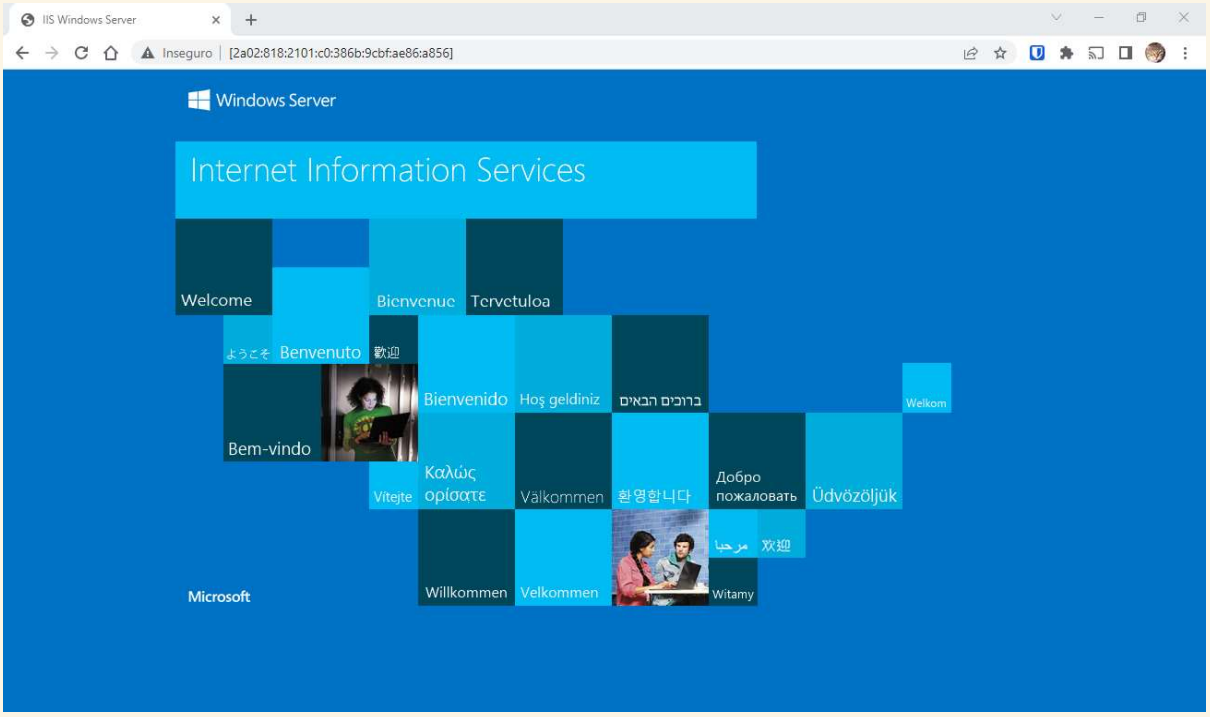




Quando o Commit estiver concluído, clique em "Close":



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

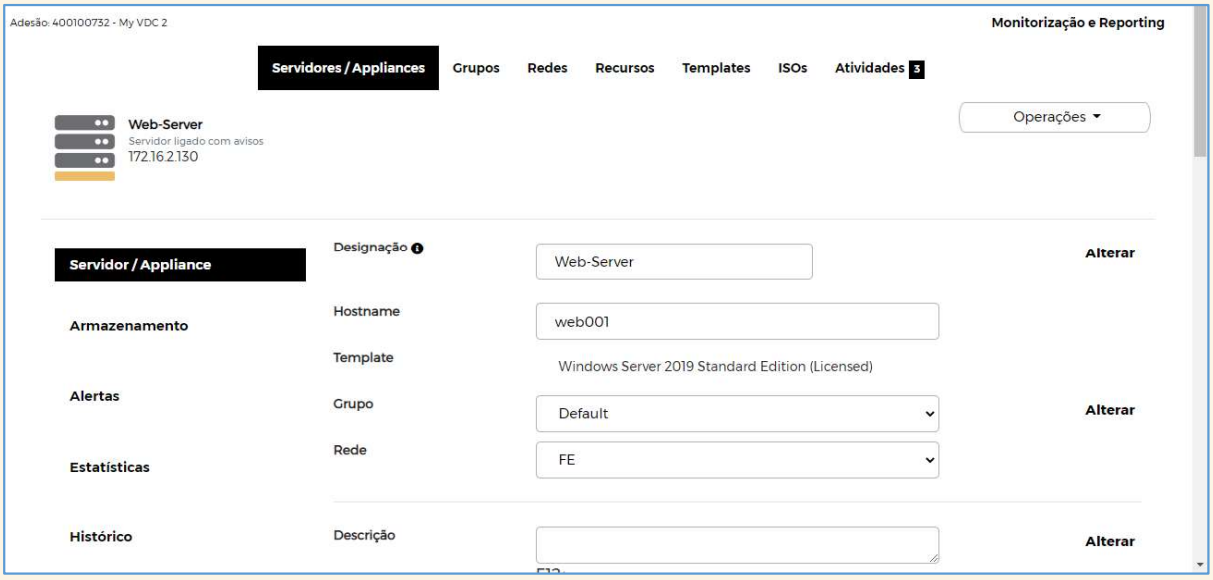


2.5. Como faço para estabelecer um Túnel VPN IPSEC entre a minha Firewall e uma Firewall remota?

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

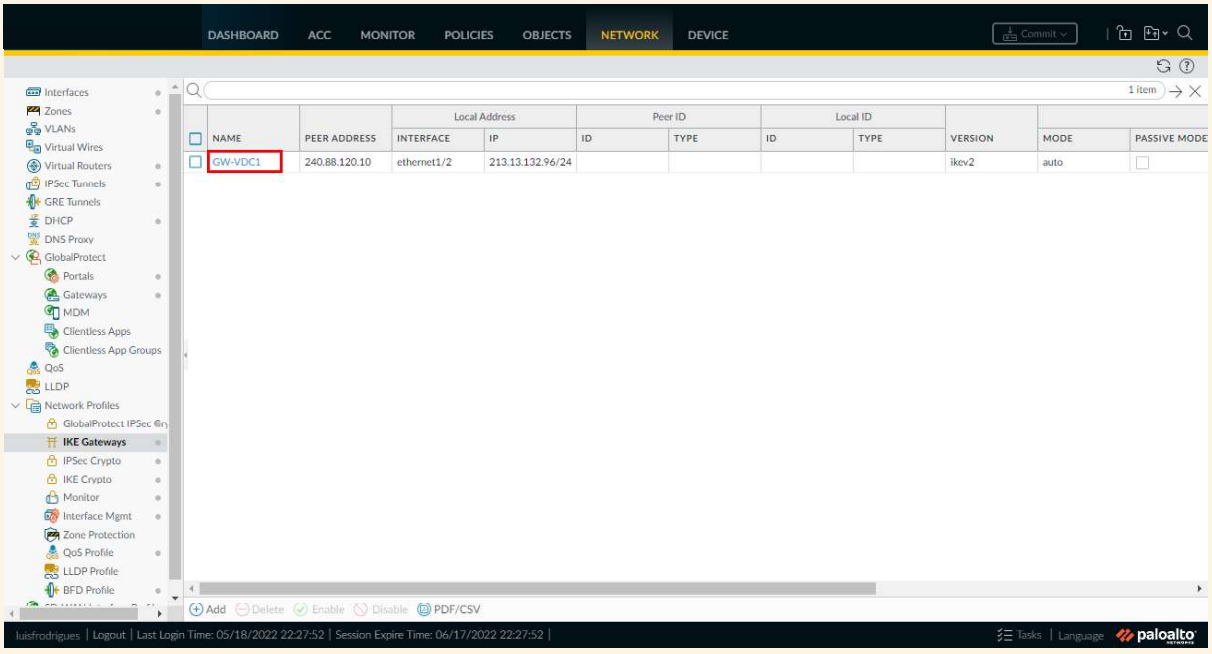
2.5.1. Túnel VPN IPSec pelo IP público de IPv4 (só nas adesões onde este foi adquirido)

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:

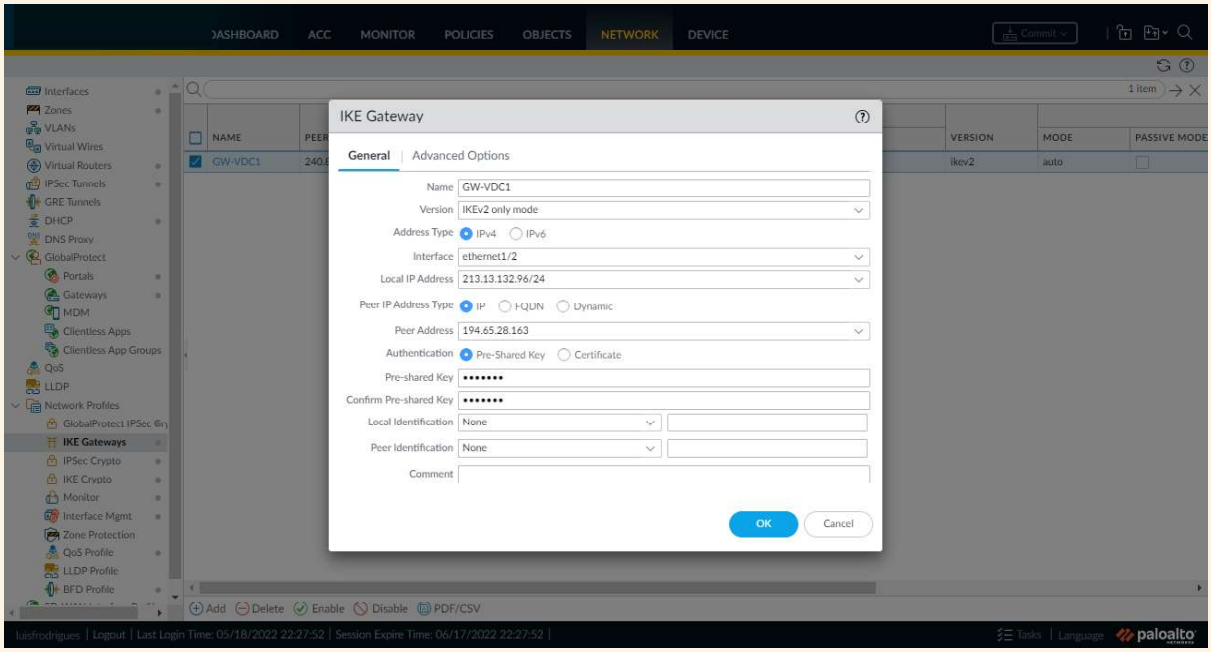


A firewall remota tem o IPv4 público **194.65.28.163**. A Pre-shared Key escolhida para a configuração do túnel VPN IPSec foi **QQtC^9AbZs**. Na rede remota encontra-se um servidor Windows semelhante ao nosso, com o IP 10.50.1.130. No final iremos verificar que conseguimos pingar o servidor remoto a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

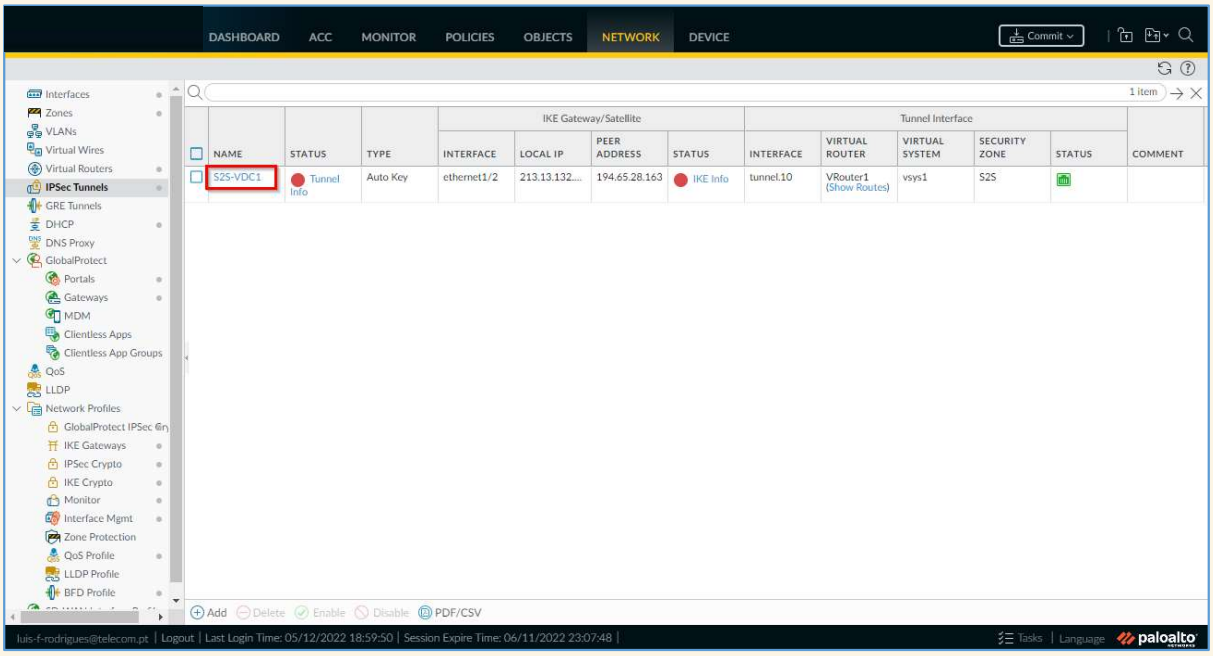


Introduza o endereço público IPv4 da firewall remota no campo “Peer Address” e a Pre-shared Key no campo respetivo. Clique em “OK”:

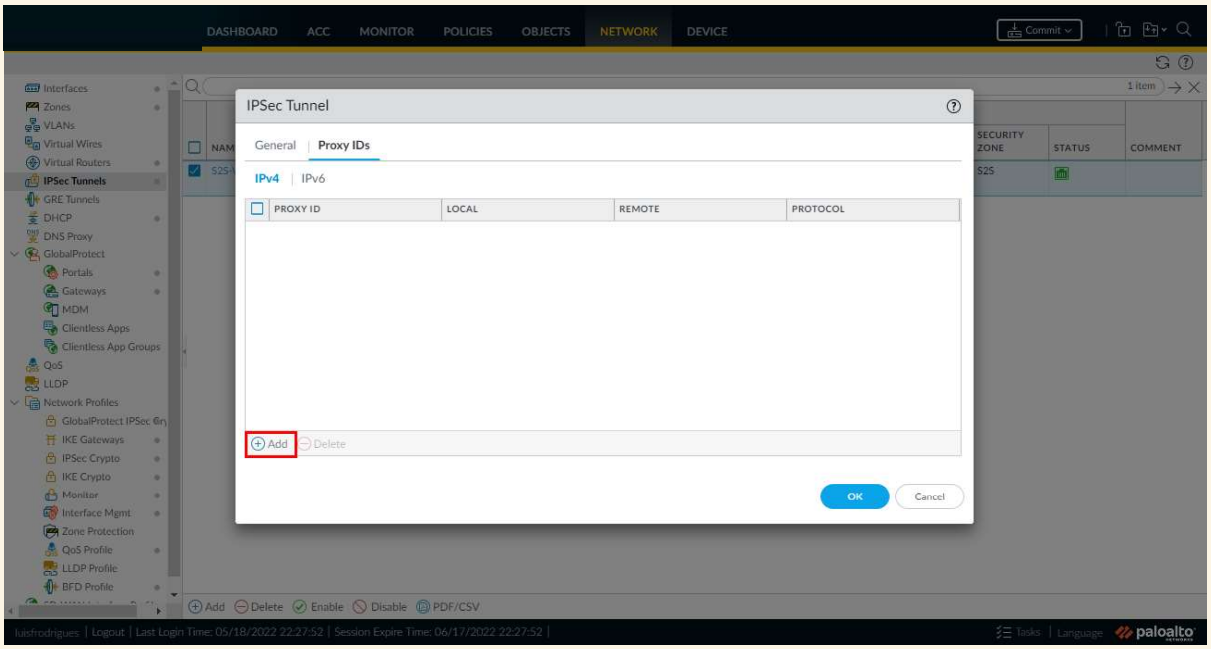


Na firewall remota também devem ser configurados o “Peer Address” com o IP público de IPv4 da nossa firewall Palo Alto e a Pre-shared Key.

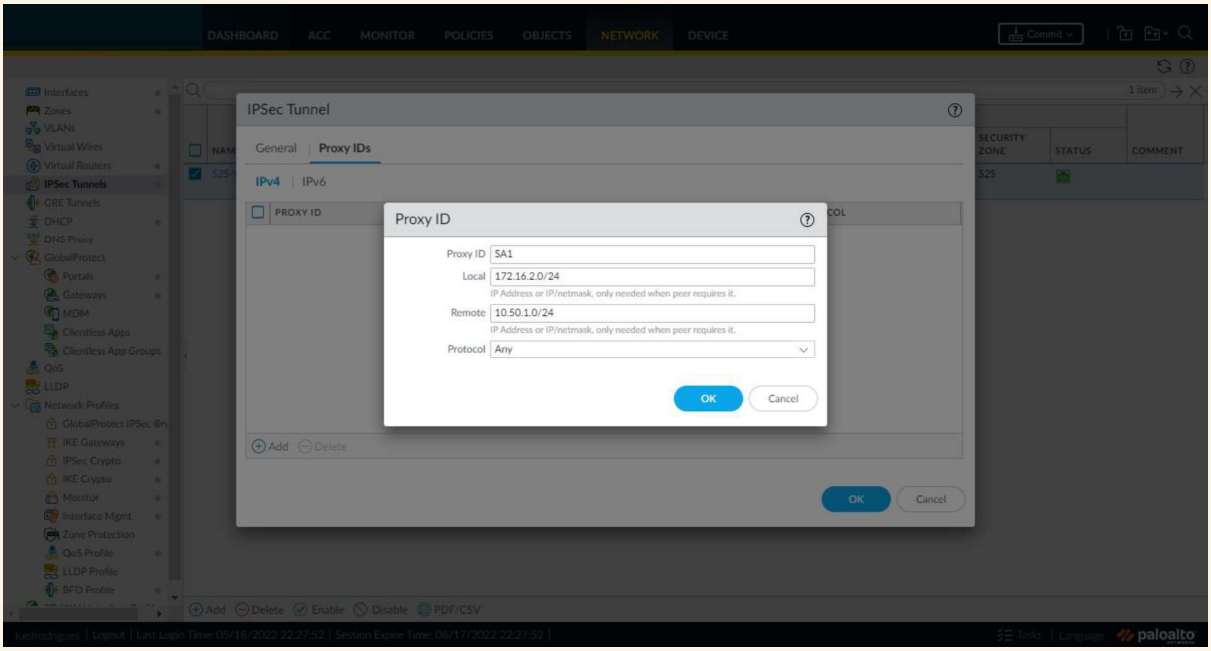
No menu da esquerda, selecione a opção “IPSec Tunnels” e clique no túnel de nome “S2S-VDC1”:



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

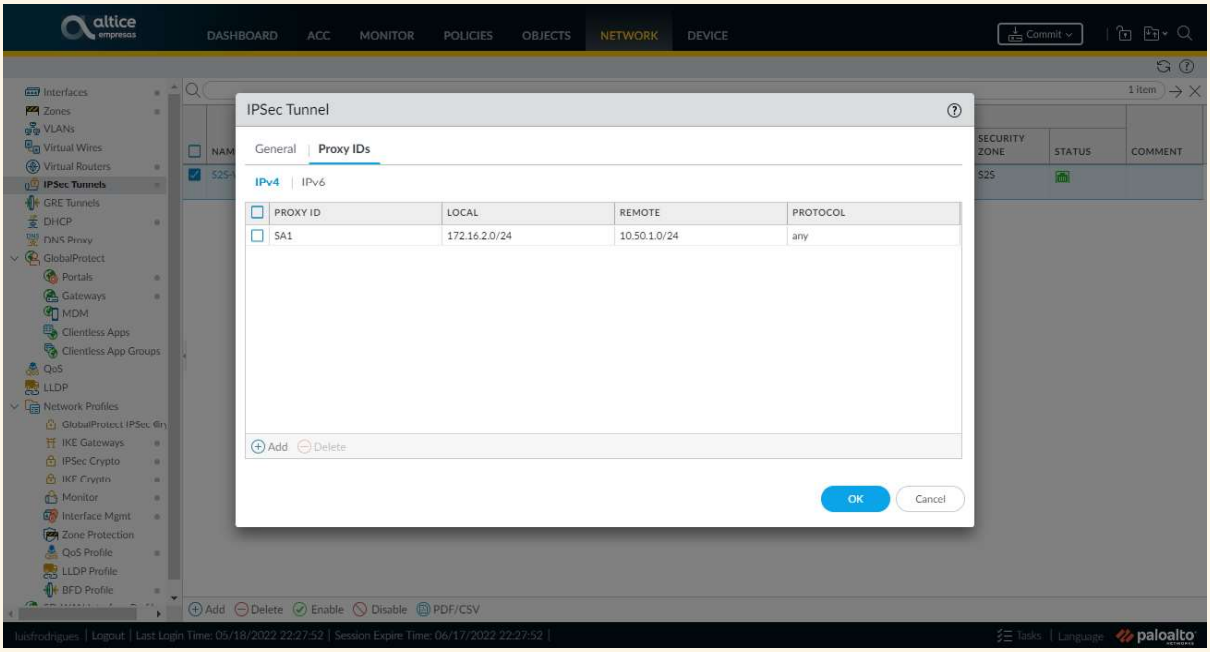


Preencha o campo “Proxy ID” com “SA1”, o campo “Local” com a nossa rede privada 172.16.2.0/24, o campo “Remote” com a rede remota 10.50.1.0/24 e clique em “OK”:



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.

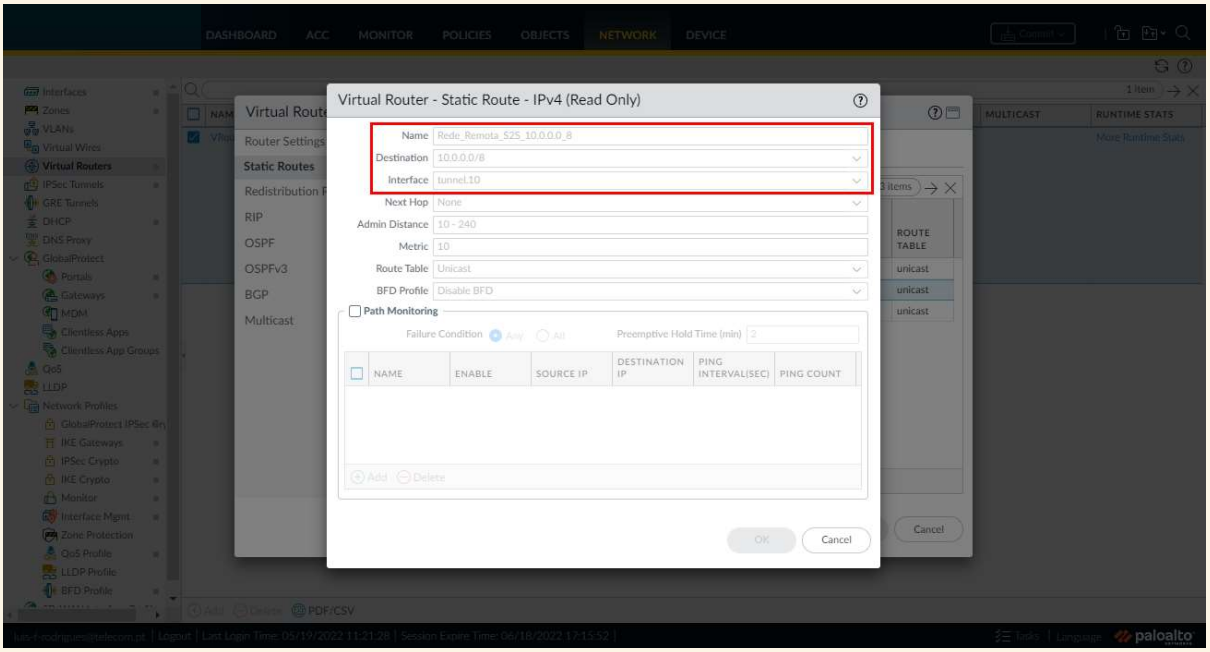
Clique em “OK” para fechar o diálogo de configuração do túnel IPSec:



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.

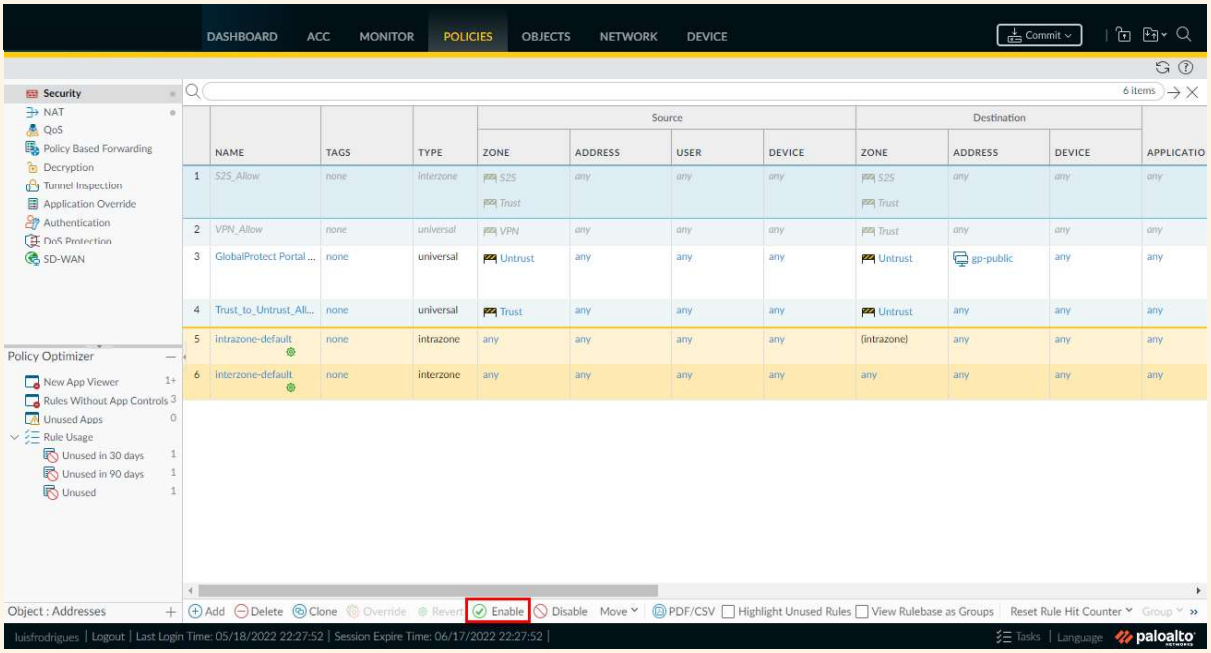
Para este túnel IPSec “S2S-VDC1” já se encontram pré-configuradas rotas estáticas IPv4 no Virtual Router “VRouter1” da firewall de modo a encaminhar o tráfego com destino às gamas de endereçamento privado IPv4 10.0.0.0/8 e 192.168.0.0/16 pela interface “tunnel.10”.

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



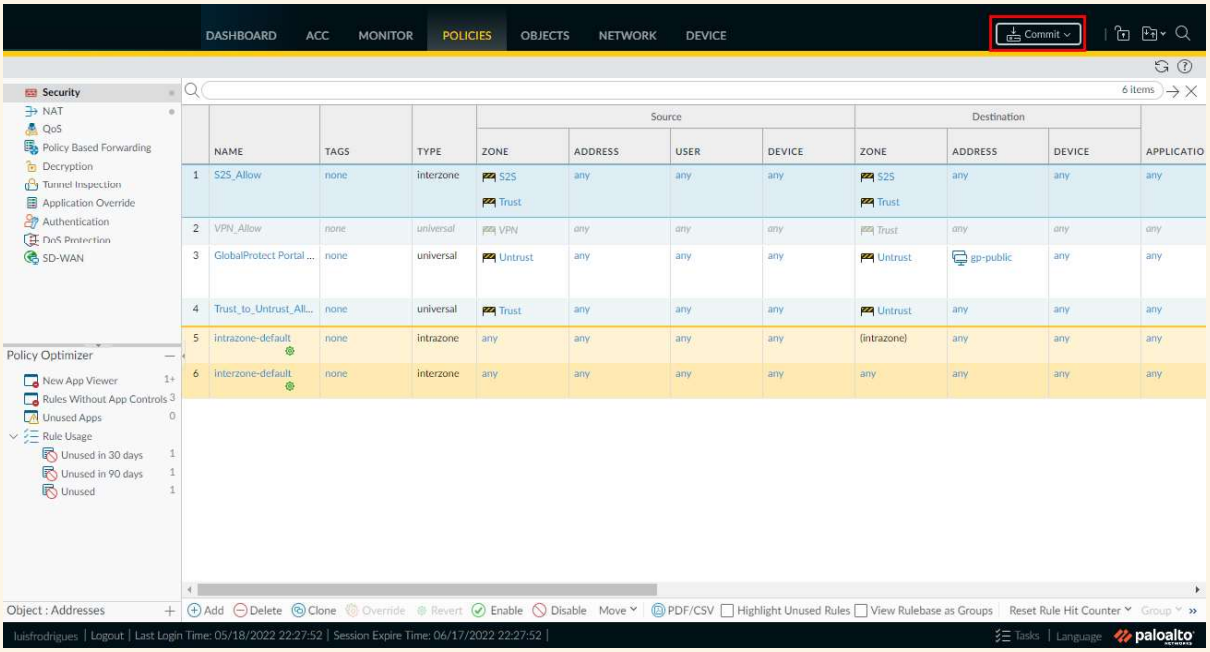
É também necessária uma regra de segurança a permitir o tráfego da VPN entre a nossa rede local e a rede remota. Já se encontra previamente configurada uma regra de segurança para este túnel IPSec "S2S-VDC1", sendo apenas necessário ativá-la.

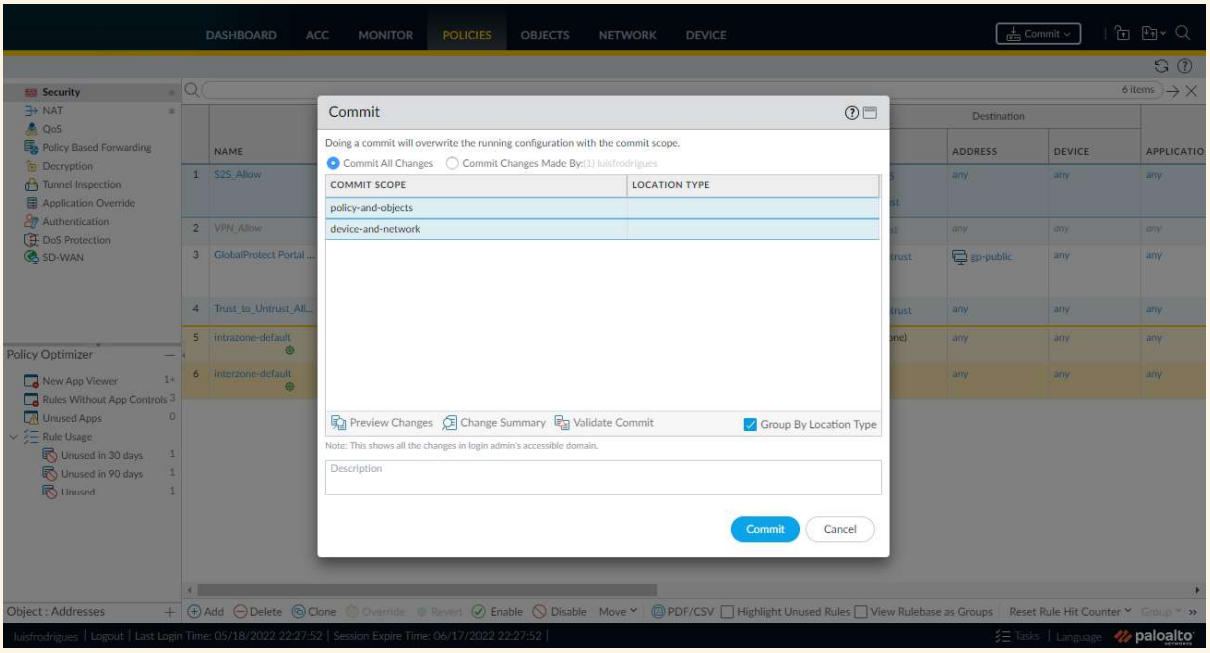
Selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Selecione a regra de segurança pré-configurada de nome "S2S_Allow" clicando sobre o número dela (1). Clique em "Enable" para ativar a regra:



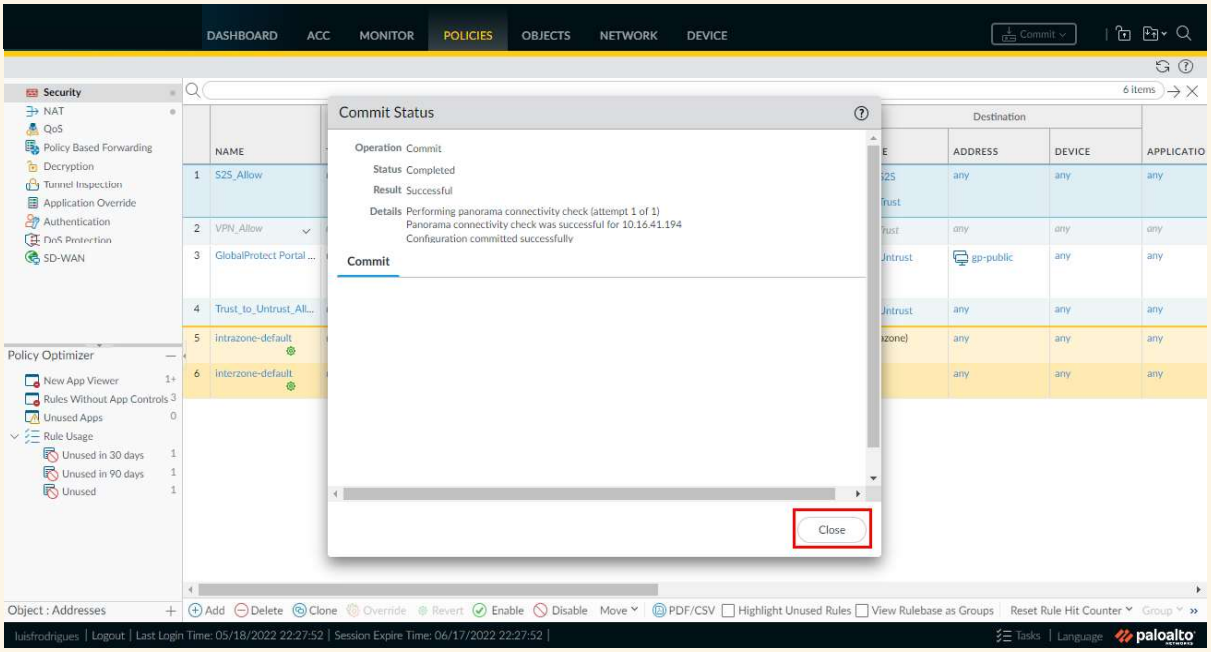
Na firewall remota também deve haver uma regra semelhante para permitir o tráfego do túnel VPN IPSec para a rede 10.50.1.0/24 e vice-versa.

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

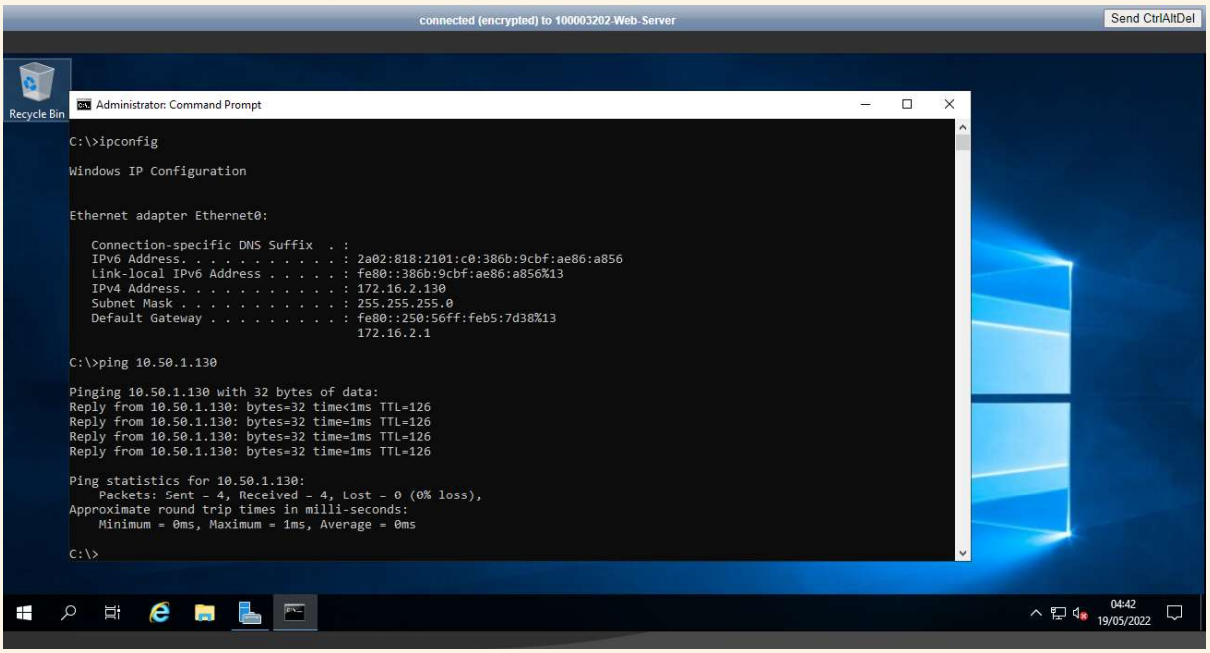




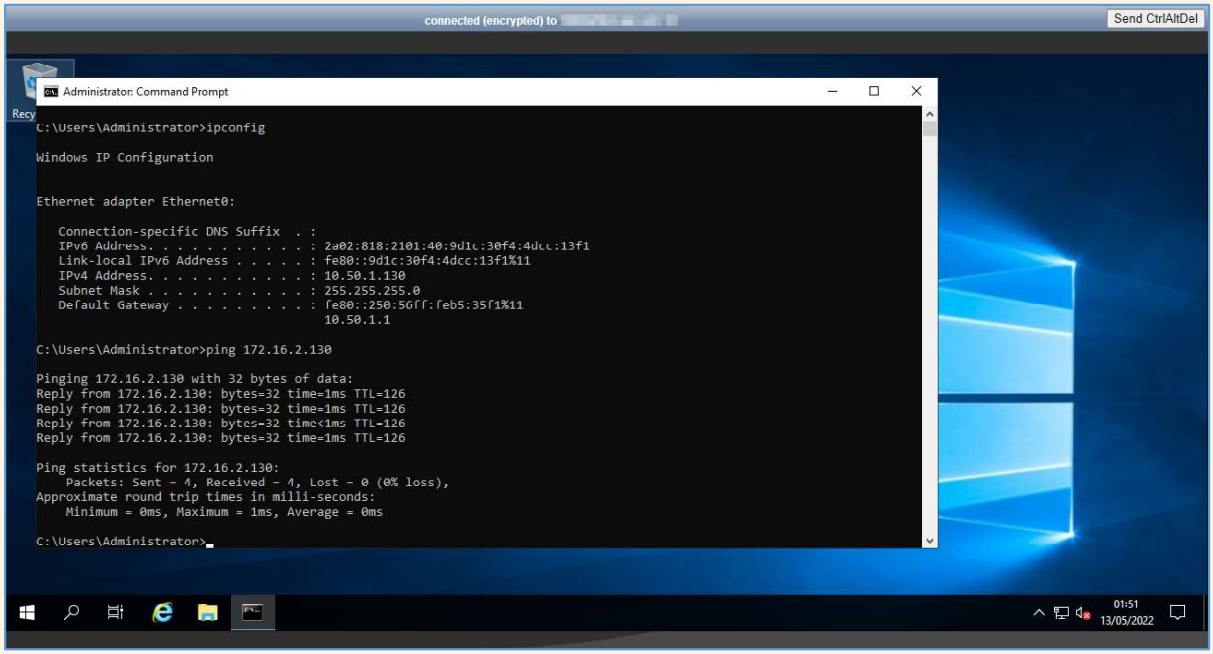
Quando o Commit estiver concluído, clique em “Close”:



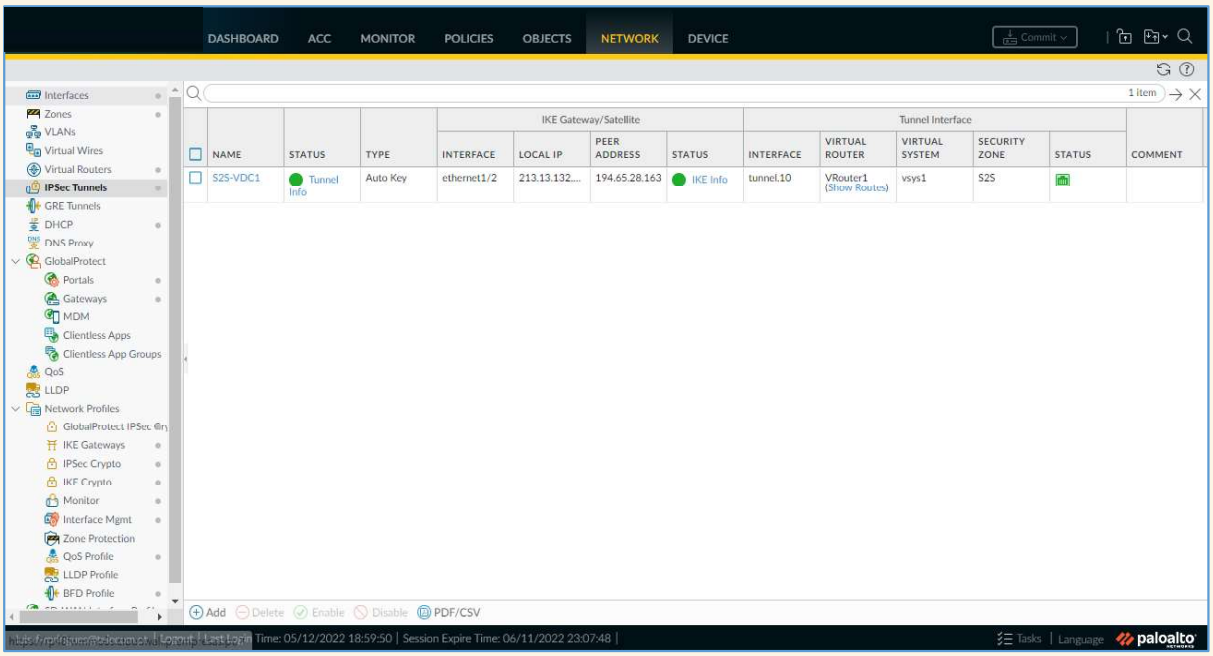
Para testar o túnel VPN IPSec, fazemos login no servidor web001 da nossa adesão e verificamos que conseguimos pingar o servidor remoto com o IP 10.50.1.130:



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



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:

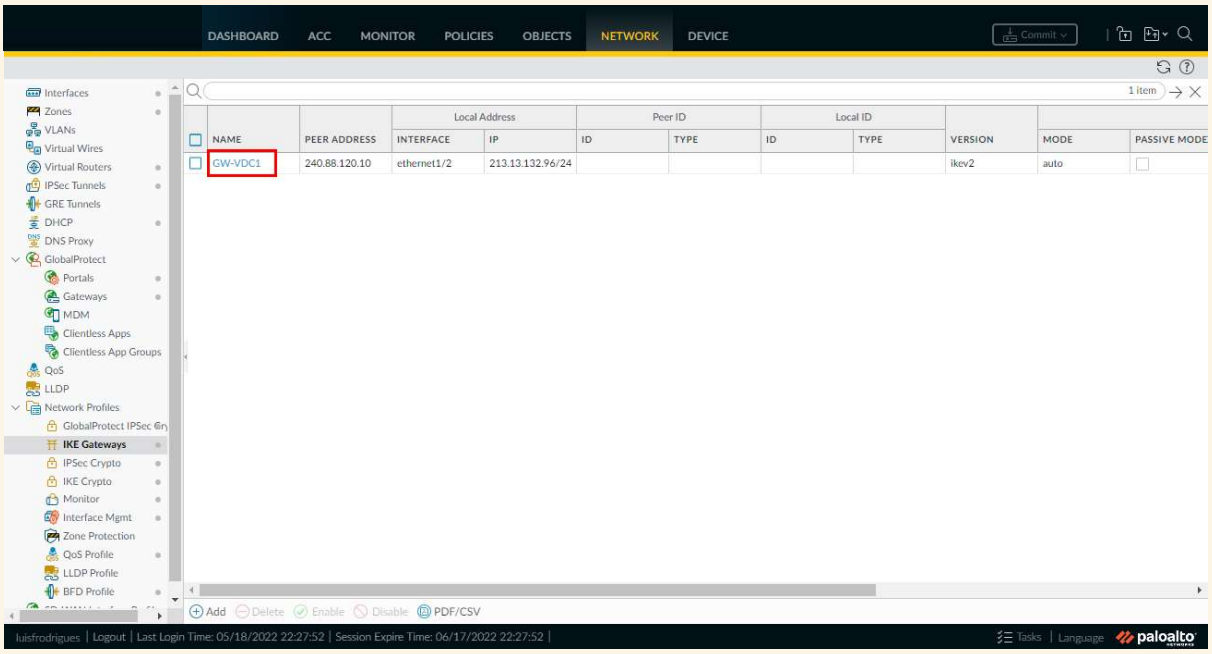


2.5.2. Túnel VPN IPSec pelo IP de IPv6

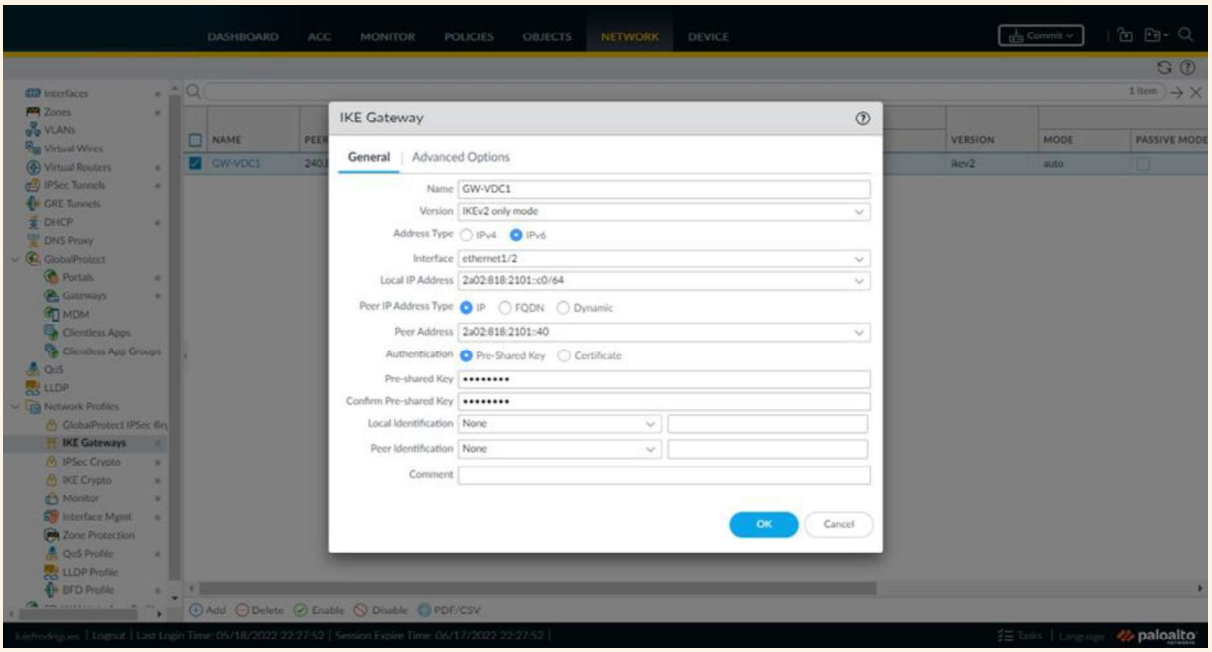
No exemplo que se segue vamos utilizar a pré-configuração do túnel VPN IPSec existente na firewall Palo Alto para ligar a nossa rede interna 2a02:818:2101:c0::/64 a uma rede remota **2a02:818:2101:40::/64** ligada noutra firewall. Na nossa rede interna encontra-se um servidor com o IP de IPv6 2a02:818:2101:c0:386b:9cbf:ae86:a856.

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":

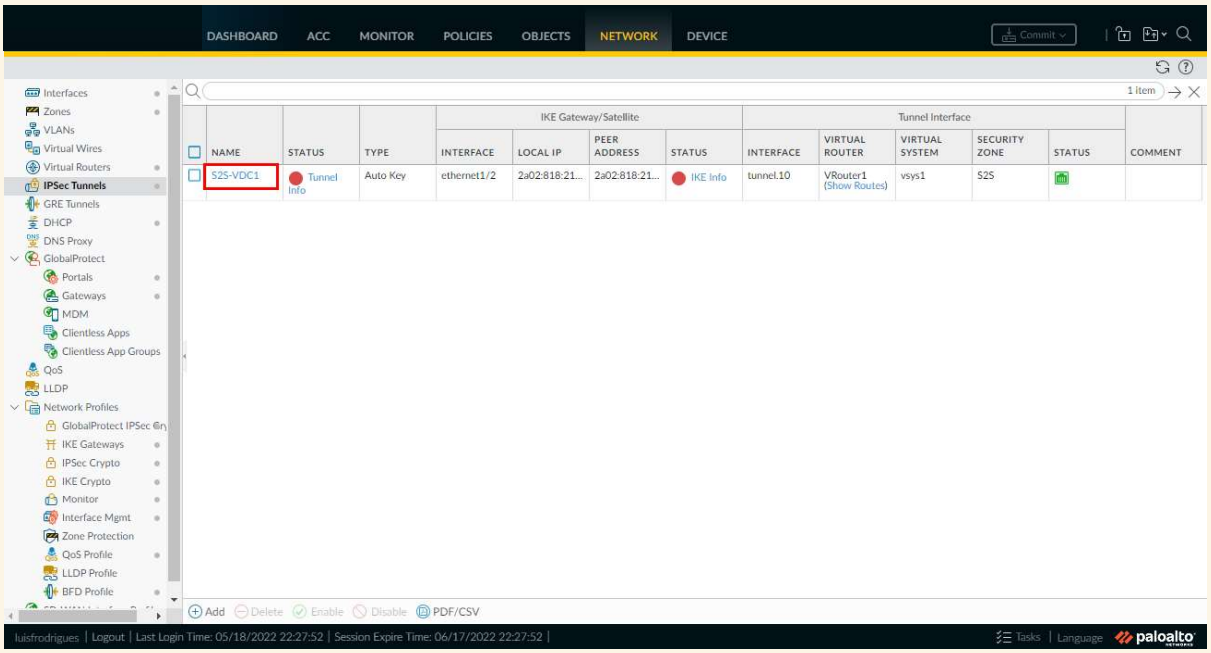


Selecione o "Address Type" IPv6, selecione o "Local IP Address" IPv6 da ethernet1/2, introduza o endereço IP de IPv6 da firewall remota no campo "Peer Address" e a Pre-shared Key no campo respetivo. Clique em "OK":

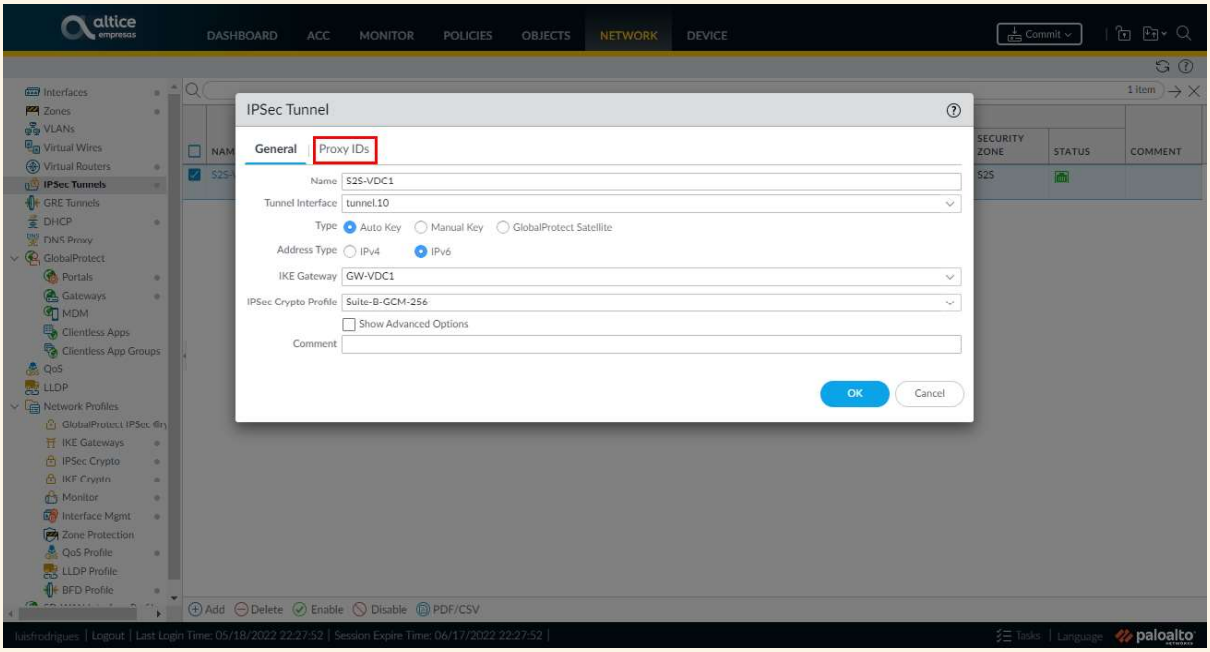


Na firewall remota também devem ser configurados o "Peer Address" com o IP de IPv6 da nossa firewall Palo Alto e a Pre-shared Key.

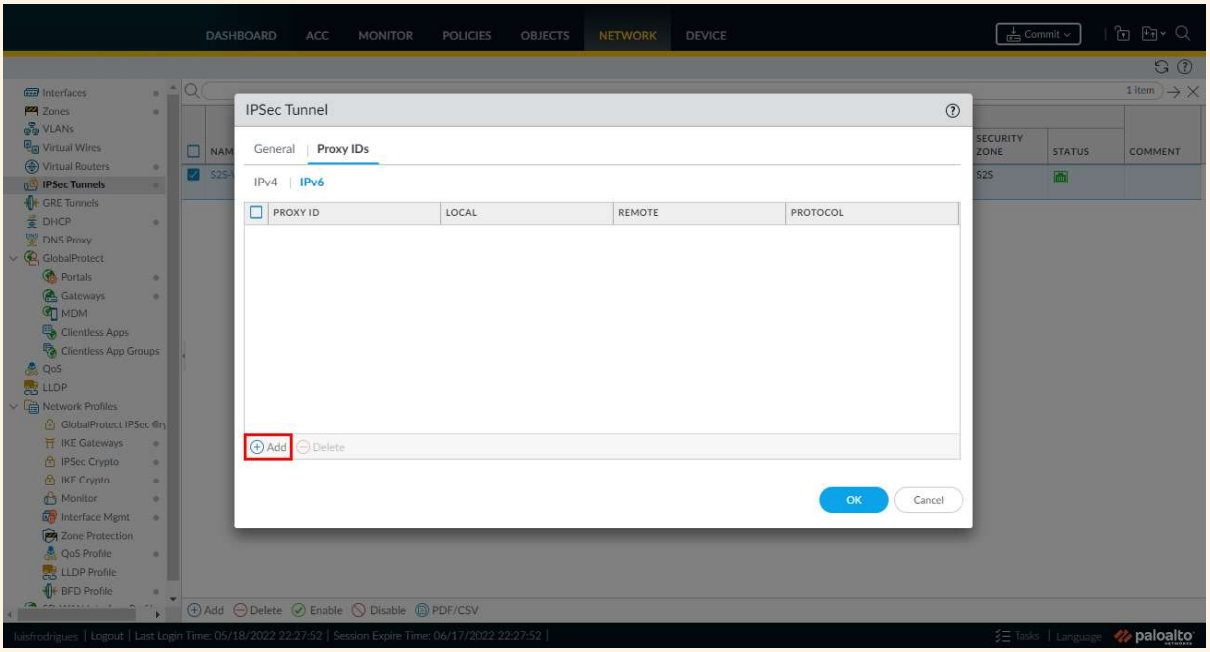
No menu da esquerda, selecione a opção "IPSec Tunnels" e clique no túnel de nome "S2S-VDC1":



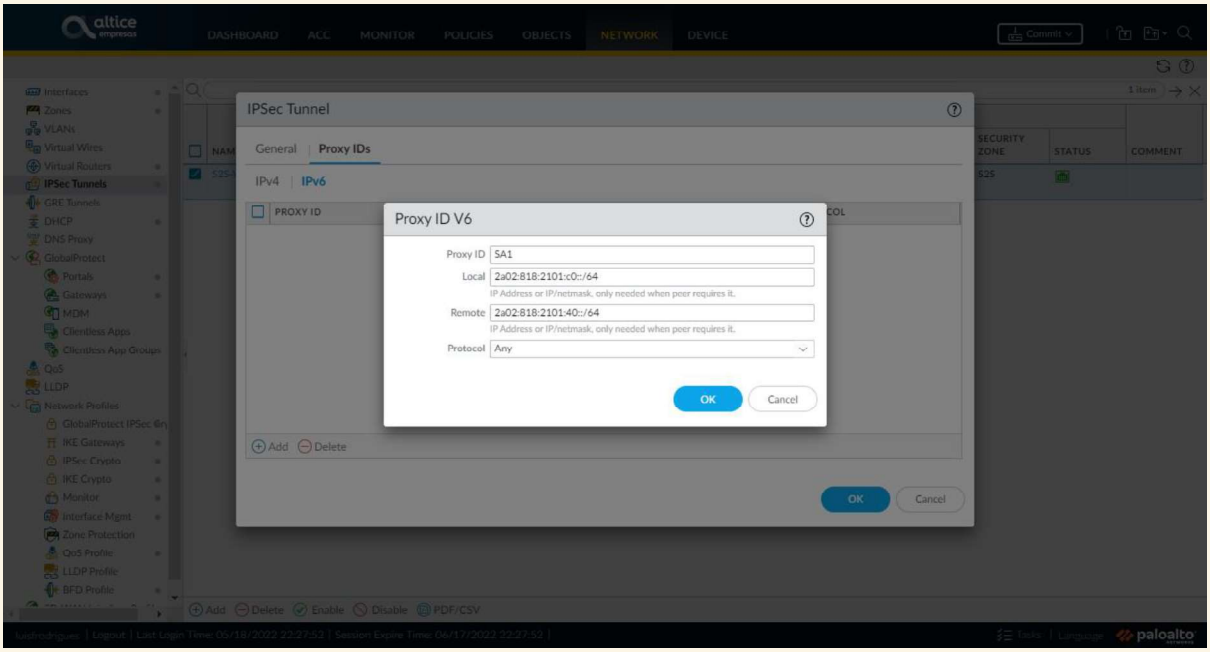
Selecione o "Address Type" IPv6 e selecione a "IKE Gateway" GW-VDC1. A seguir selecione a aba "Proxy IDs":



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

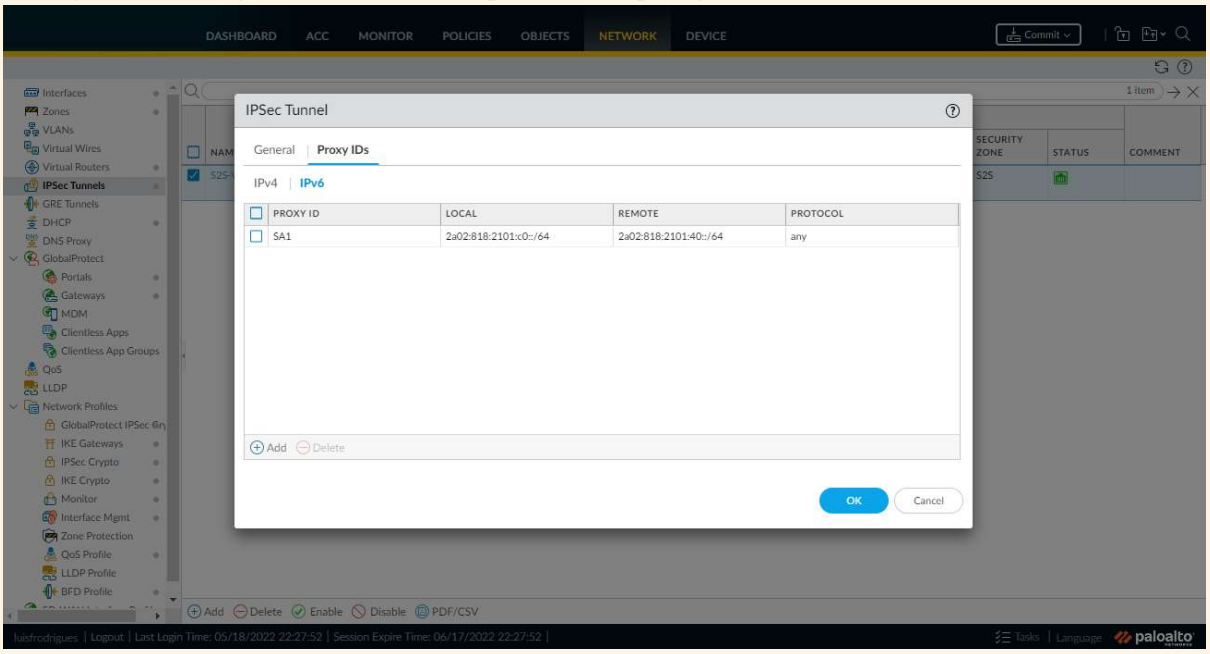


Preencha o campo “Proxy ID” com “SA1”, o campo “Local” com a nossa rede interna 2a02:818:2101:c0::/64, o campo “Remote” com a rede remota 2a02:818:2101:40::/64 e clique em “OK”:



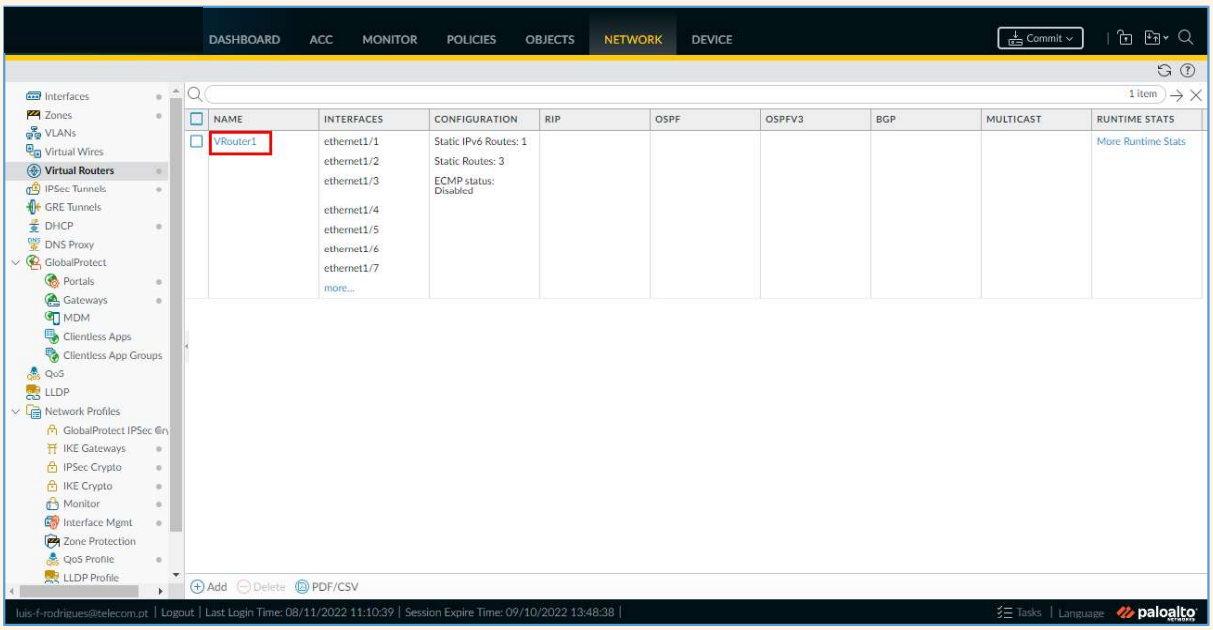
Na firewall remota também deve ser feita esta configuração do Proxy ID "SA1", mas colocando como "Remote" a nossa rede 2a02:818:2101:c0::/64.

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

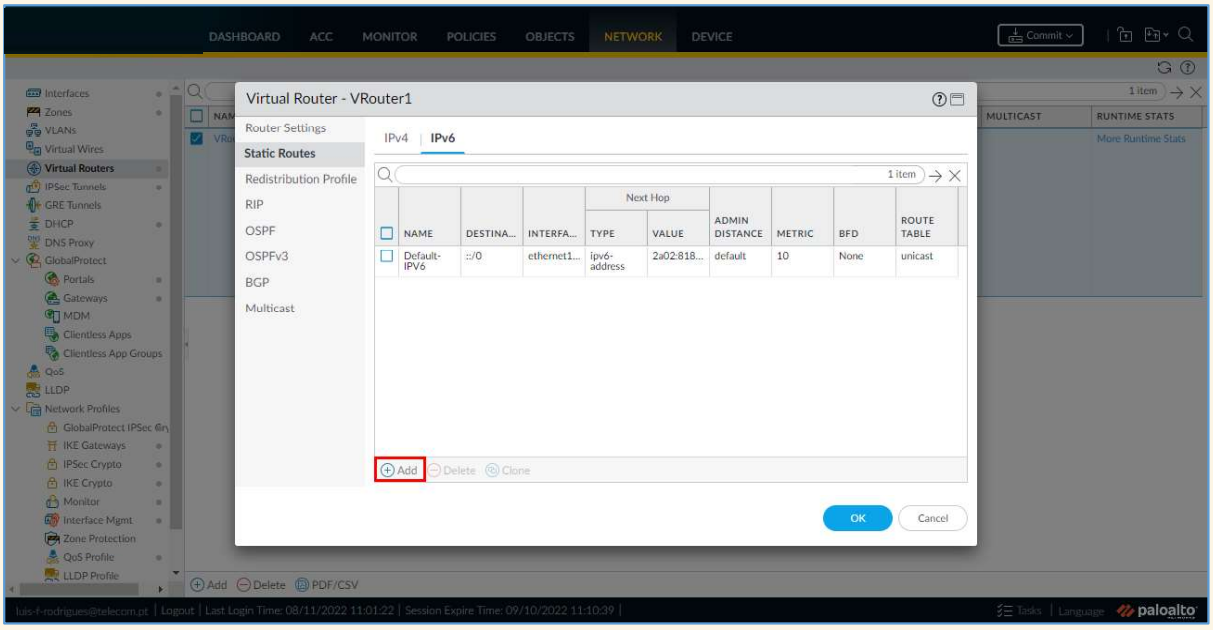


Para que o tráfego com destino à rede remota 2a02:818:2101:40::/64 seja corretamente encaminhado pelo túnel IPSec é necessário adicionar uma rota estática no Virtual Router.

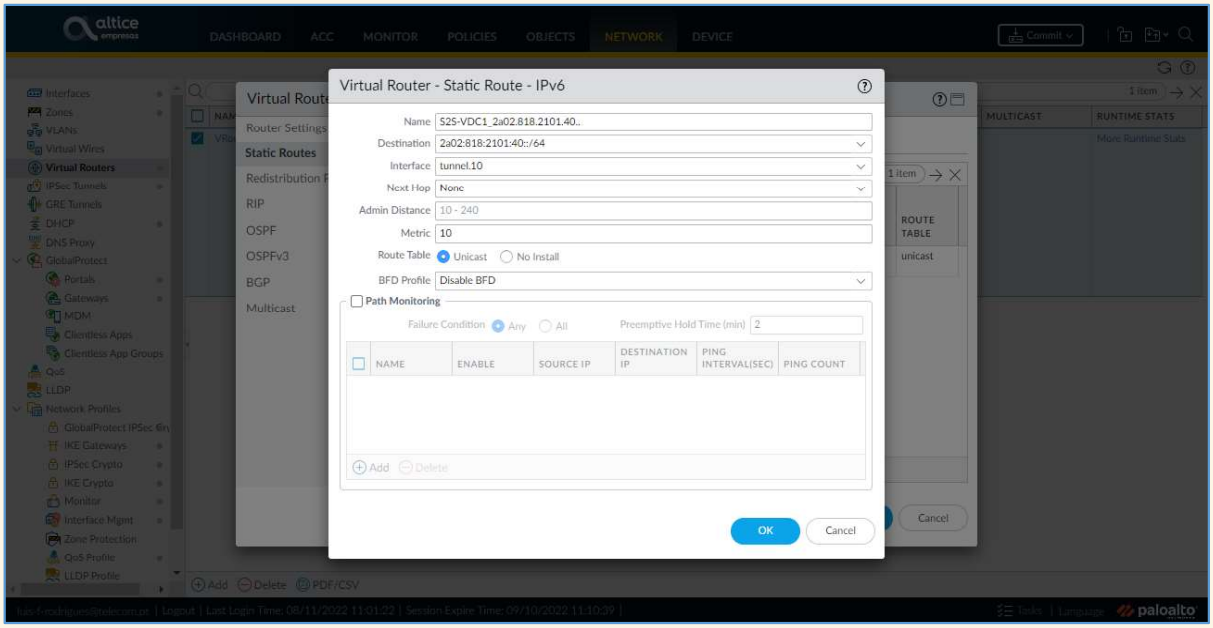
No menu da esquerda, selecione a opção "Virtual Routers" e clique no router de nome "VRouter1":



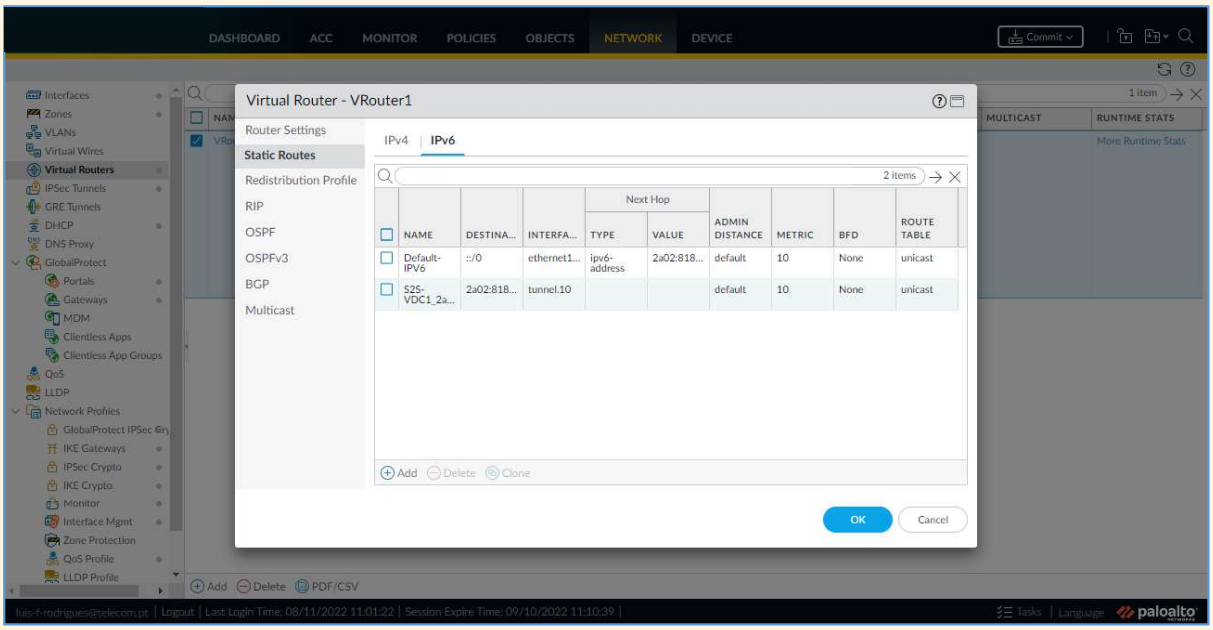
Selecione a opção “Static Routes”, selecione a aba “IPv6” e clique em “Add” para adicionar uma rota nova:



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”:

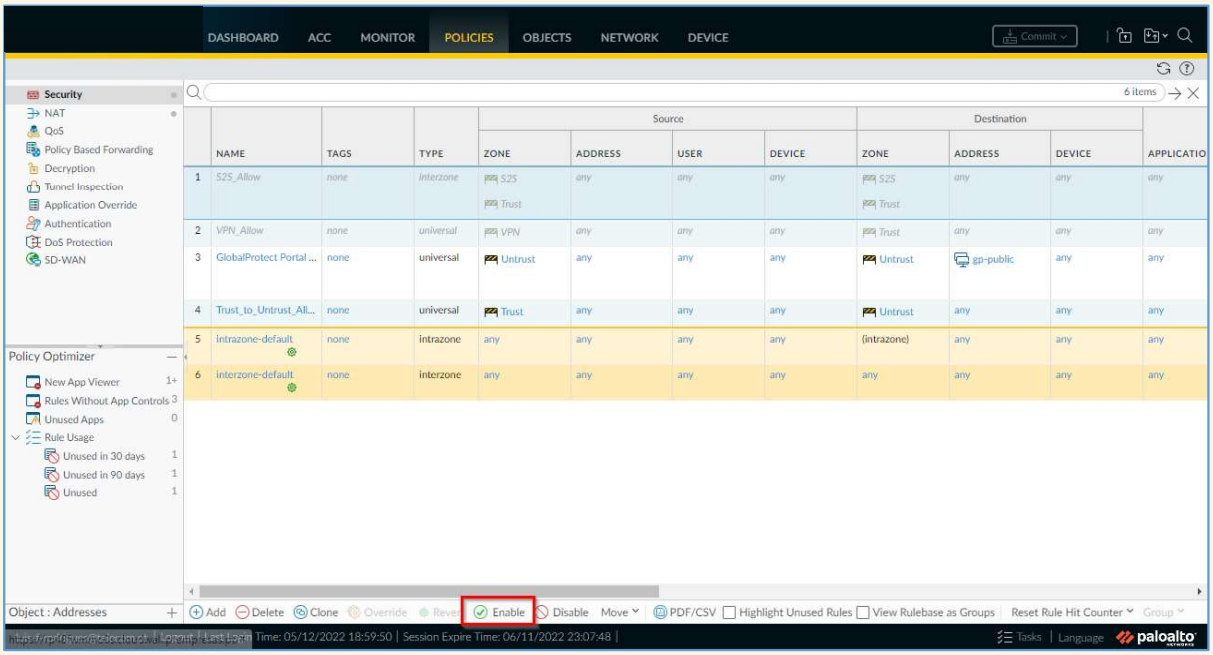


Clique em "OK" para fechar o diálogo de configuração do Virtual Router:



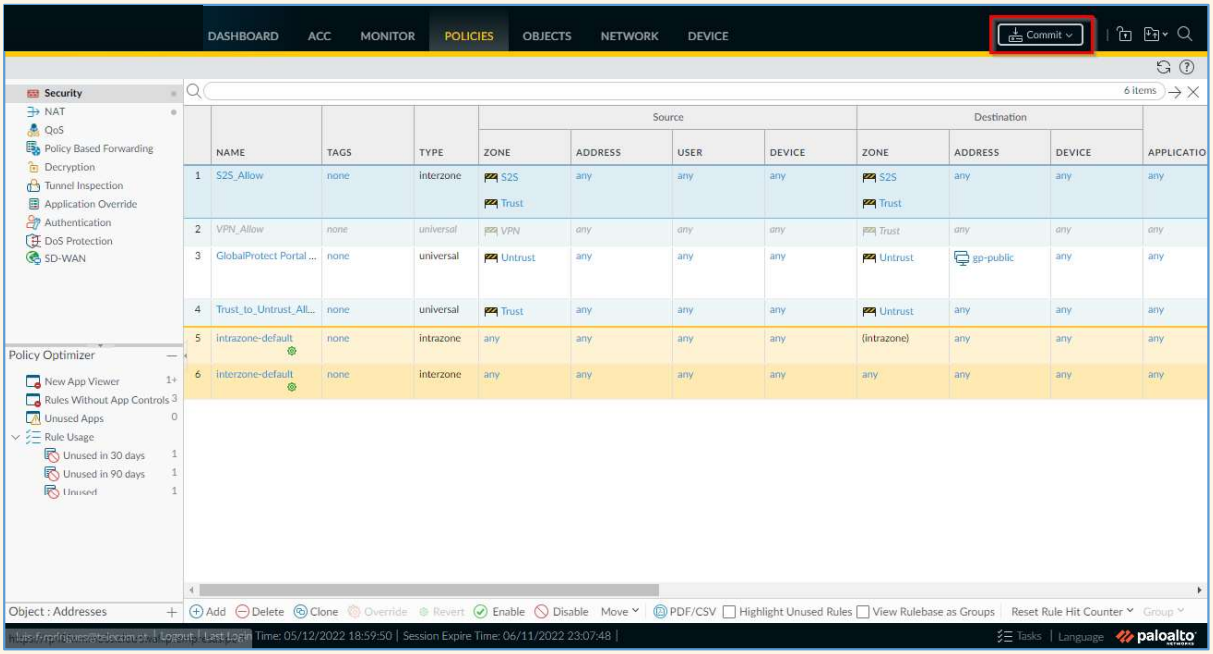
De seguida vamos ativar a regra de segurança que irá permitir o tráfego da VPN entre a nossa rede local e a rede remota.

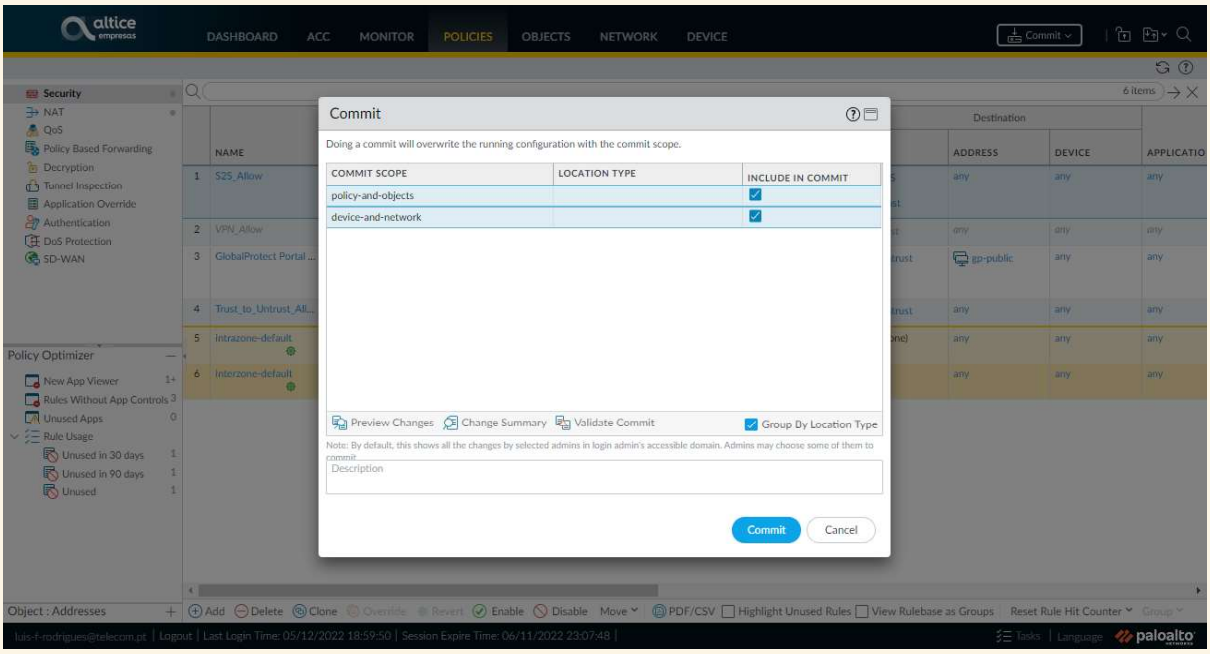
Selecione a aba "POLICIES" e no menu à esquerda selecione a opção "Security". Selecione a regra de segurança pré-configurada de nome "S2S_Allow" clicando sobre o número dela (1). Clique em "Enable" para ativar a regra:



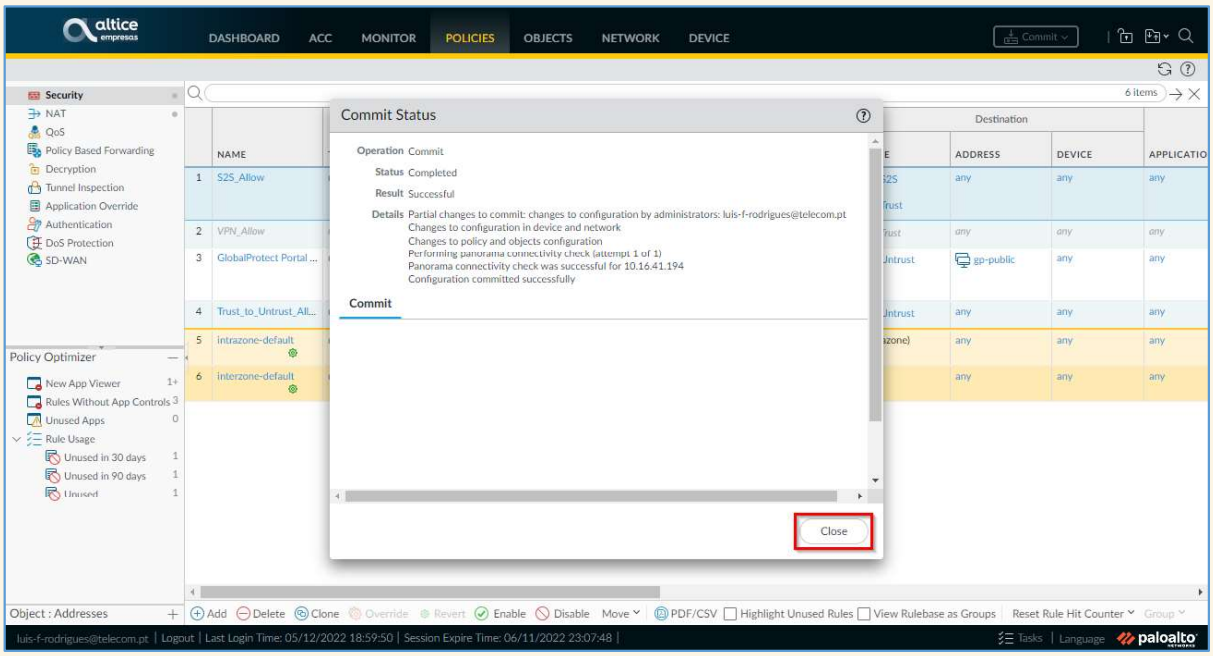
Na firewall remota também deve haver uma regra semelhante para permitir o tráfego do túnel VPN IPSec para a rede 2a02:818:2101:40::/64 e vice-versa.

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

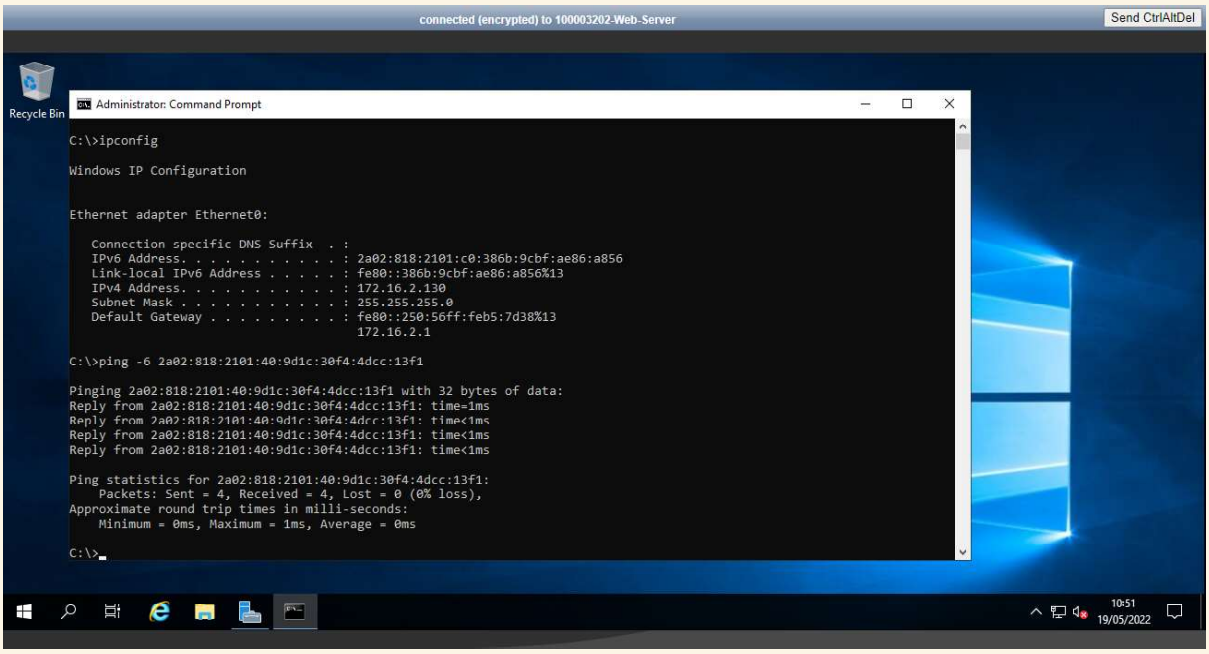




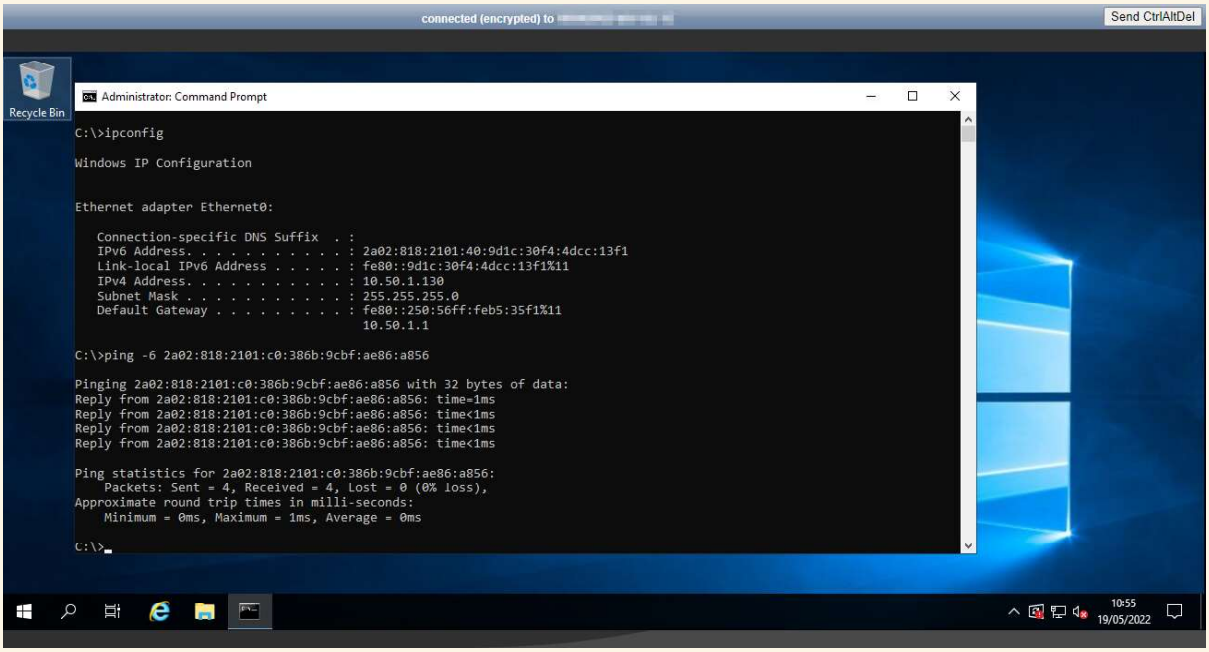
Quando o Commit estiver concluído, clique em "Close":



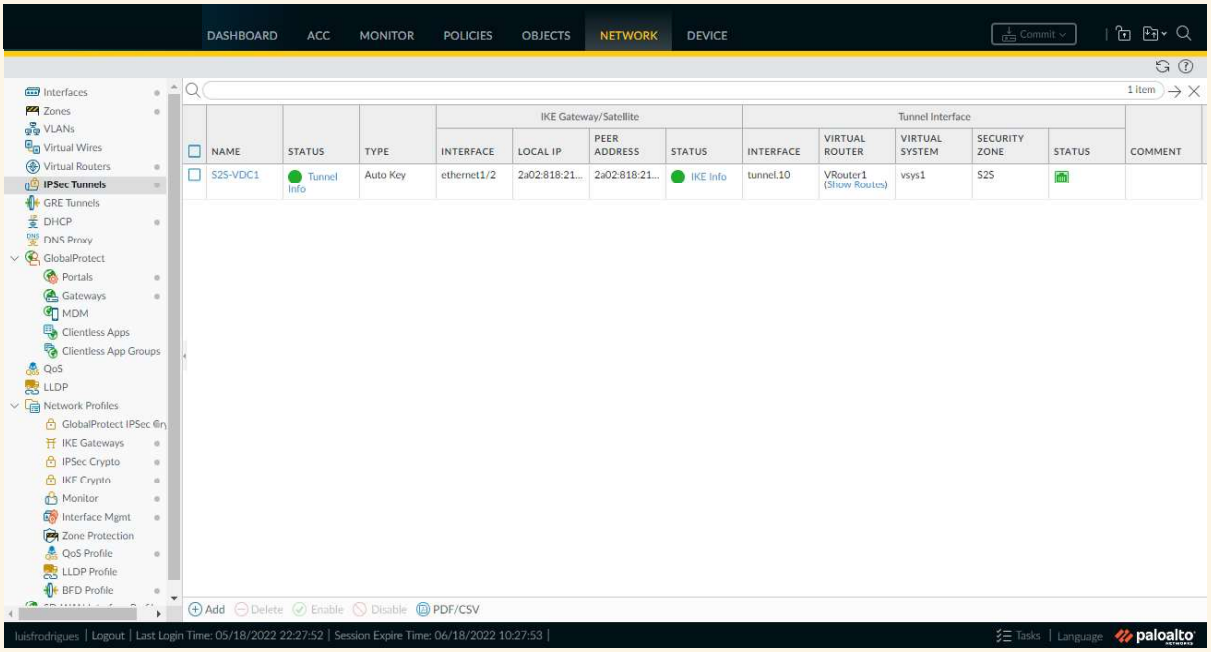
Para testar o túnel VPN IPSec, fazemos login no servidor web001 da nossa adesão e verificamos que conseguimos pingar o servidor remoto com o IP 2a02:818:2101:40:9d1c:30f4:4dcc:13f1:



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



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:



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"

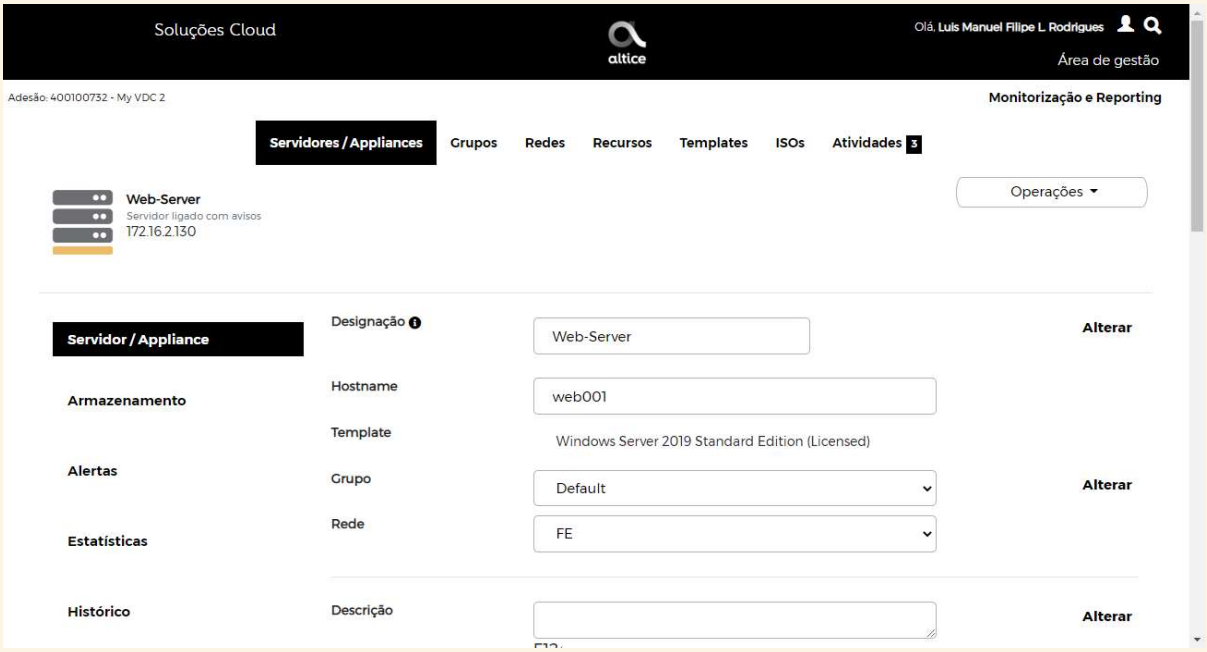
Os eventos relacionados com VPNs podem ser consultados na aba "MONITOR" » opção "Logs | System" do menu à esquerda.

2.6. Como faço para me ligar com um cliente VPN aos Servidores Privados da minha Adesão?

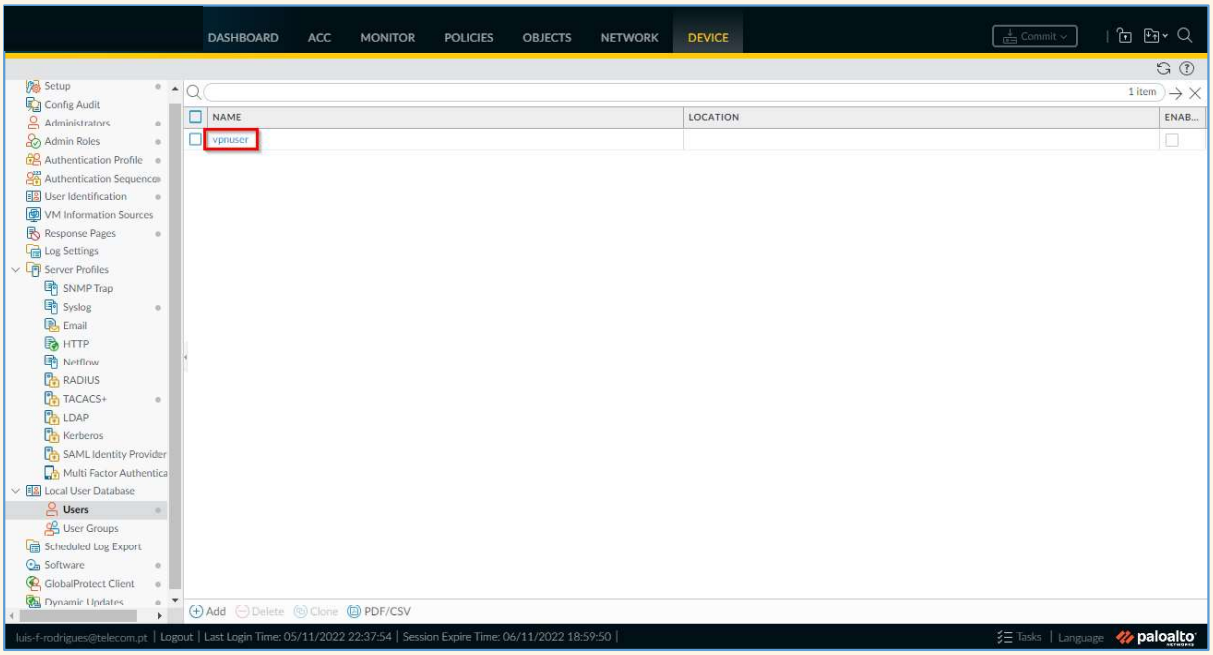
2.6.1. VPN GlobalProtect pelo IP público de IPv4 (só nas adesões onde este foi adquirido)

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.

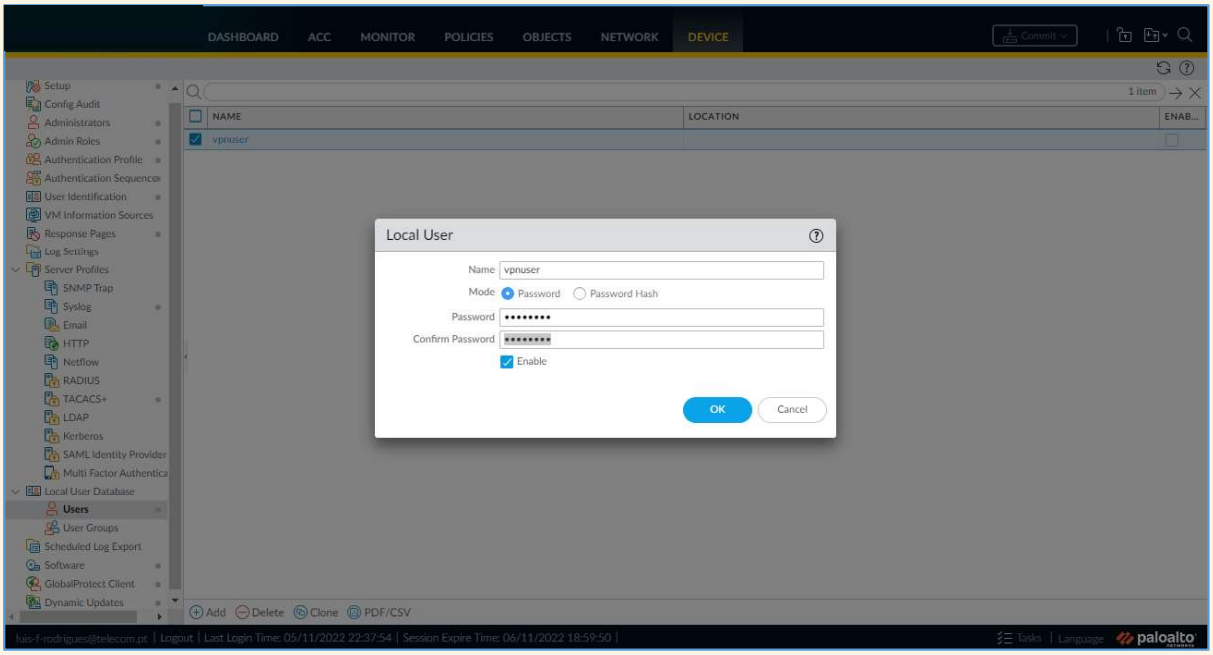
No exemplo que se segue a nossa firewall Palo Alto tem o IP público de IPv4 213.13.132.96 e vamos utilizar a pré-configuração existente na firewall para ligar um PC cliente com Internet, por VPN, à rede privada 172.16.2.0/24 da adesão. Nesta rede privada encontra-se um servidor privado com sistema operativo 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:



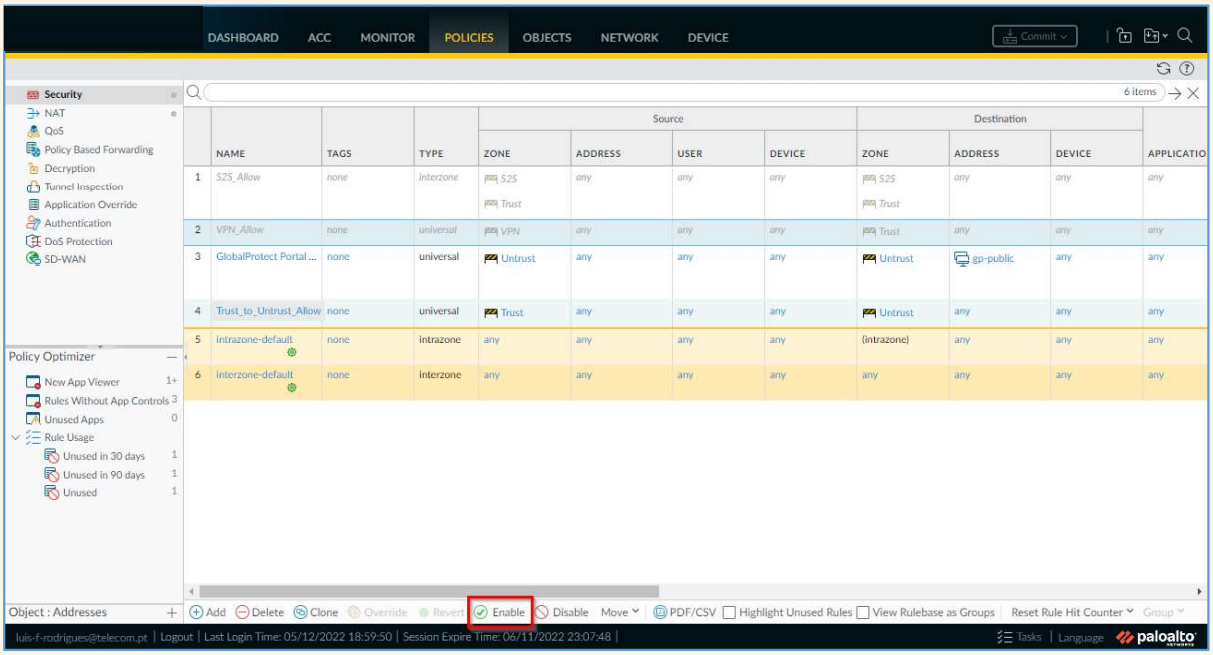
Vamos ativar a conta de VPN pré-configurada para fazer login no Portal e no agente GlobalProtect. Faça login na firewall. Selecione a aba "DEVICE" e no menu à esquerda selecione a opção "Local User Database » Users". Clique na conta "vpnuser":



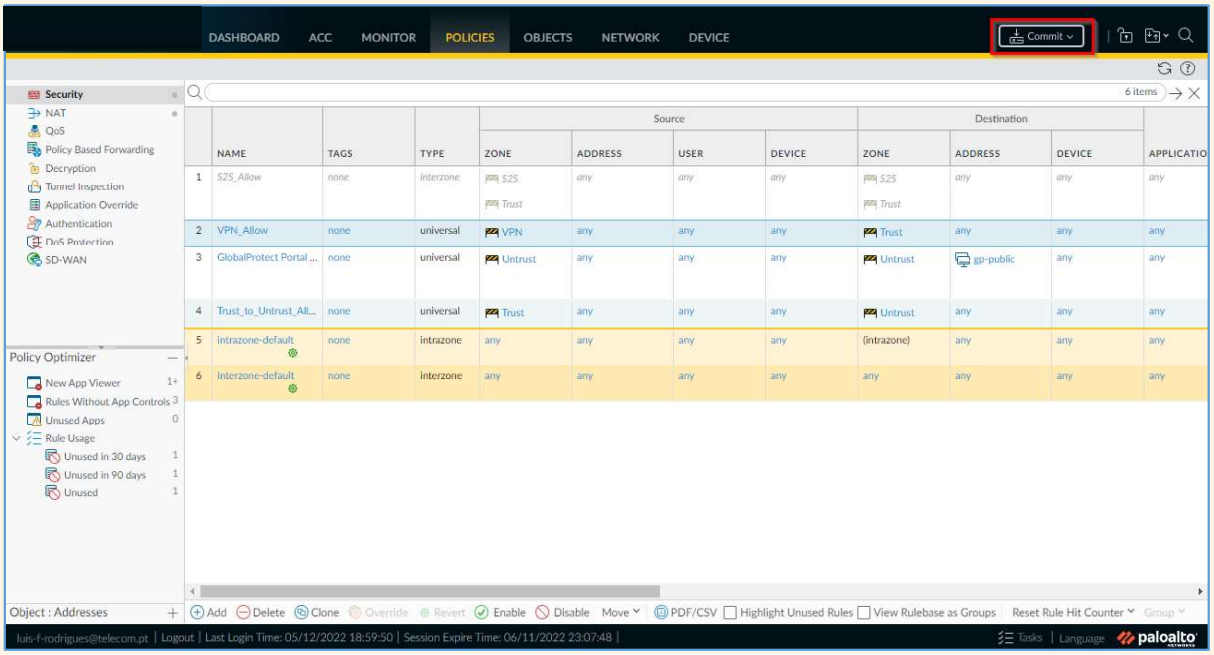
Ative a conta (“Enable”), altere a password e clique em “OK”:

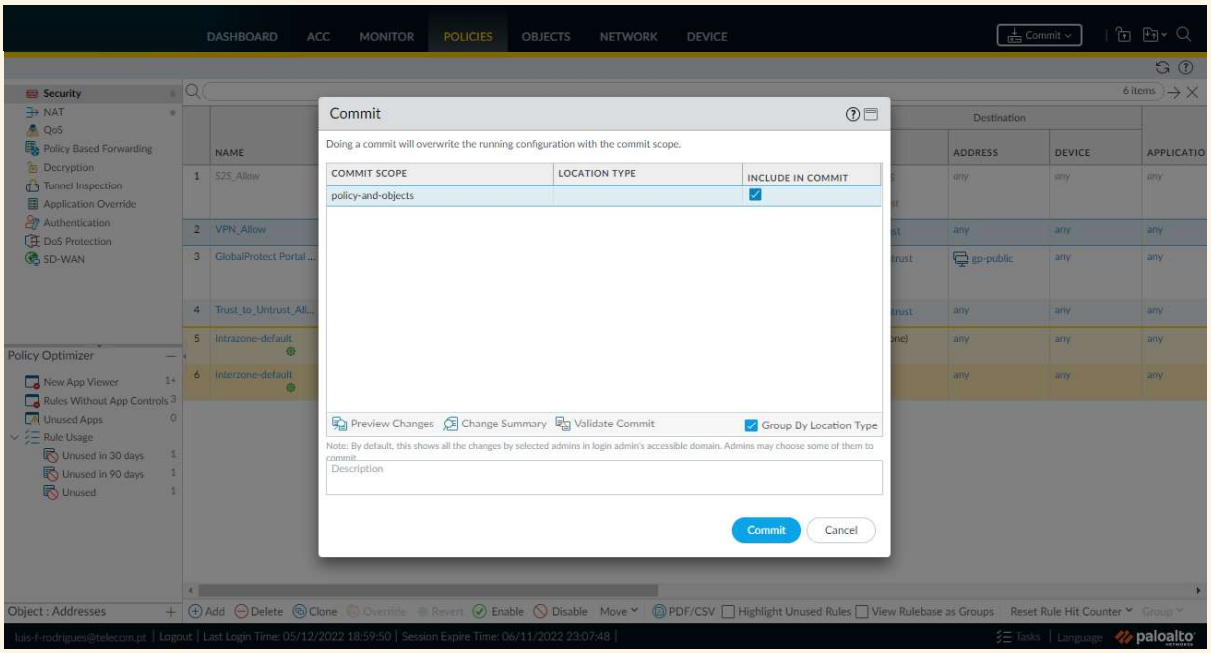


Agora selecione a aba “POLICIES” e no menu à esquerda selecione a opção “Security”. Selecione a regra de segurança pré-configurada de nome “VPN_Allow” clicando sobre o número dela (2). Clique em “Enable” para ativar a regra:

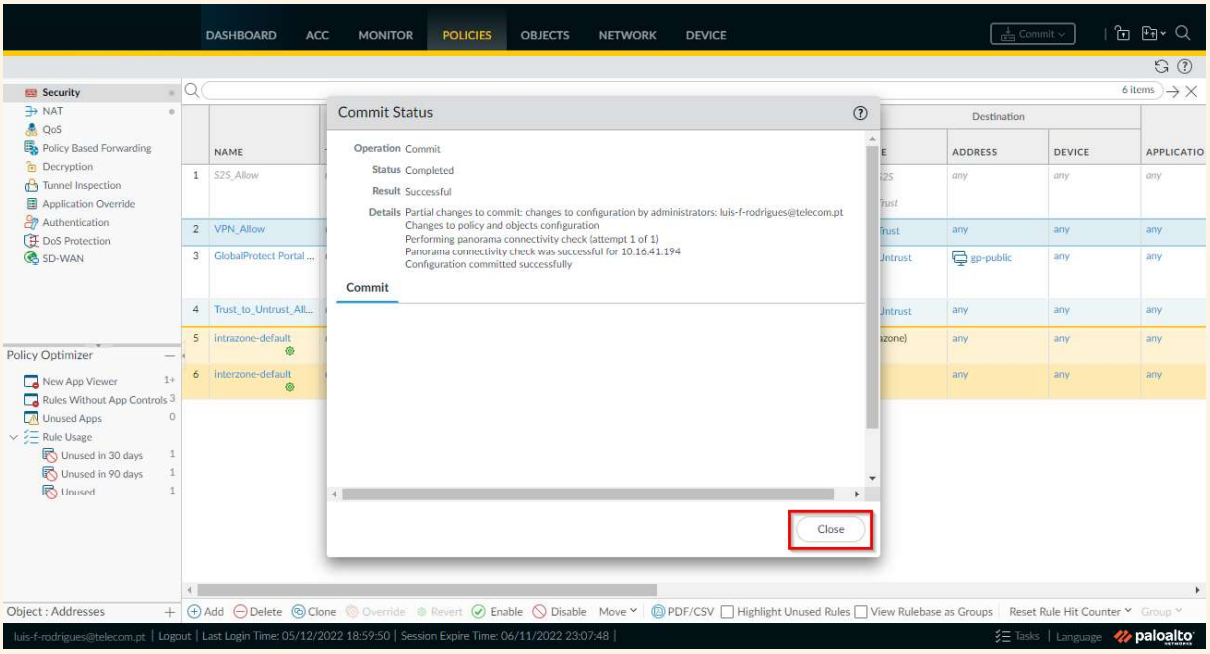


Para tornar as alterações efetivas, clique no botão “Commit” e na caixa de diálogo clique em “Commit”:

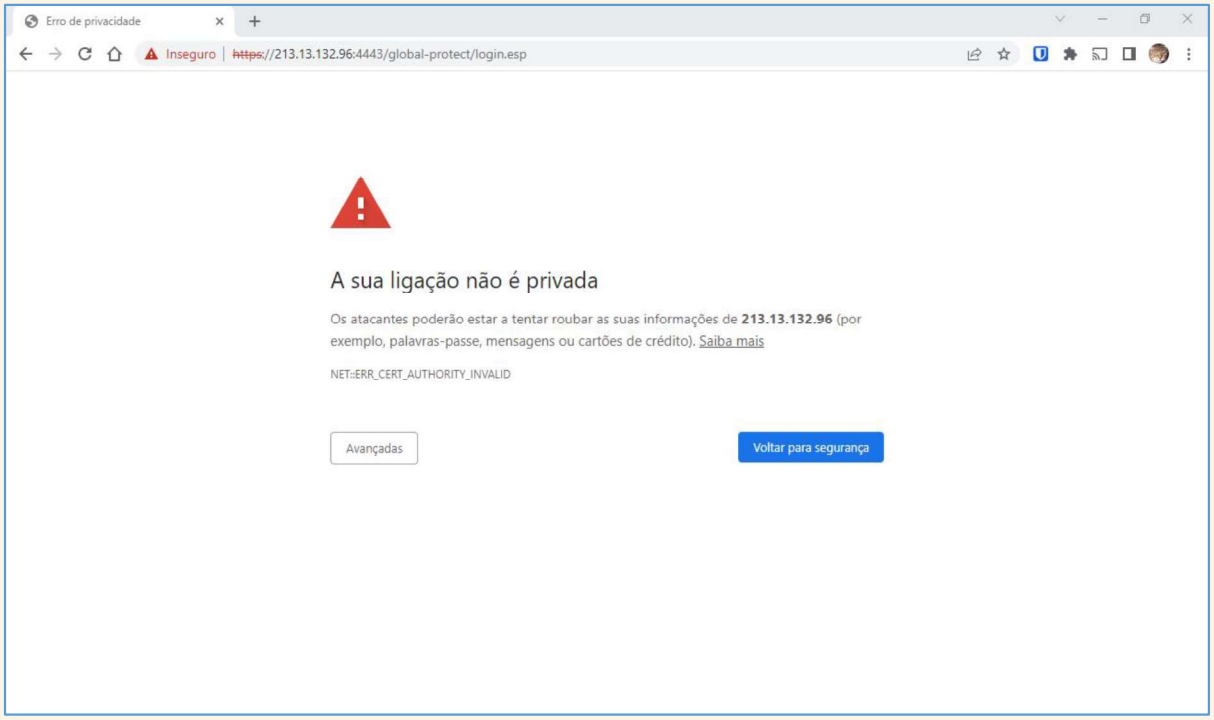




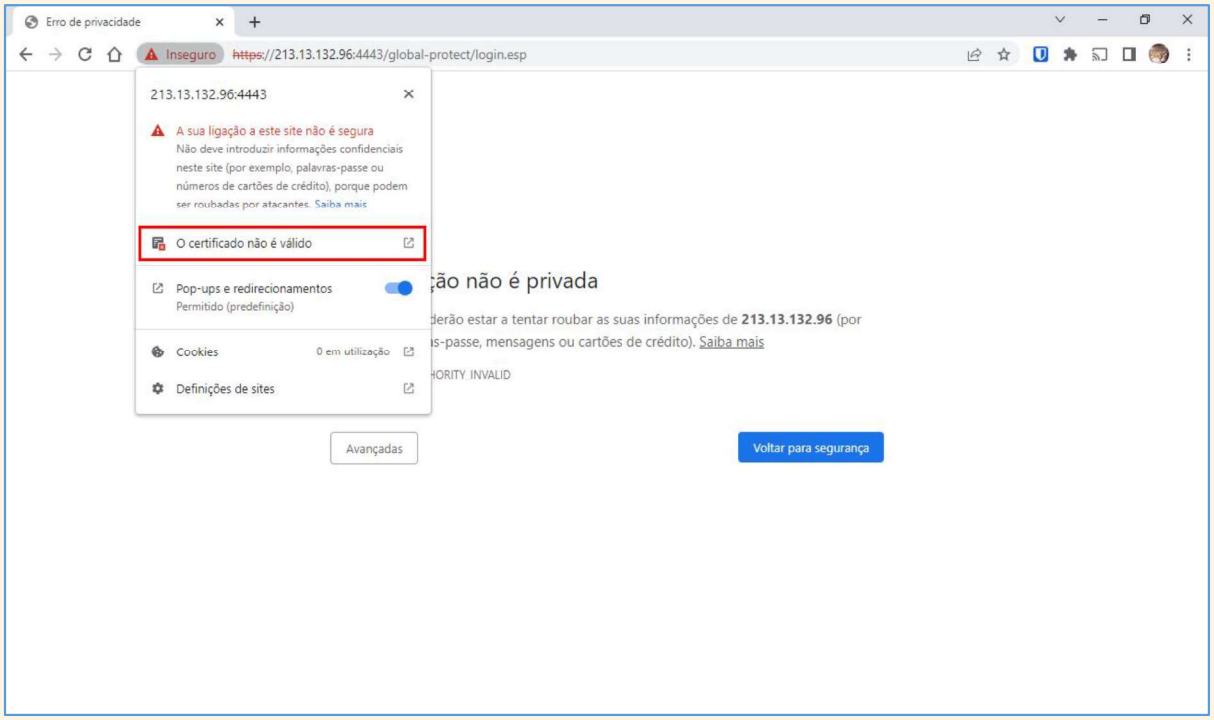
Quando o Commit estiver concluído, clique em "Close":



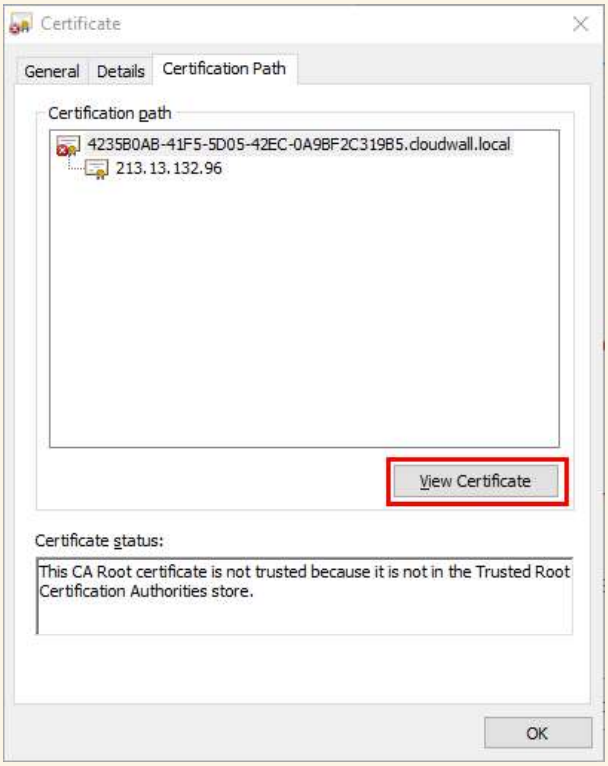
Abra uma janela de browser e introduza o URL com o seu IP Publico IPv4 da adesão no seguinte formato https://IPv4PublicodaAdesao:4443 (exemplo: https://213.13.132.96:4443). O browser irá indicar que a ligação não é privada. Isto deve-se ao certificado do portal ter sido emitido por uma Root CA self signed da própria firewall:



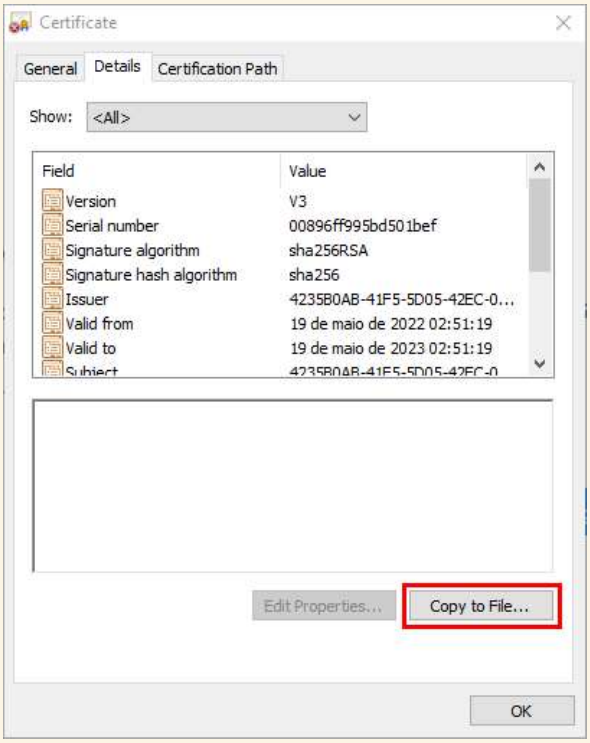
Para que os browsers deixem de apresentar este aviso e para o correto funcionamento posterior do agente GlobalProtect é necessário guardar o certificado da Root CA self signed na pasta dos Trusted Root Certification Authorities do PC cliente. Clique no aviso Inseguro que se encontra à esquerda do URL e de seguida clique em "O certificado não é válido":



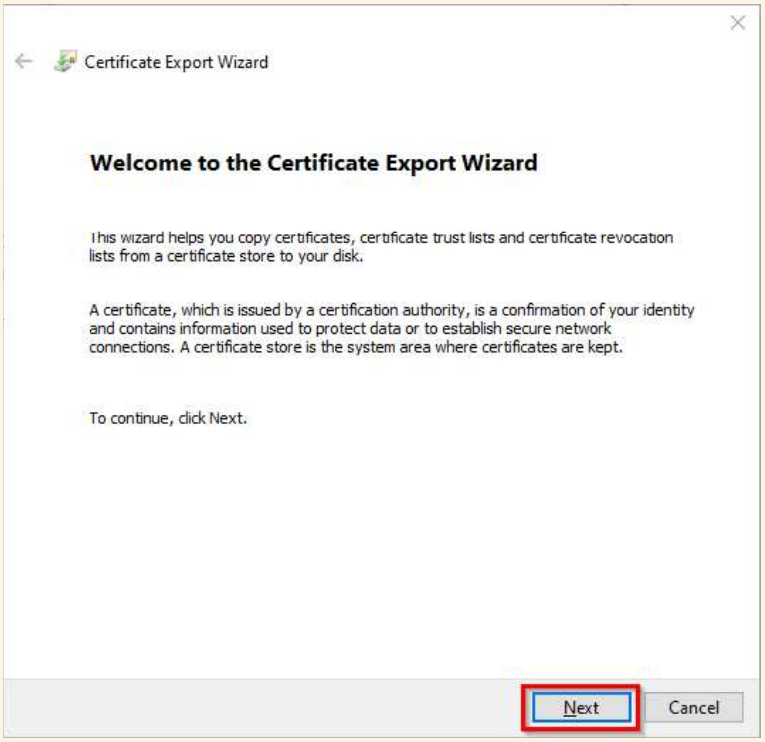
Selecione a aba “Certification Path”, selecione o certificado “4235B0AB-41F5-5D05-42EC-0A9BF2C319B5.cloudwall.local” e clique em “View Certificate”:



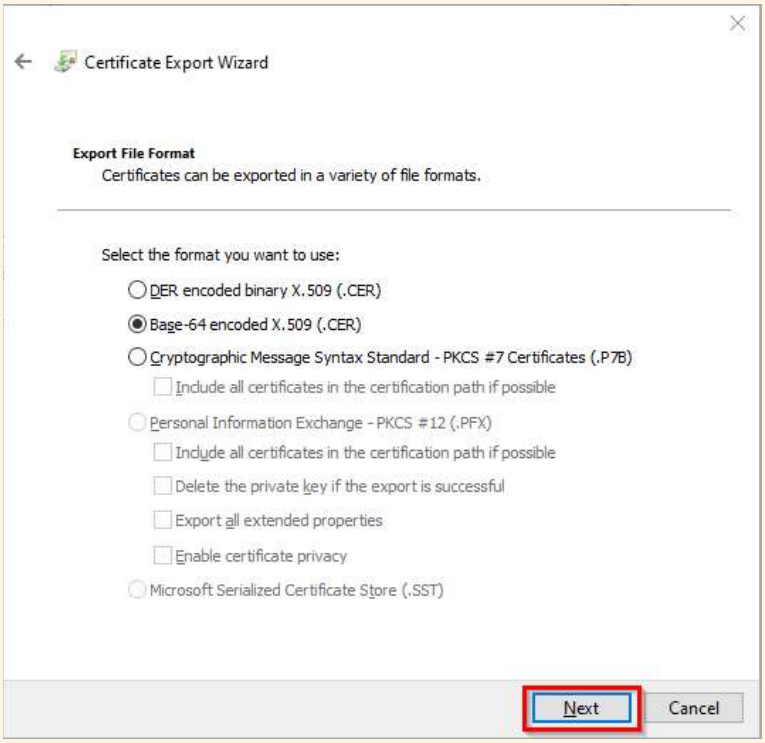
Selecione a aba “Details” e clique em “Copy to File...”:



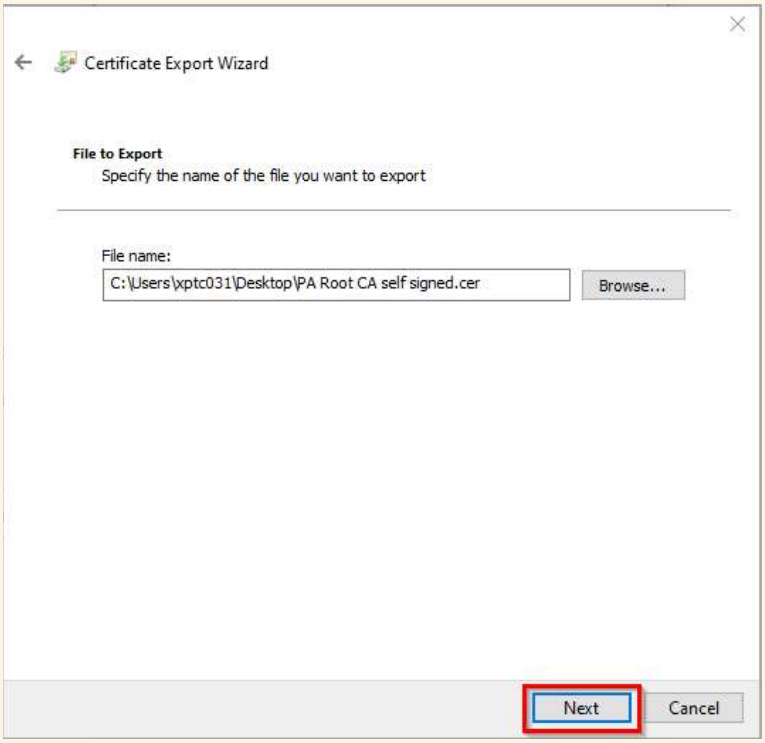
Irá ser executado o Certificate Export Wizard. Clique em “Next”:



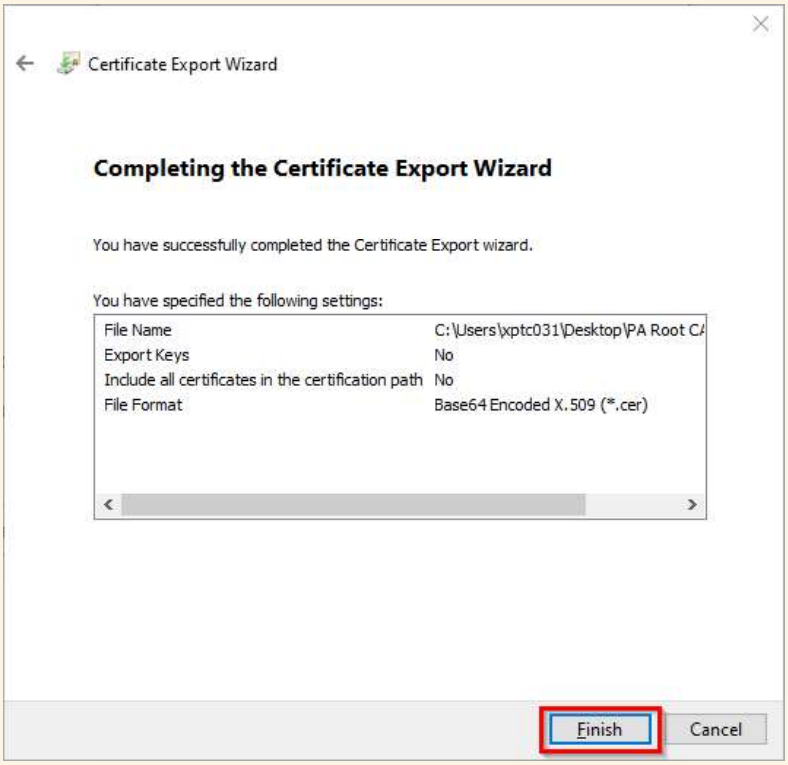
Selecione a opção “Base-64 encoded X.509 (.CER)” e clique em “Next”:



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



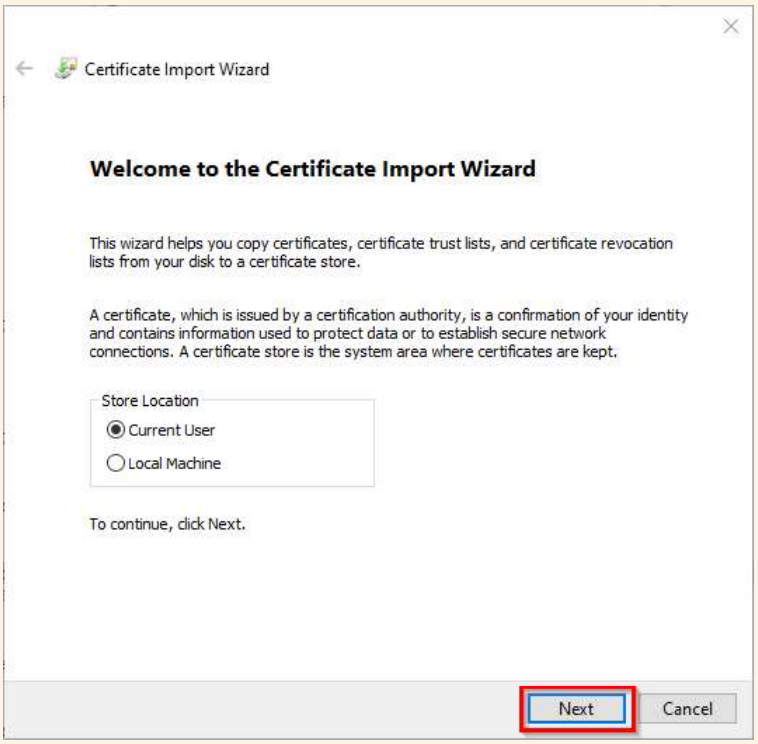
Clique em "Finish" para exportar o certificado:



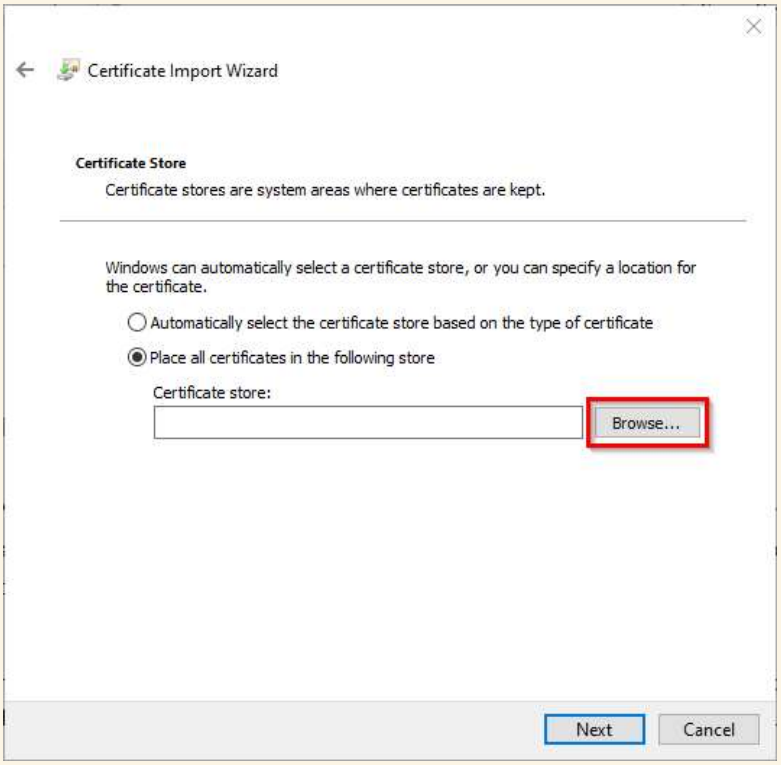
Se o seu PC cliente fizer parte de um domínio, poderá dar-se a situação de não ter privilégios para executar os passos de importação do certificado indicados a seguir. Se assim for, fale com o administrador do domínio Windows em que o seu PC se insere para ultrapassar a situação.

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

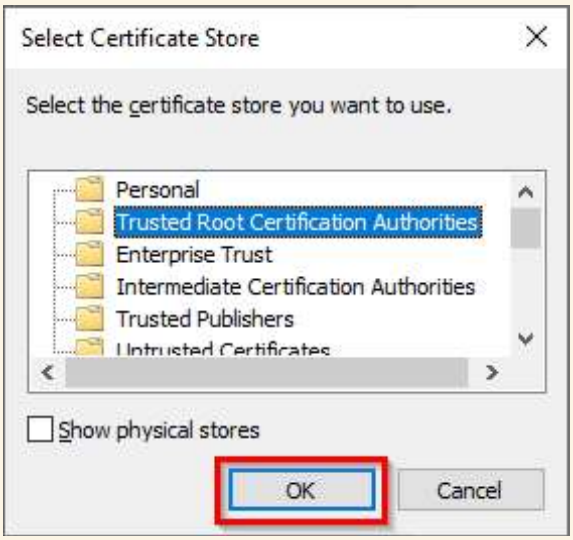
Irá ser executado o Certificate Import Wizard. Escolha a certificate store que mais se adeque ao seu caso, neste exemplo foi escolhida a certificate store do "Current User". Clique em "Next":



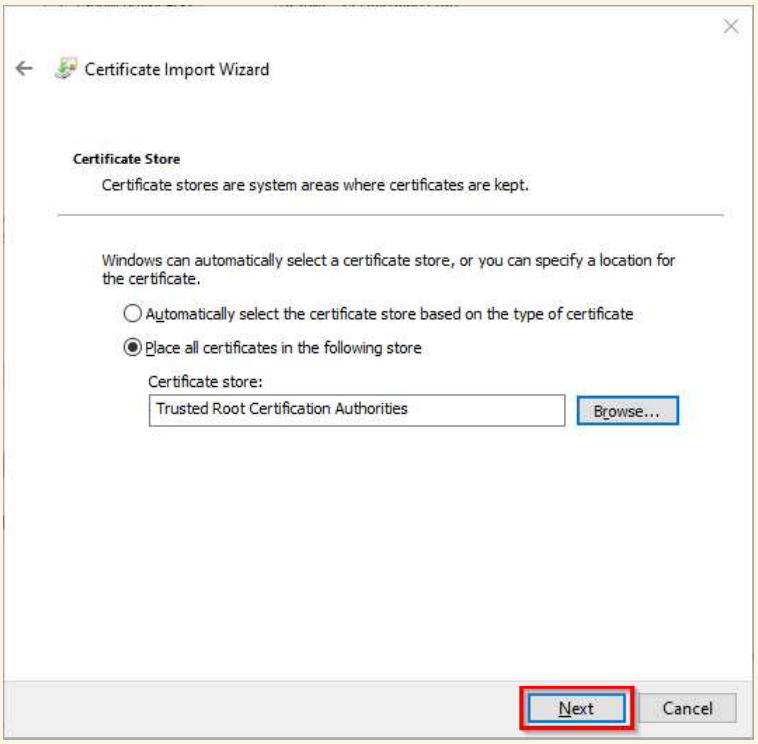
Clique em "Browse" para escolher a store para onde vai ser importado o certificado:



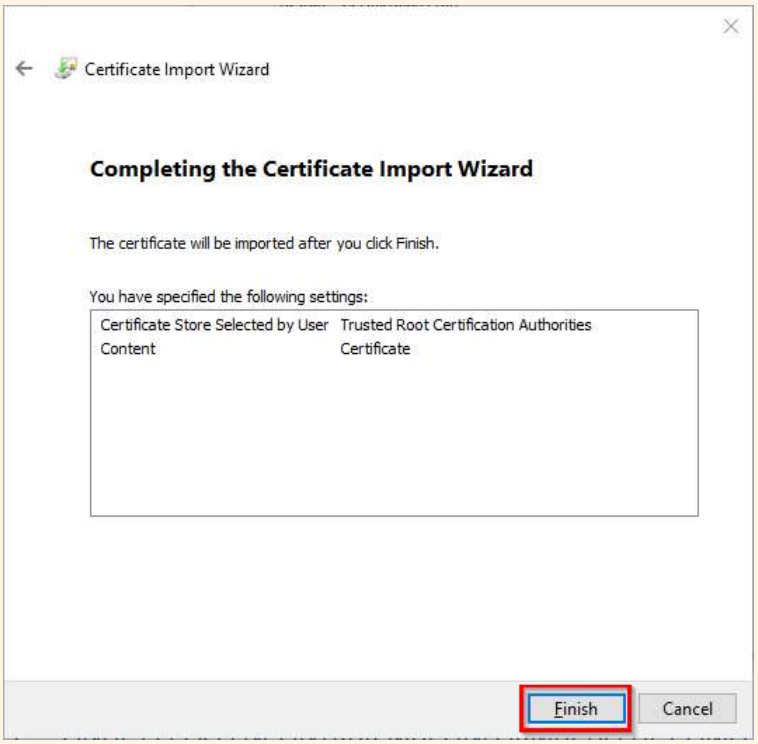
Selecione a store "Trusted Root Certification Authorities" e clique em "OK":



Clique em “Next”:



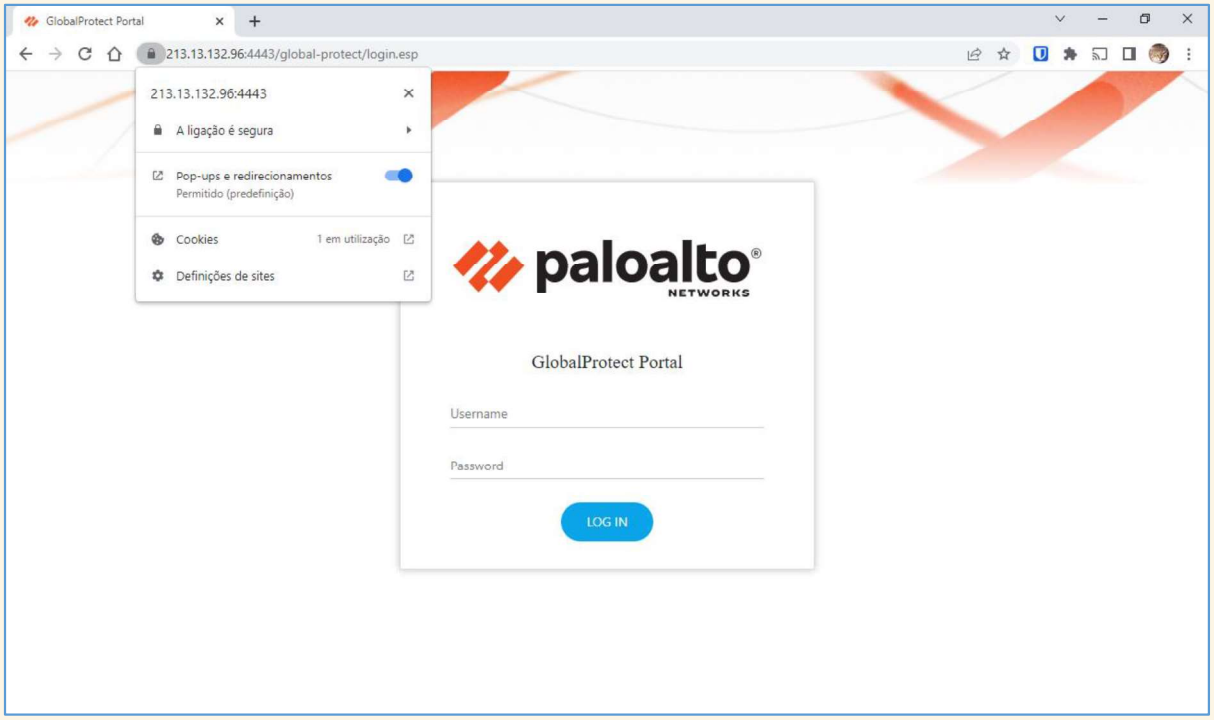
Clique em “Finish” para concluir o processo de importação:



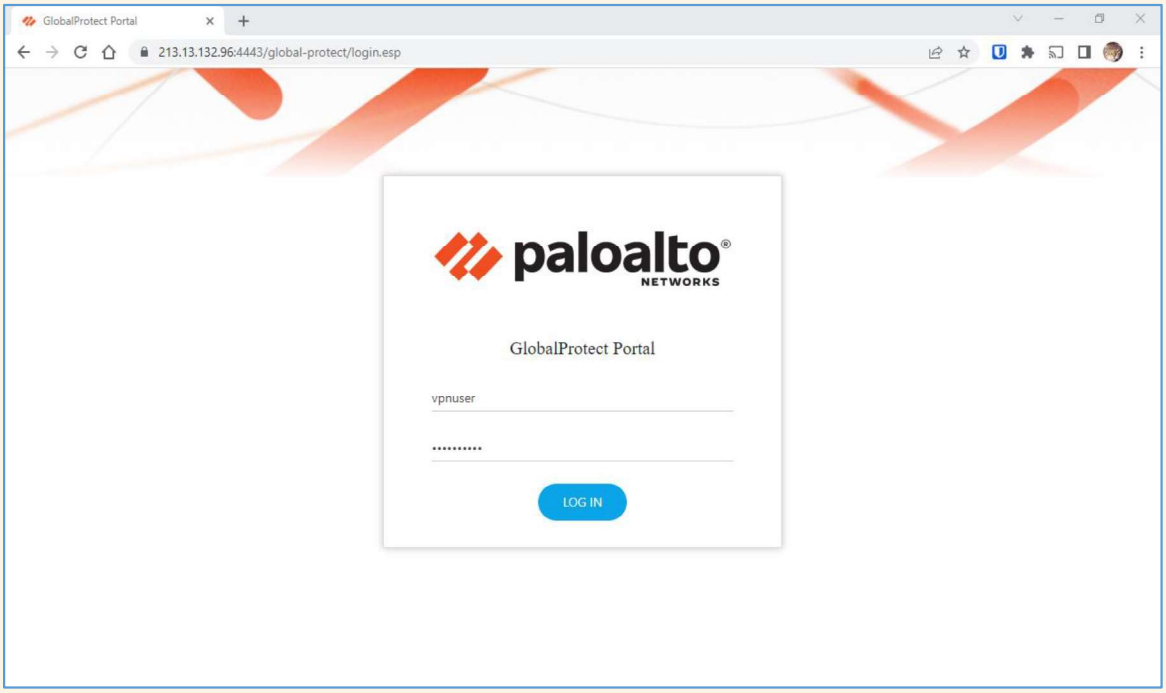
Ser-lhe-á apresentado um aviso de segurança. Clique em "Yes" para aceitar os riscos inerentes e importar o certificado:

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

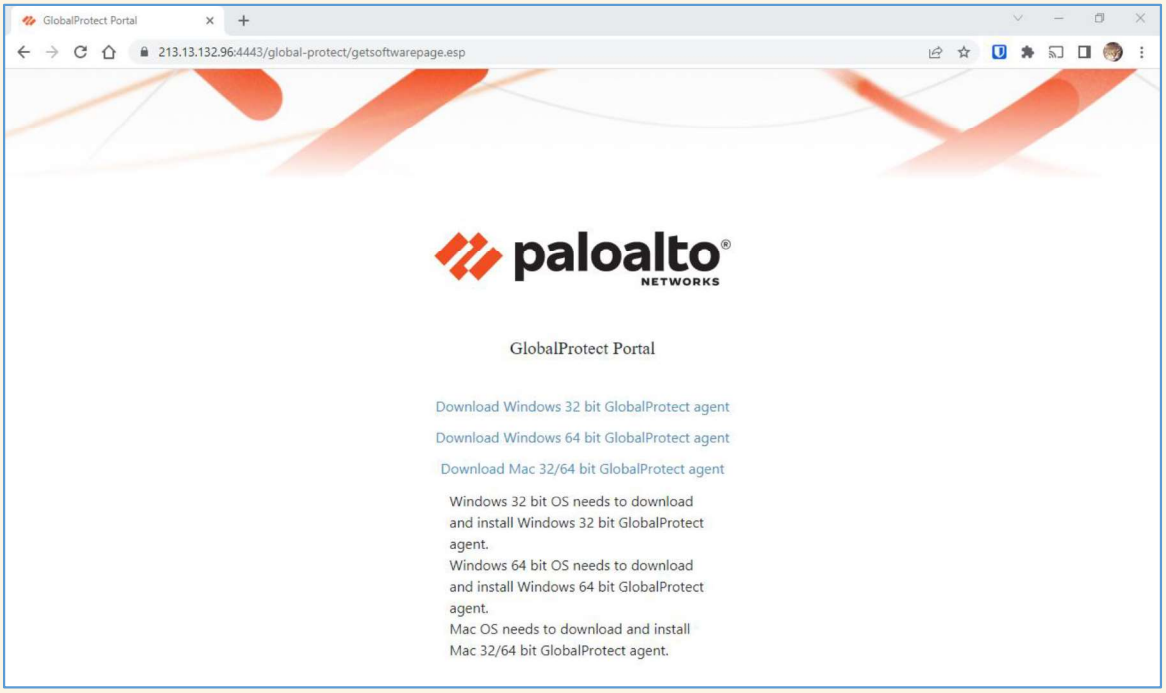
Carregue no botão de refresh do browser. Agora já será apresentada a página do portal GlobalProtect sem o aviso ⚠ Inseguro, tendo este sido substituído por um cadeado (🔒 - indica que a ligação é segura):



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

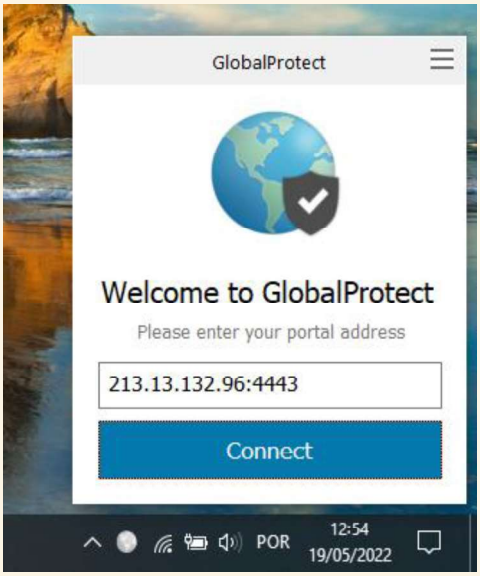


É apresentada uma lista de agentes GlobalProtect para descarregar e instalar. Descarregue o que corresponder à versão do sistema operativo instalado no seu PC cliente:

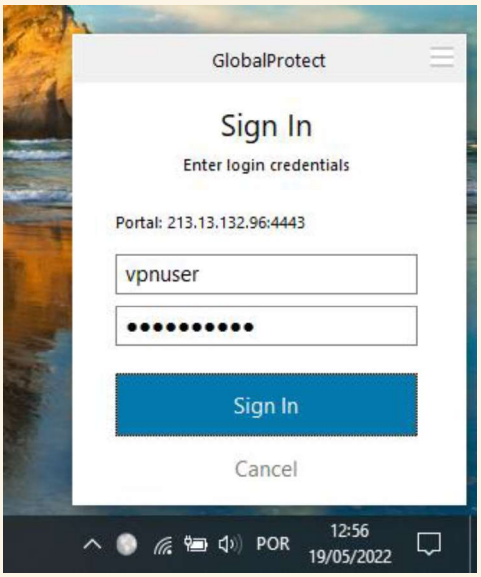


Clique duas vezes no agente que acabou de descarregar para iniciar a instalação e prossiga pelos menus clicando em "Next" até ficar concluída.

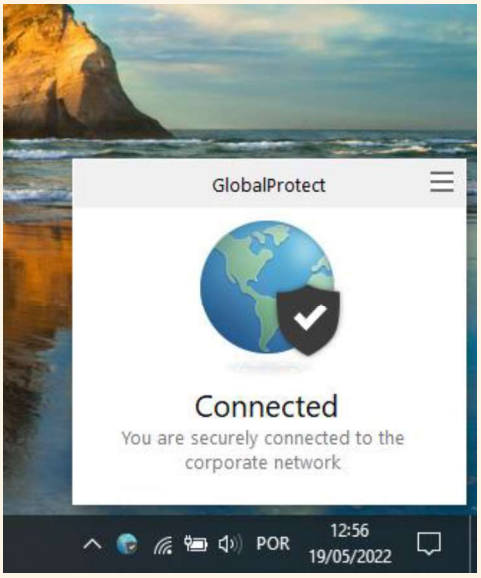
Após o agente GlobalProtect ter sido instalado com sucesso no PC cliente irá aparecer o ícone  na taskbar do Windows juntamente com uma janela de diálogo do agente a pedir a introdução do endereço do portal. Preencha com o IP:porto **213.13.132.96:4443** e clique em "Connect":



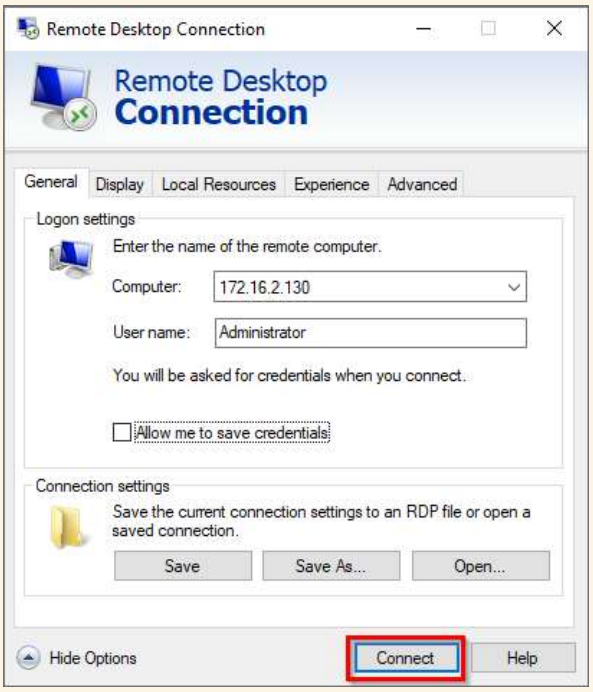
De seguida introduza as credencias da conta vpnuser e clique em "Sign In":



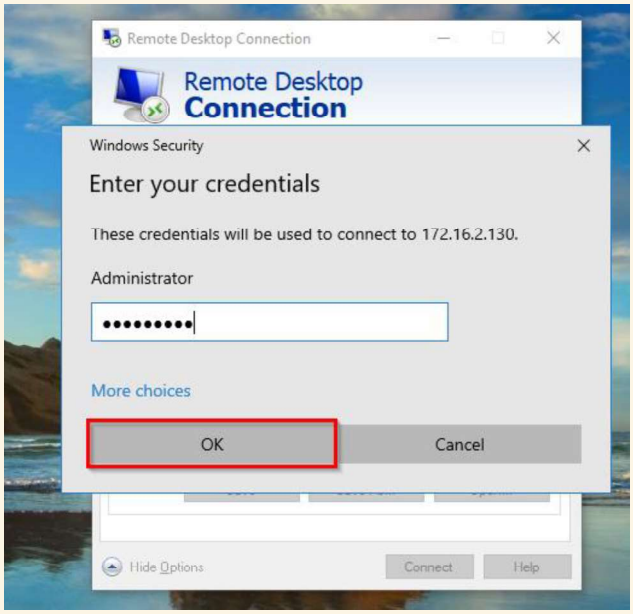
O agente irá estabelecer a VPN e apresentará a seguinte mensagem de sucesso:



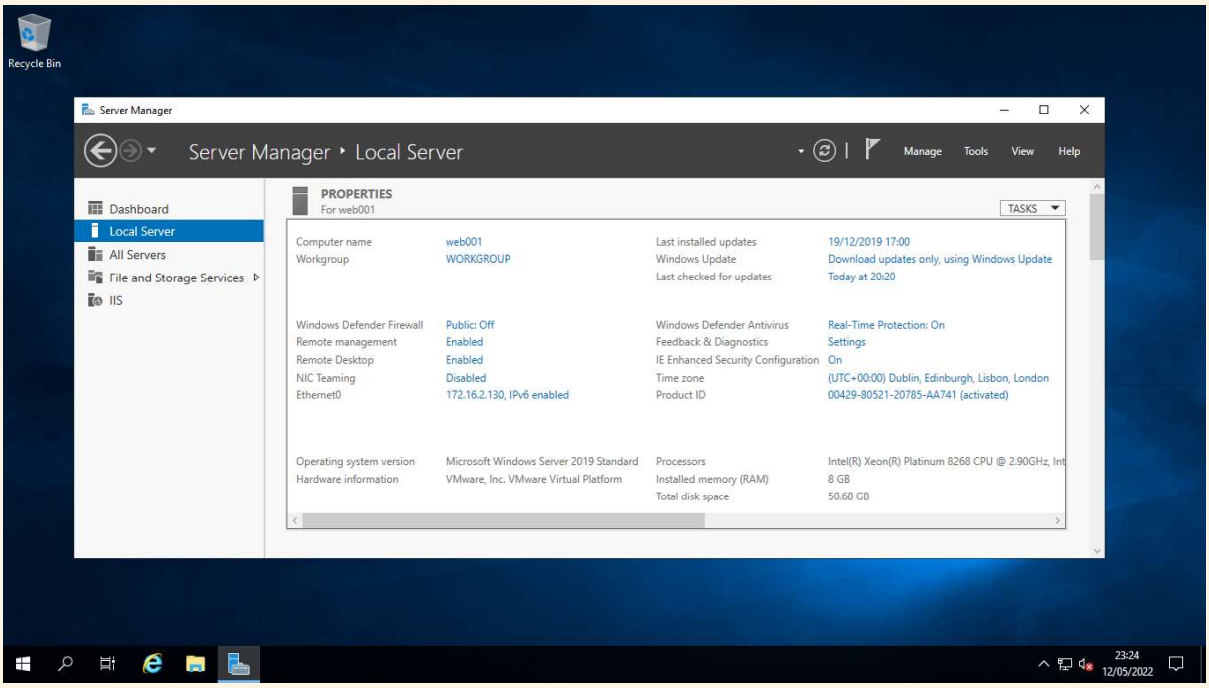
Agora vamos ligar-nos remotamente ao servidor virtual da adesão a partir do PC cliente. Abra a aplicação de Remote Desktop Connection e preencha os campos com o IP do servidor remoto – 172.16.2.130 – e o User name da conta pretendida para login. Clique em "Connect":



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



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.

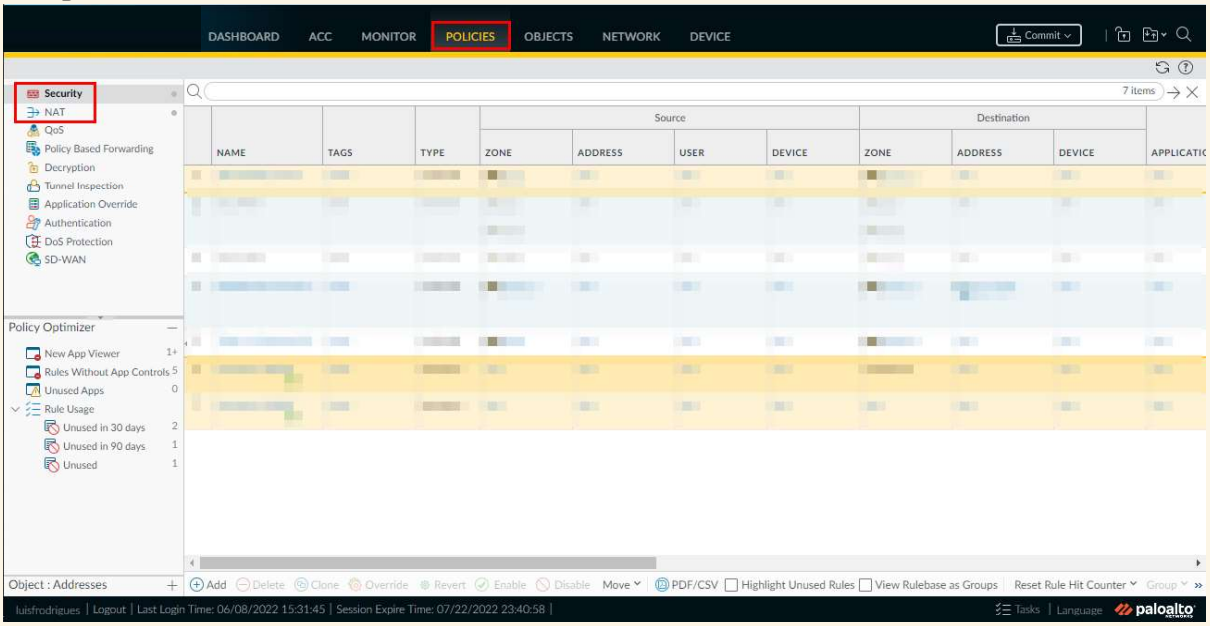
2.7. Que configurações devo alterar antes de remover um IP da minha Firewall?

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.

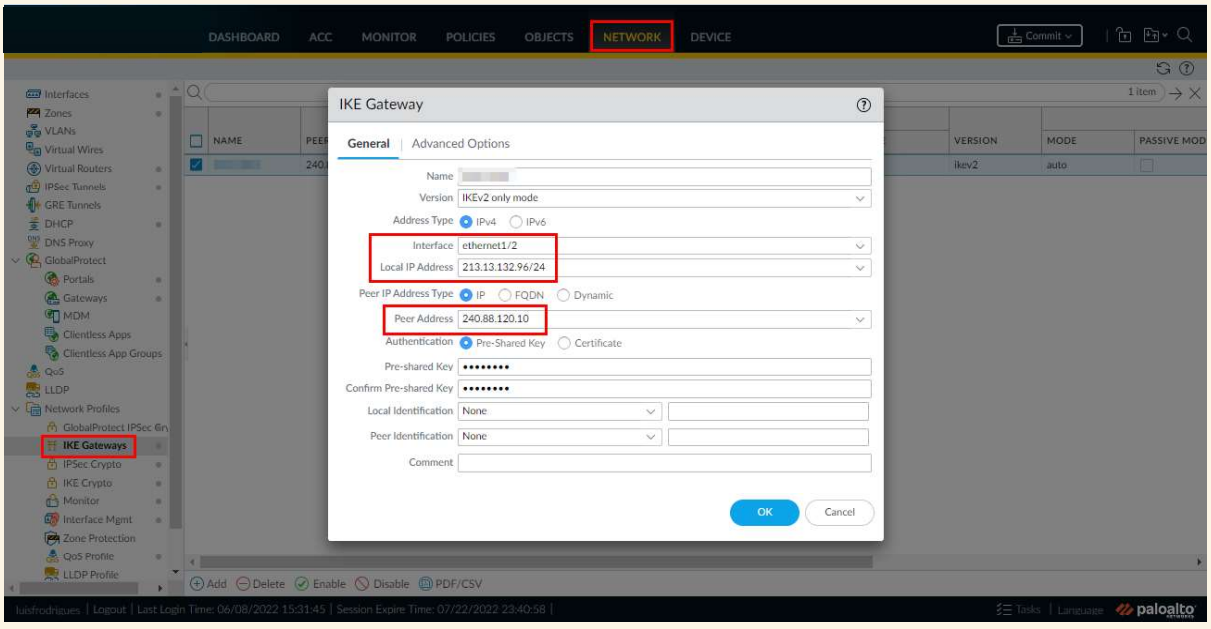
Sítios comuns na configuração da firewall (mas não exaustivos) onde são usados IPs públicos de IPv4 são os seguintes:

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

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



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



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;

Remoção da pré-configuração básica *ready to use* da VPN GlobalProtect;(gateway "VPN-GW" e portal "VPN-PORTAL");

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  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
DNS Forwarder	S	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 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	N	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	N	Acesso remoto por SSL VPN https:// ao IP da VFW + porto
SD-WAN	N	Não está disponível embora apareça na VFW para configuração
DOS Protection	N	Não está disponível embora apareça na VFW para configuração
QOS	N	Não está disponível embora apareça na VFW para configuração
Policy Based Forwarding	N	Não está disponível embora apareça na VFW para configuração

Legenda:

S – Disponível

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