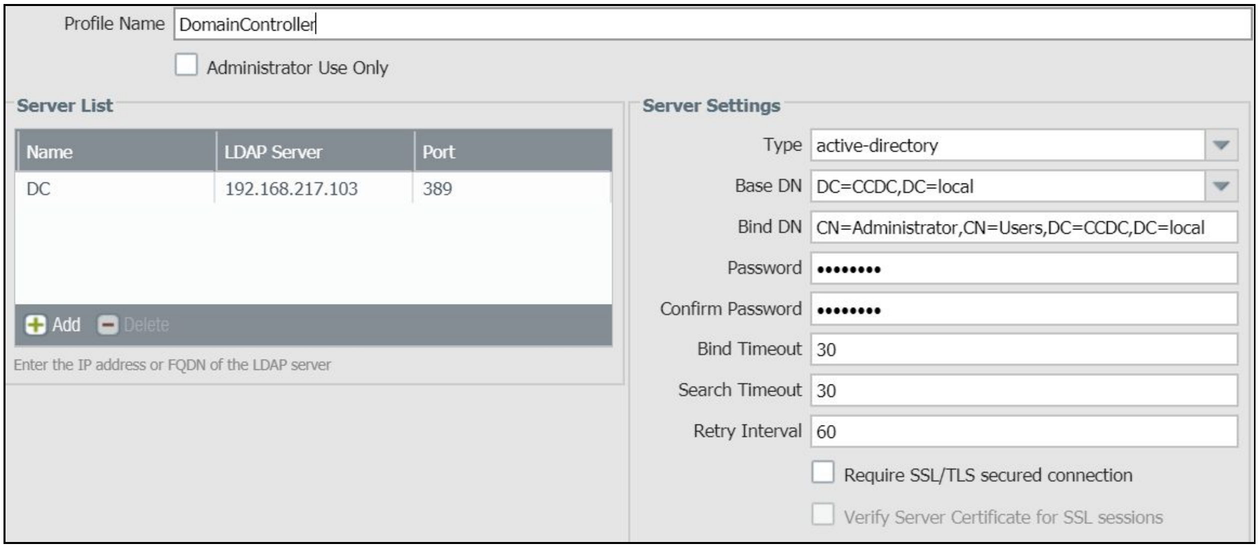
Connecting Palo Alto to LDAP

- docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/authentication/configure-ldap-authentication
- knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFQCA0
- knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGOCA0

1. Setup LDAP server profile: Device -> Server Profiles -> LDAP
    a. May want to require SSL/TLS if LDAP is configured for it
    b. Bind DN (run this on LDAP server): `dsquery user -name john`
    c. Base DN pull the DC values from the return of the above query



Profile Name: DomainController

□ Administrator Use Only

Server List

Name	LDAP Server	Port
DC	192.168.217.103	389

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: DC=CCDC,DC=local

Bind DN: CN=Administrator,CN=Users,DC=CCDC,DC=local

Password: ••••••••

Confirm Password: ••••••••

Bind Timeout: 30

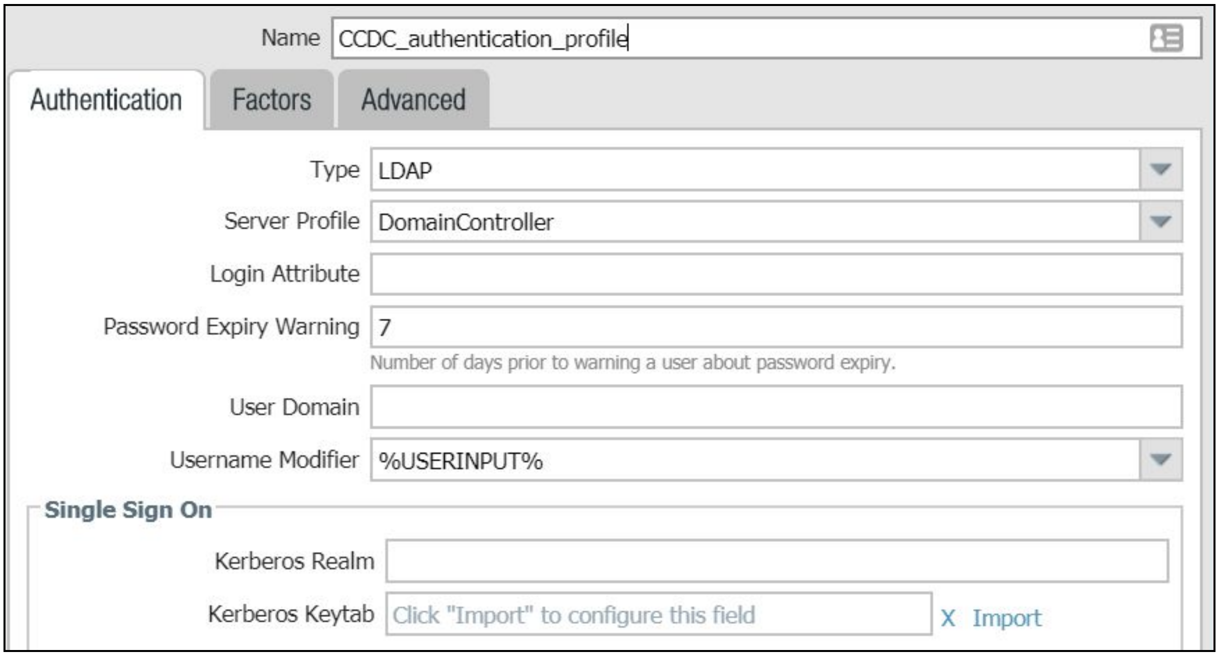
Search Timeout: 30

Retry Interval: 60

□ Require SSL/TLS secured connection

□ Verify Server Certificate for SSL sessions

2. Add authentication profile: Device -> Authentication Profile



Name: CCDC_authentication_profile

Type: LDAP

Server Profile: DomainController

Login Attribute:

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain:

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field

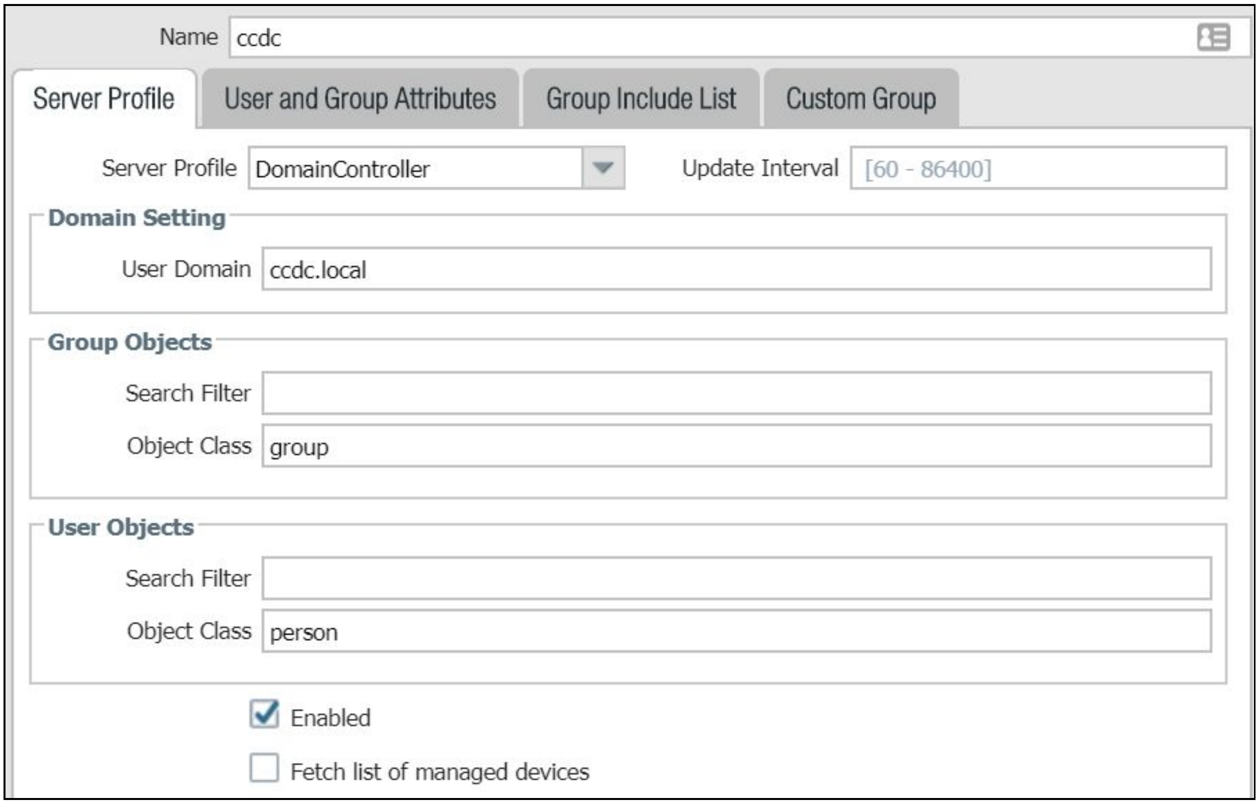
    a. Add users and groups that can authenticate with this profile: Advanced; Blank = all

3. Test the connection from Palo Alto CLI to LDAP

DON'T FORGET TO COMMIT

```
test authentication authentication-profile
CCDC_authentication_profile username Administrator password
```

4. Add user identification from LDAP: Device -> User Identification



Name: ccdc

Server Profile: DomainController

Update Interval: [60 - 86400]

Domain Setting

User Domain: ccdc.local

Group Objects

Search Filter:

Object Class: group

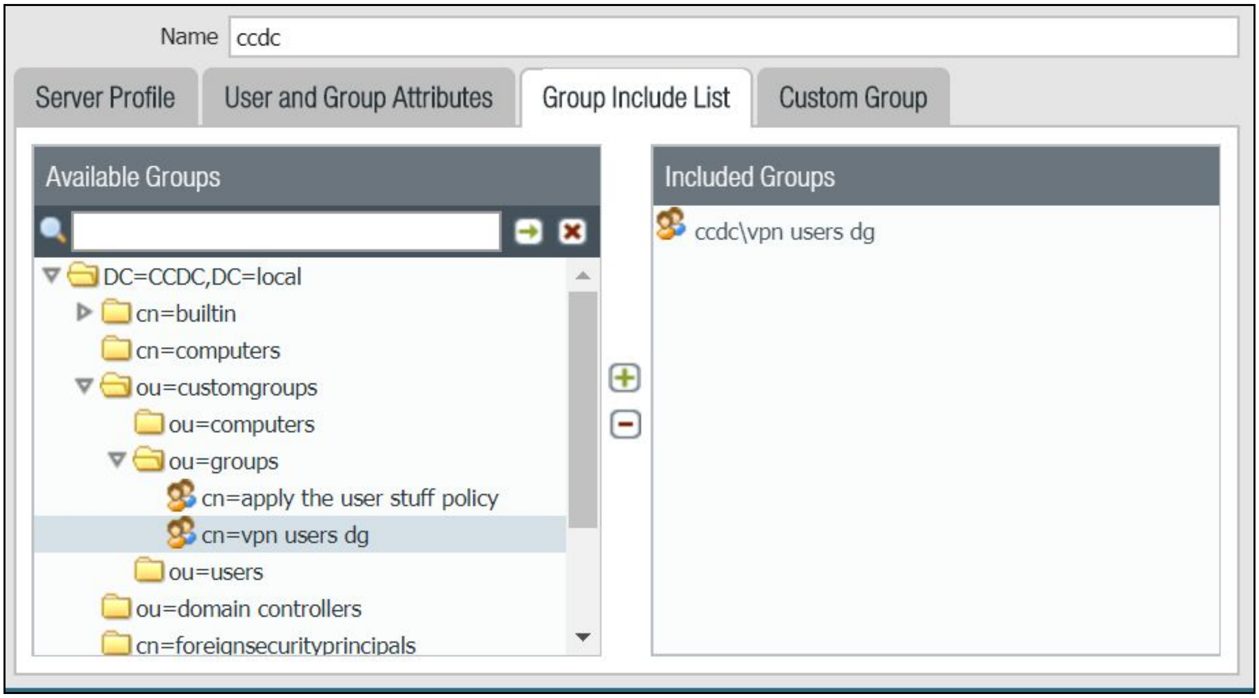
User Objects

Search Filter:

Object Class: person

☑ Enabled

□ Fetch list of managed devices



Name: ccdc

Available Groups

- DC=CCDC,DC=local
  - cn=builtin
  - cn=computers
  - ou=customgroups
    - ou=computers
    - ou=groups
      - cn=apply the user stuff policy
      - cn=vpn users dg
    - ou=users
  - ou=domain controllers
  - cn=foreignsecurityprincipals

Included Groups

- ccdc\vpn users dg

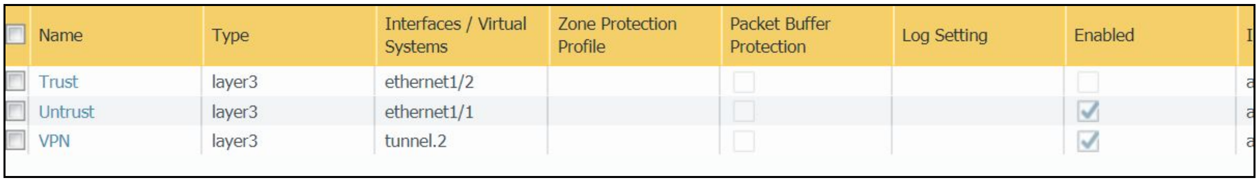
DON'T FORGET TO COMMIT

Setting Up a Palo Alto Remote to Site VPN

- docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-authentication-profile
- https://docs.paloaltonetworks.com/globalprotect/8-1/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/deploy-server-certificates-to-the-globalprotect-components.html#idd02df51f-f514-4a59-9cba-ecb14c03c70b_id98ae40da-a2ca-4413-9a92-bc7c1967f1df
- https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClH2CAK

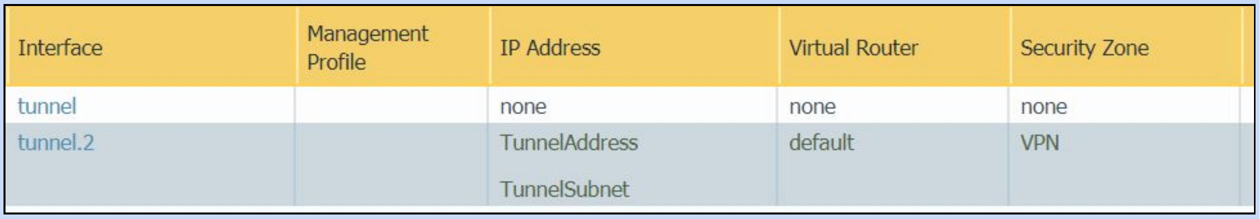
Setup Interfaces/Zones:

1. Create a VPN Security Zone and enable UserID on it and the Untrust: Network -> Zones



☐	Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Packet Buffer Protection	Log Setting	Enabled	I
☐	Trust	layer3	ethernet1/2		☐		☐	a
☐	Untrust	layer3	ethernet1/1		☐		☑	a
☐	VPN	layer3	tunnel.2		☐		☑	a

2. Create tunnel.2 and assign to VPN Zone: Network -> Interfaces -> Tunnel
   a. tunnel gets automatically created

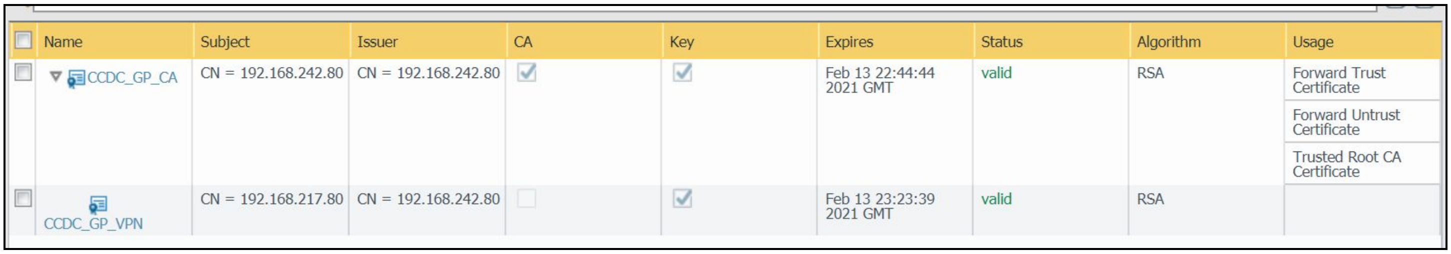


Interface	Management Profile	IP Address	Virtual Router	Security Zone
tunnel		none	none	none
tunnel.2		TunnelAddress TunnelSubnet	default	VPN

3. Add a security policy to allow traffic from VPN to Trust: Policies -> Security

Setup Certificates:

1. Assuming you need self-signed certs: Device -> Certificate Management -> Certificates -> Device Certificates

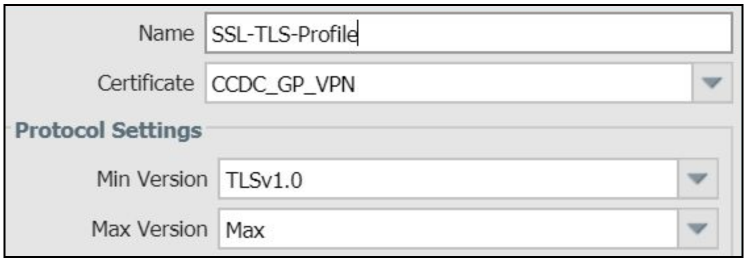


☐	Name	Subject	Issuer	CA	Key	Expires	Status	Algorithm	Usage
☐	CCDC_GP_CA	CN = 192.168.242.80	CN = 192.168.242.80	☑	☑	Feb 13 22:44:44 2021 GMT	valid	RSA	Forward Trust Certificate Forward Untrust Certificate Trusted Root CA Certificate
☐	CCDC_GP_VPN	CN = 192.168.217.80	CN = 192.168.242.80	☐	☑	Feb 13 23:23:39 2021 GMT	valid	RSA	

   a. This should include one root certificate authority (CA) whose issuer and subject are itself.
   b. This should also include one certificate, signed by the created CA, whose subject is whatever resource is being accessed.

2. Create TLS/SSL Profile: Device -> Certificate Management -> TLS / SSL Service Profile

DON'T FORGET TO COMMIT



Name: SSL-TLS-Profile

Certificate: CCDC_GP_VPN

Protocol Settings

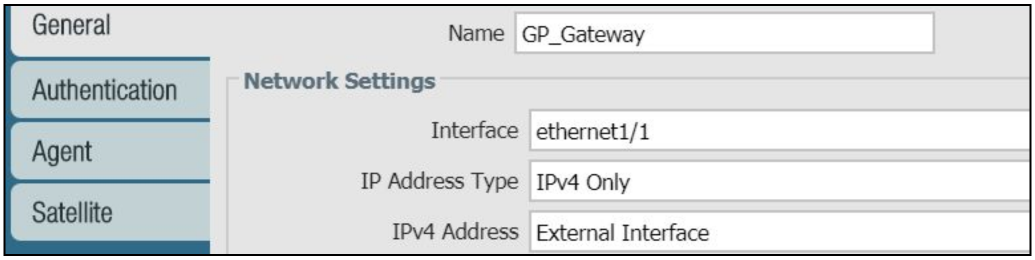
Min Version: TLSv1.0

Max Version: Max

Setup GlobalProtect Gateway:

Setup GP Gateways: Network -> Global Protect -> Gateways

- Note: Will end up with a hardcoded IP in Agent->Client Settings->Config->Split Tunnel->Access Route->Include
- Note: Will end up with a hardcoded IP in Agent->Client Settings->Config->Network Services->DNS Server
- Note: Will end up with a hardcoded IP in Agent->Network Services->DNS



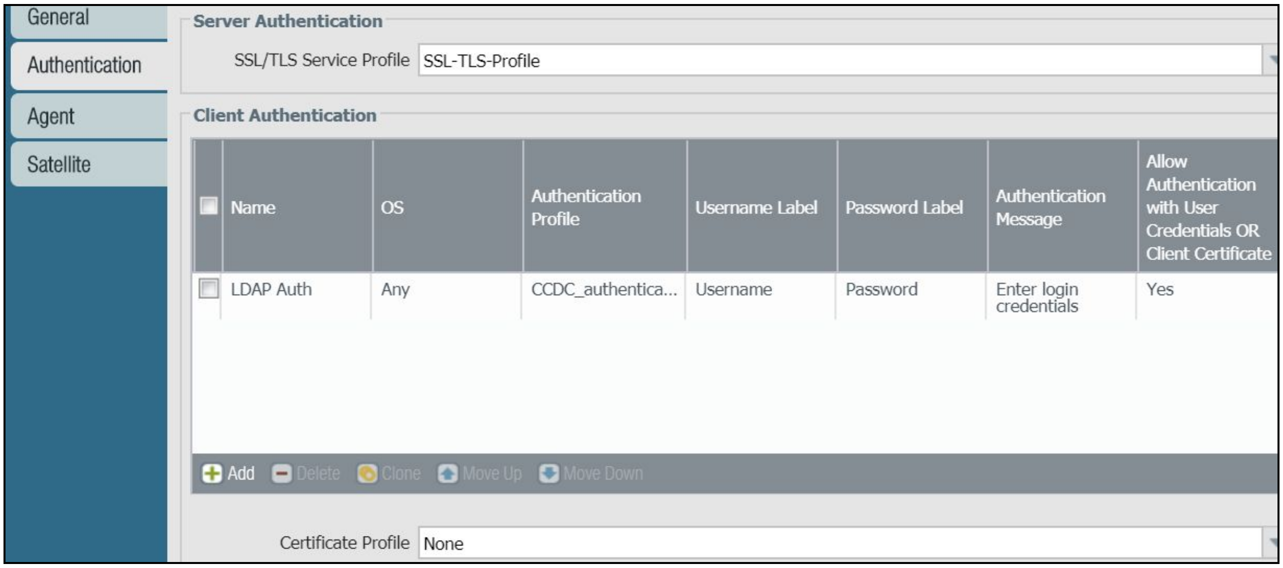
Name: GP_Gateway

Network Settings

Interface: ethernet1/1

IP Address Type: IPv4 Only

IPv4 Address: External Interface



Server Authentication

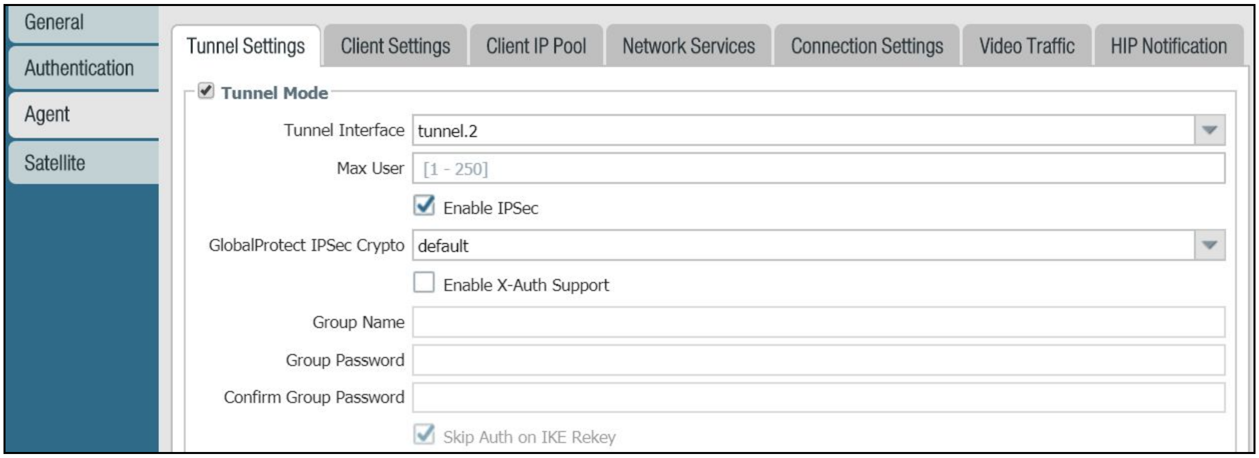
SSL/TLS Service Profile: SSL-TLS-Profile

Client Authentication

□	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message	Allow Authentication with User Credentials OR Client Certificate
□	LDAP Auth	Any	CCDC_authentica...	Username	Password	Enter login credentials	Yes

Certificate Profile: None

DON'T FORGET TO COMMIT



☑ Tunnel Mode

Tunnel Interface: tunnel.2

Max User: [1 - 250]

☑ Enable IPSec

GlobalProtect IPSec Crypto: default

□ Enable X-Auth Support

Group Name:

Group Password:

Confirm Group Password:

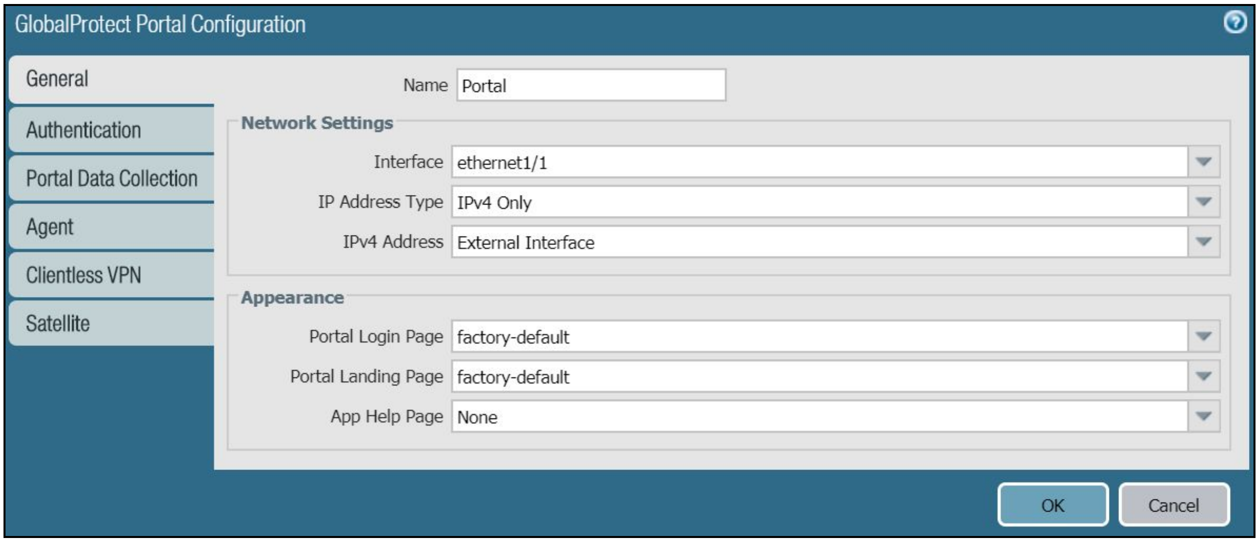
☑ Skip Auth on IKE Rekey

1. Client Settings -> Add
    a. Change name in Config Selection Criteria
    b. Nothing in Authentication Override
    c. IP pools add a network that isn't being used for clients to connect with.
    d. Split tunnel -> Access Route -> Include add the internal network to reach when VPN'd in.
        i. Needs to be a hardcoded subnet, not referencing an object.
    e. Network Services add DNS records, leave everything else as none
        i. Doesn't let you add objects; these are hardcoded IPs
    f. Skip other tabs
2. Skip Client IP Pool if you assigned it in the client settings tab
3. Network Services add DNS records
    a. Doesn't let you add objects; these are hardcoded IPs
4. Skip everything else

Setup GlobalProtect Portal:

Setup GlobalProtect Portals: Network -> Global Protect -> Portals

- Note: Will end up with a hardcoded IP in Agent -> Config -> External -> External Gateways



Name: Portal

Network Settings

Interface: ethernet1/1

IP Address Type: IPv4 Only

IPv4 Address: External Interface

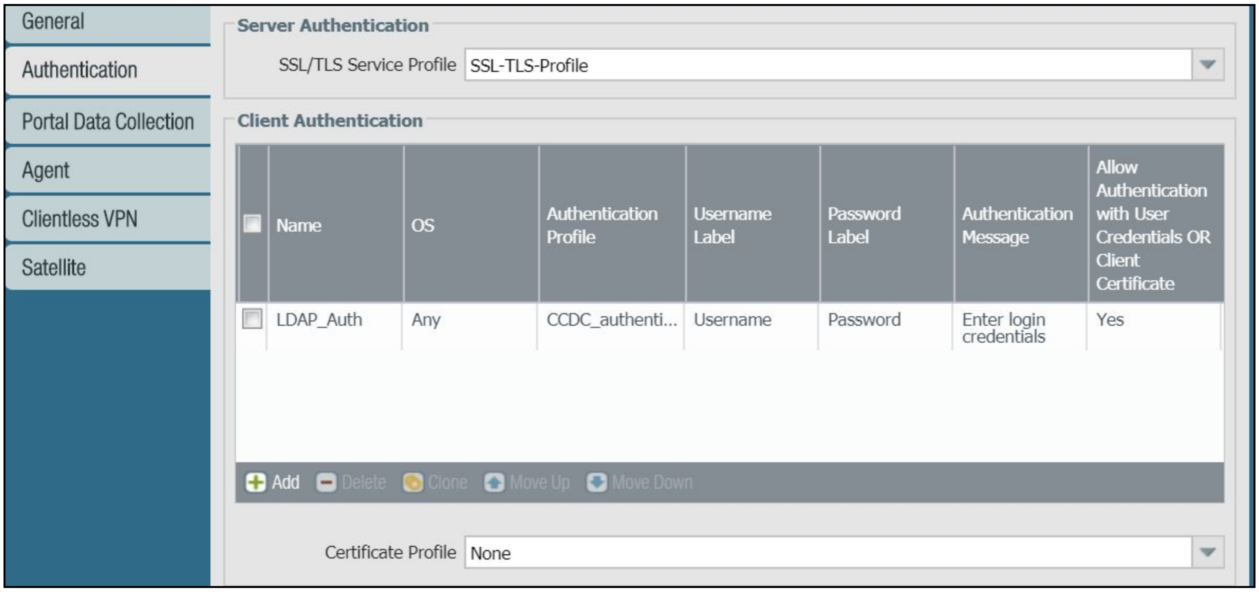
Appearance

Portal Login Page: factory-default

Portal Landing Page: factory-default

App Help Page: None

DON'T FORGET TO COMMIT



Server Authentication

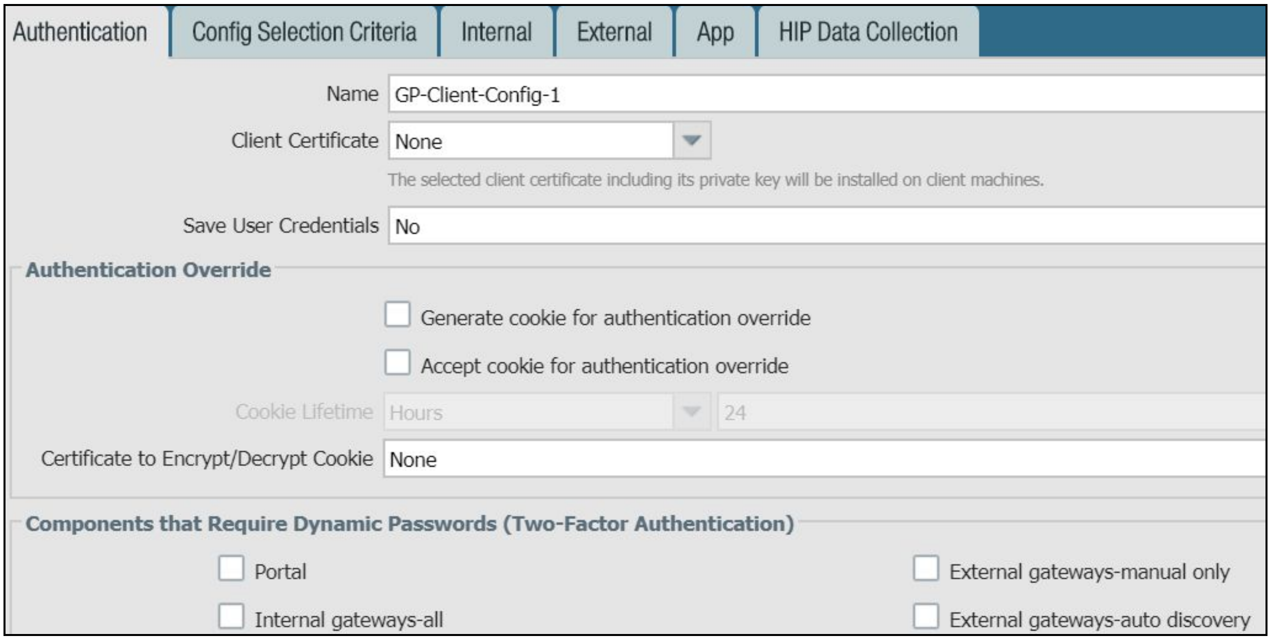
SSL/TLS Service Profile: SSL-TLS-Profile

Client Authentication

□	Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message	Allow Authentication with User Credentials OR Client Certificate
□	LDAP_Auth	Any	CCDC_authenti...	Username	Password	Enter login credentials	Yes

Certificate Profile: None

1. Agent configuration as follows:
   a. Ignore (leave defaults) for all tabs not shown below



Name: GP-Client-Config-1

Client Certificate: None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: No

Authentication Override

□ Generate cookie for authentication override

□ Accept cookie for authentication override

Cookie Lifetime: Hours 24

Certificate to Encrypt/Decrypt Cookie: None

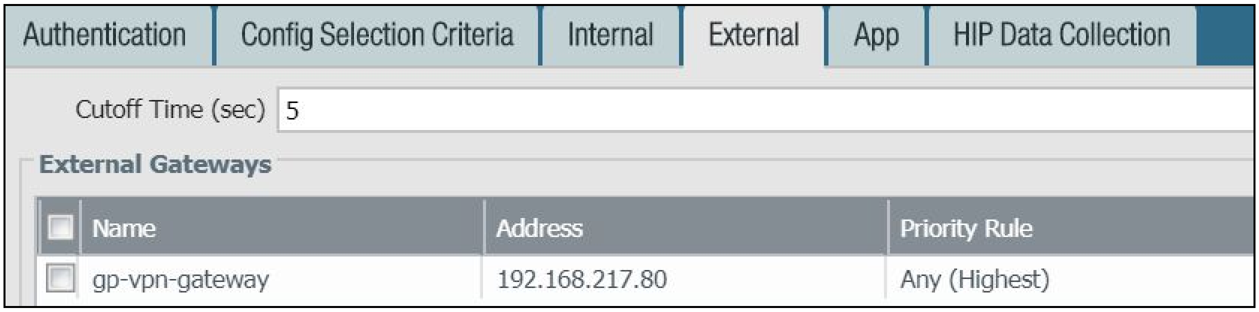
Components that Require Dynamic Passwords (Two-Factor Authentication)

□ Portal

□ External gateways-manual only

□ Internal gateways-all

□ External gateways-auto discovery

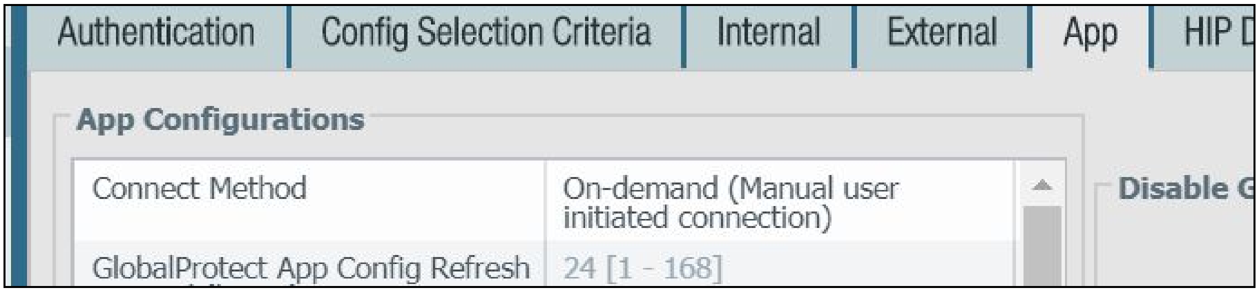


Cutoff Time (sec): 5

External Gateways

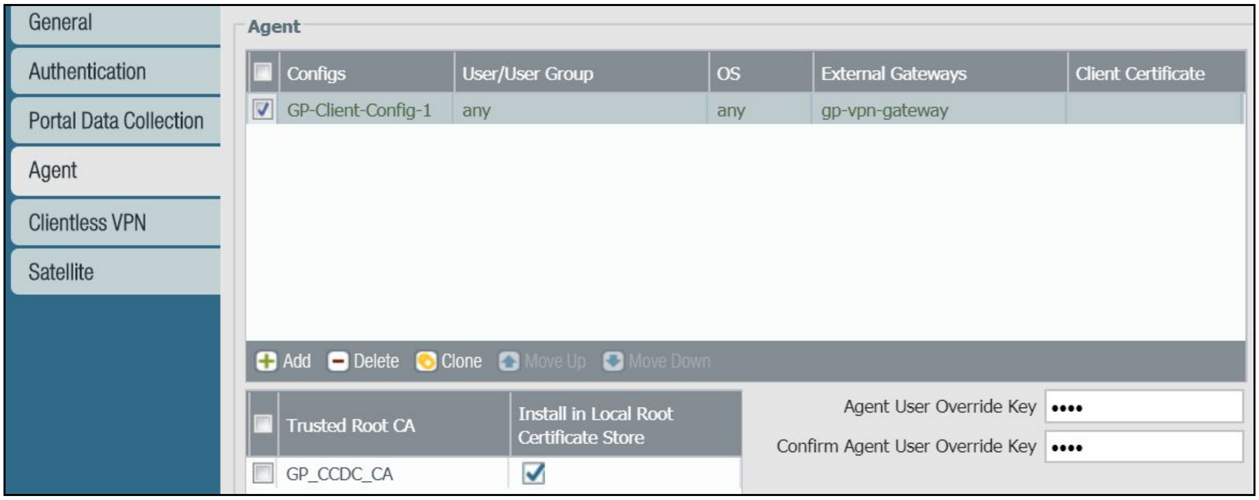
□	Name	Address	Priority Rule
□	gp-vpn-gateway	192.168.217.80	Any (Highest)

DON'T FORGET TO COMMIT



App Configurations

Connect Method	On-demand (Manual user initiated connection)
GlobalProtect App Config Refresh	24 [1 - 168]



Agent

☐	Configs	User/User Group	OS	External Gateways	Client Certificate
☑	GP-Client-Config-1	any	any	gp-vpn-gateway	

☐	Trusted Root CA	Install in Local Root Certificate Store
☐	GP_CCDC_CA	☑

Agent User Override Key ••••

Confirm Agent User Override Key ••••

Setup GlobalProtect Client:

Setup the Global Protect Client: Device -> Global Protect Client

1. Check now
2. Download Client
3. Activate

DON'T FORGET TO COMMIT

Our Configuration for Reference

Interfaces:

ethernet1/1:	Layer3, External Interface, Untrust Zone
ethernet1/2:	Layer3, Internal Interface, Trust Zone
tunnel.2:	TunnelAddress / Tunnel Subnet, default Virtual Router, VPN Zone

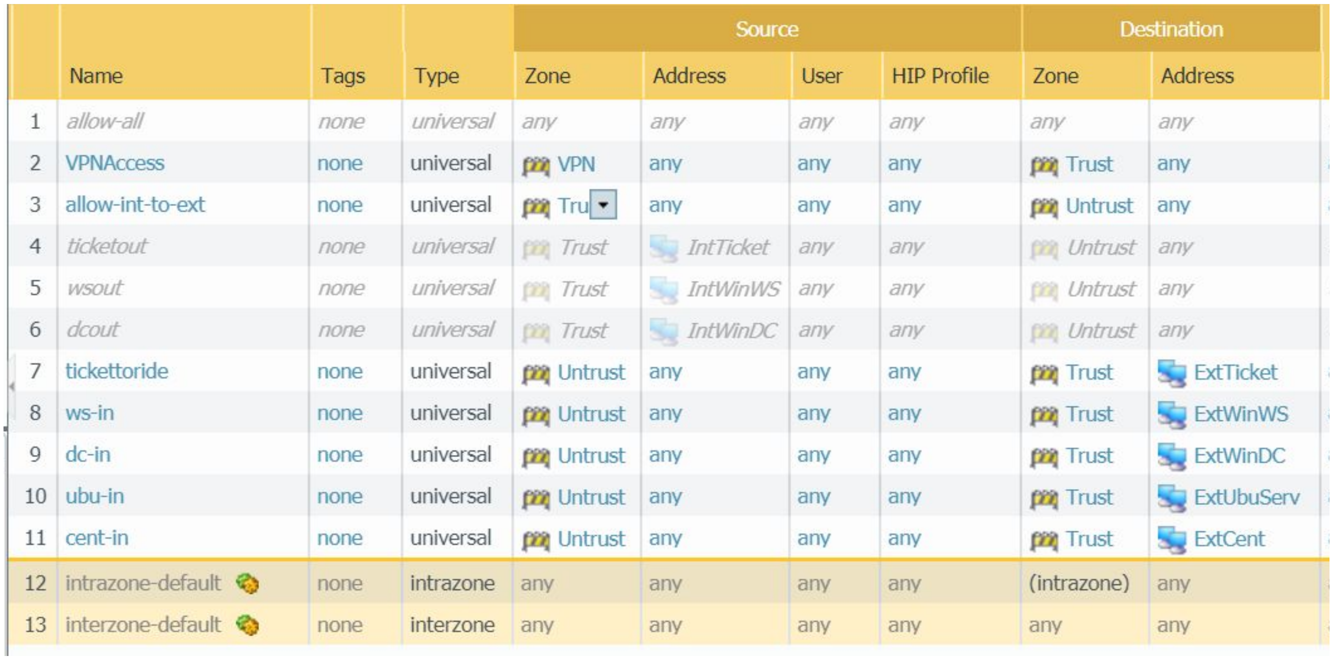
Objects:

External Gateway:	192.168.217.1
External Interface:	192.168.217.80
Internal Interface:	192.168.209.1/24

CheckSvcs-VPN:	192.168.217.100
TunnelAddress:	10.0.217.1
TunnelSubnet:	10.0.217.0/24

ExtTicket:	192.168.217.101	IntTicket:	192.168.209.101
ExtWinWS:	192.168.217.102	IntWinWS:	192.168.209.102
ExtWinDC:	192.168.217.103	IntWinDC:	192.168.209.103
ExtUbuServer:	192.168.217.104	IntUbuServer:	192.168.209.104
ExtCent:	192.168.217.105	IntCent:	192.168.209.105

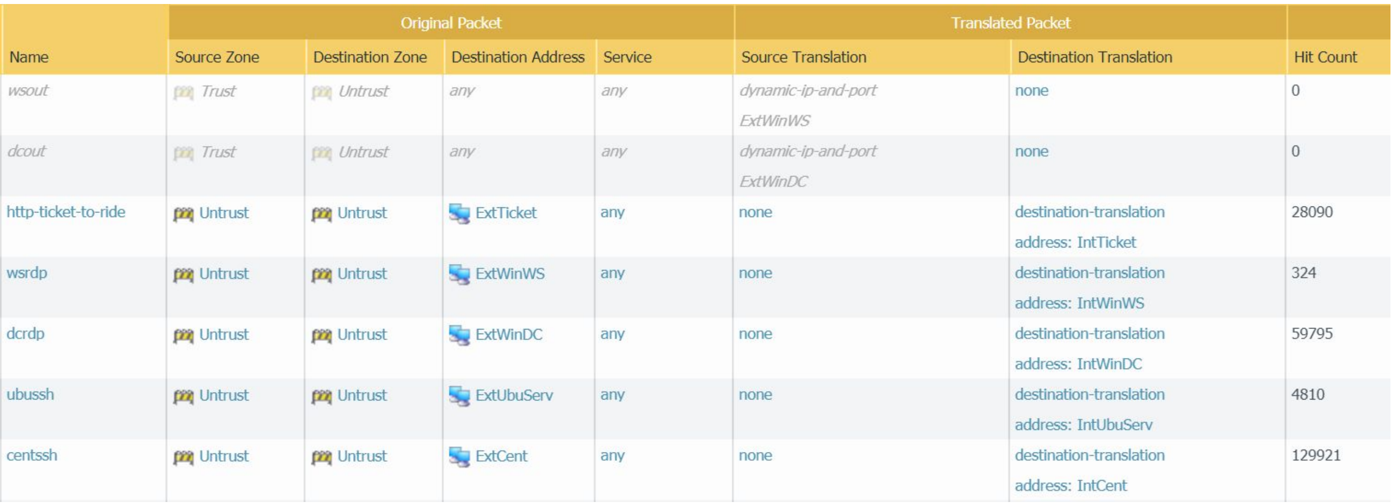
Security Policies:



				Source				Destination	
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
1	*allow-all*	*none*	*universal*	*any*	*any*	*any*	*any*	*any*	*any*
2	VPNAccess	none	universal	VPN	any	any	any	Trust	any
3	allow-int-to-ext	none	universal	Tru	any	any	any	Untrust	any
4	*ticketout*	*none*	*universal*	*Trust*	*IntTicket*	*any*	*any*	*Untrust*	*any*
5	*wsout*	*none*	*universal*	*Trust*	*IntWinWS*	*any*	*any*	*Untrust*	*any*
6	*dcout*	*none*	*universal*	*Trust*	*IntWinDC*	*any*	*any*	*Untrust*	*any*
7	tickettoride	none	universal	Untrust	any	any	any	Trust	ExtTicket
8	ws-in	none	universal	Untrust	any	any	any	Trust	ExtWinWS
9	dc-in	none	universal	Untrust	any	any	any	Trust	ExtWinDC
10	ubu-in	none	universal	Untrust	any	any	any	Trust	ExtUbuServ
11	cent-in	none	universal	Untrust	any	any	any	Trust	ExtCent
12	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any
13	interzone-default	none	interzone	any	any	any	any	any	any

DON'T FORGET TO COMMIT

NAT Policies:



	Original Packet				Translated Packet		
Name	Source Zone	Destination Zone	Destination Address	Service	Source Translation	Destination Translation	Hit Count
wsout	*Trust*	*Untrust*	*any*	*any*	*dynamic-ip-and-port* *ExtWinWS*	none	0
dcout	*Trust*	*Untrust*	*any*	*any*	*dynamic-ip-and-port* *ExtWinDC*	none	0
http-ticket-to-ride	Untrust	Untrust	ExtTicket	any	none	destination-translation address: IntTicket	28090
wsrdp	Untrust	Untrust	ExtWinWS	any	none	destination-translation address: IntWinWS	324
dcrdp	Untrust	Untrust	ExtWinDC	any	none	destination-translation address: IntWinDC	59795
ubussh	Untrust	Untrust	ExtUbuServ	any	none	destination-translation address: IntUbuServ	4810
centssh	Untrust	Untrust	ExtCent	any	none	destination-translation address: IntCent	129921

DON'T FORGET TO COMMIT