

Documentation BARRACUDA



CLAIRON Anthony-Jacques Michal

BTS SIO SISR 25.1A

Table des matières

Introduction et mission.....	3
1- Création de la BOX	4
2- Configuration Réseau	10
3- Ajout du service Firewall	12
4- Ajout du service VPN	13
Partie réseau	14
Service VPN.....	14
Règle de Firewall.....	18
Tests	21
Création du BULK	22

Introduction et mission

Notre premier objectif est de faire une configuration 'basique' afin de faire monter un Firewall (Barracuda), sur notre Control Center.

Voici les étapes que l'on va effectuer pour réussir :

1. Création de la box
2. Configuration Réseau
 - LAN
 - WAN : Config en mode PPPoE
3. Ajout du service Firewall :
 - Configuration du service afin que le LAN accède à internet (
4. Ajout du service VPN
 - Configuration du service afin de pouvoir se connecter au site distant

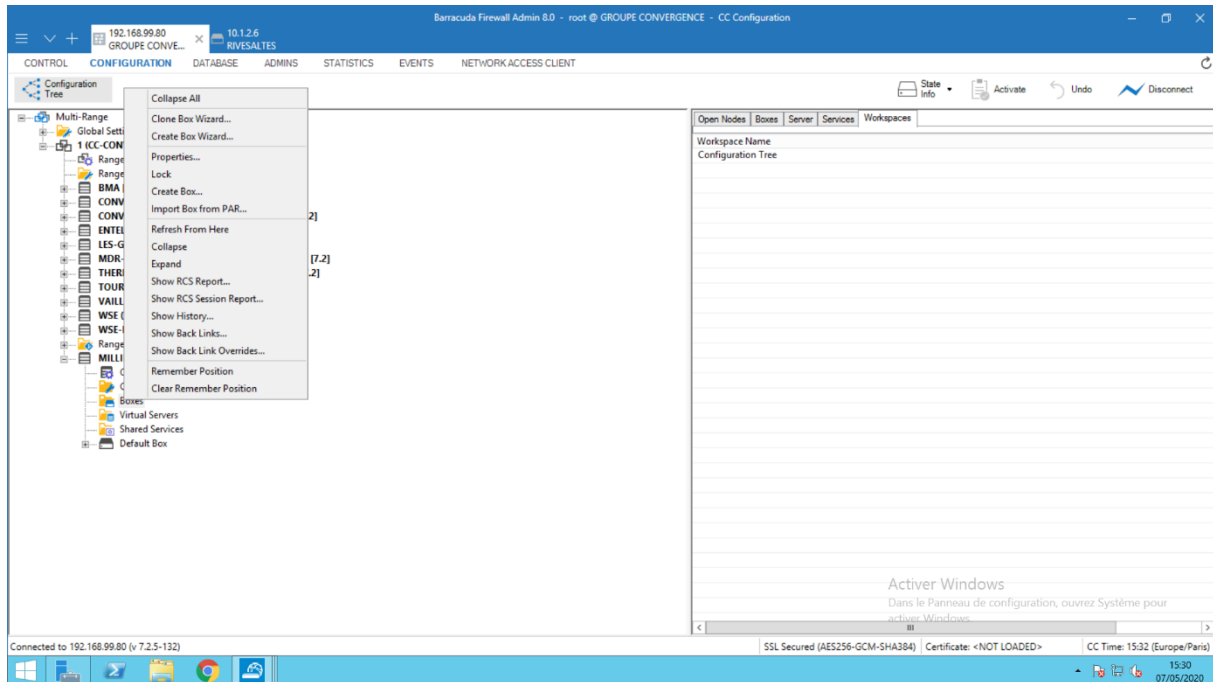
Lien vers le wiki : <https://wiki.groupe-convergence.net/#/category/tutoriels-firewall-barracuda>

Lien vers le wiki officiel :

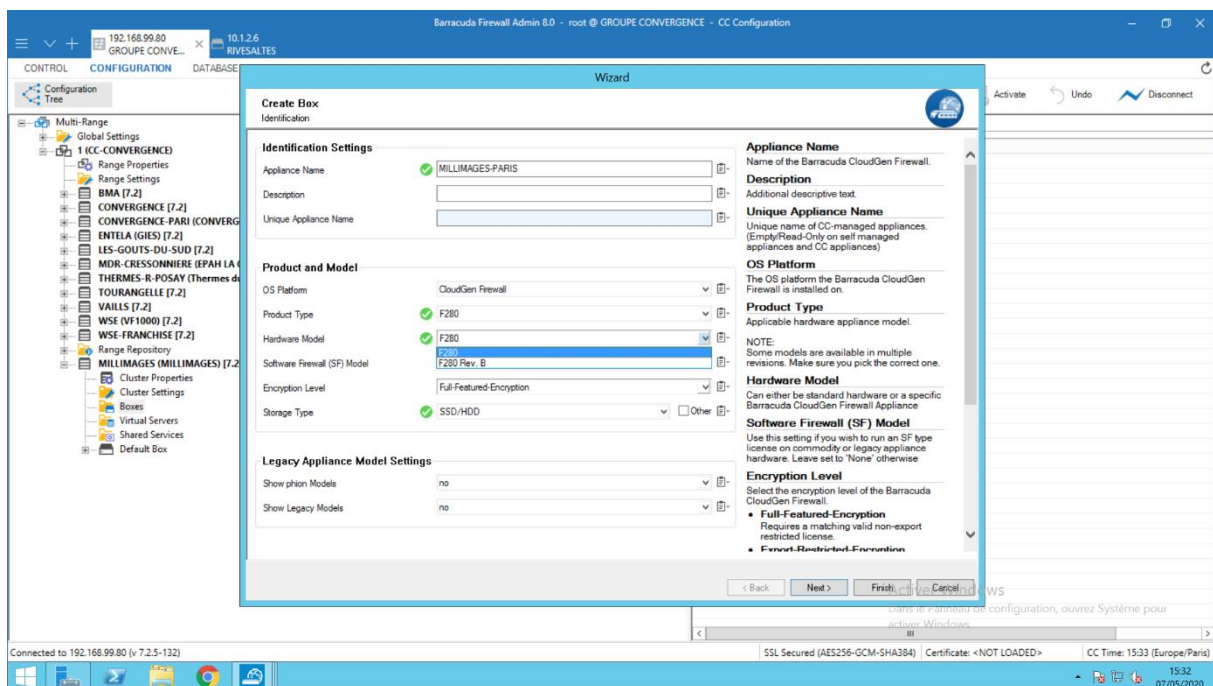
<https://campus.barracuda.com/product/cloudgenfirewall/doc/98209996/how-to-configure-vlans>

Pour Barracuda, tu auras besoin du Firewall Admin (logiciel pour les configurer) : https://entrepot.groupe-convergence.net/Softwares/Barracuda/Dernieres%20versions/FirewallAdmin_9.0.0-519.exe:

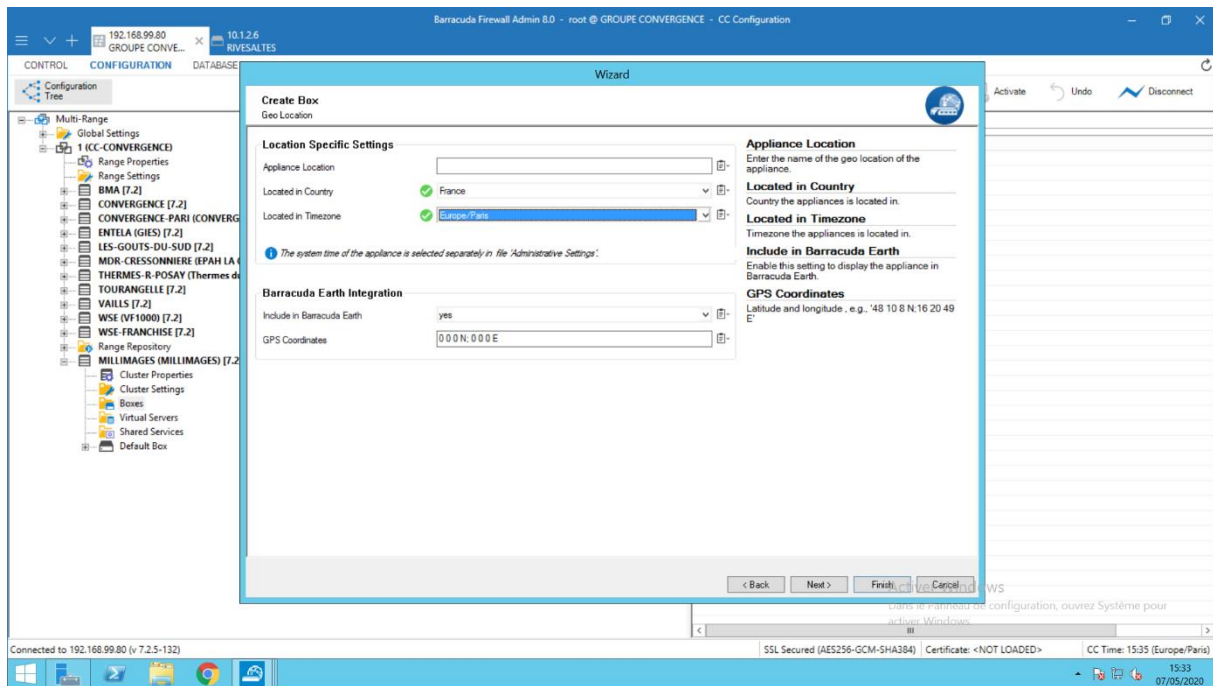
1- Création de la BOX



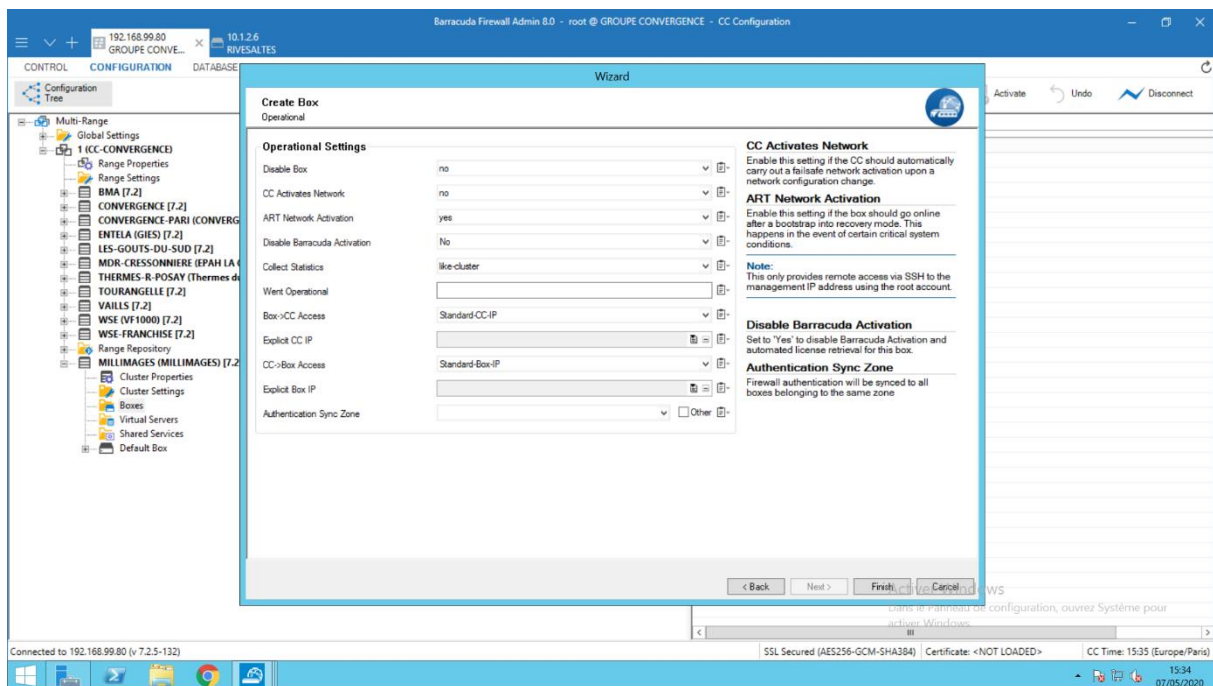
Create Box

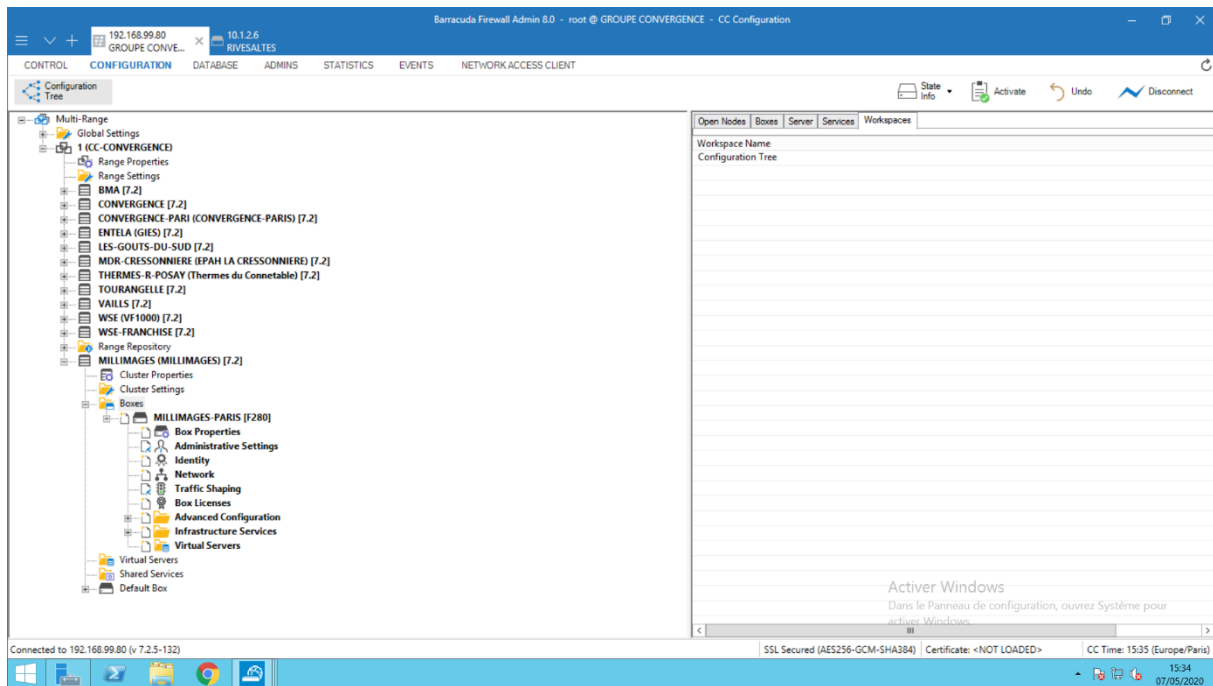


Attention à la version du Firewall avec les « Rev. B »

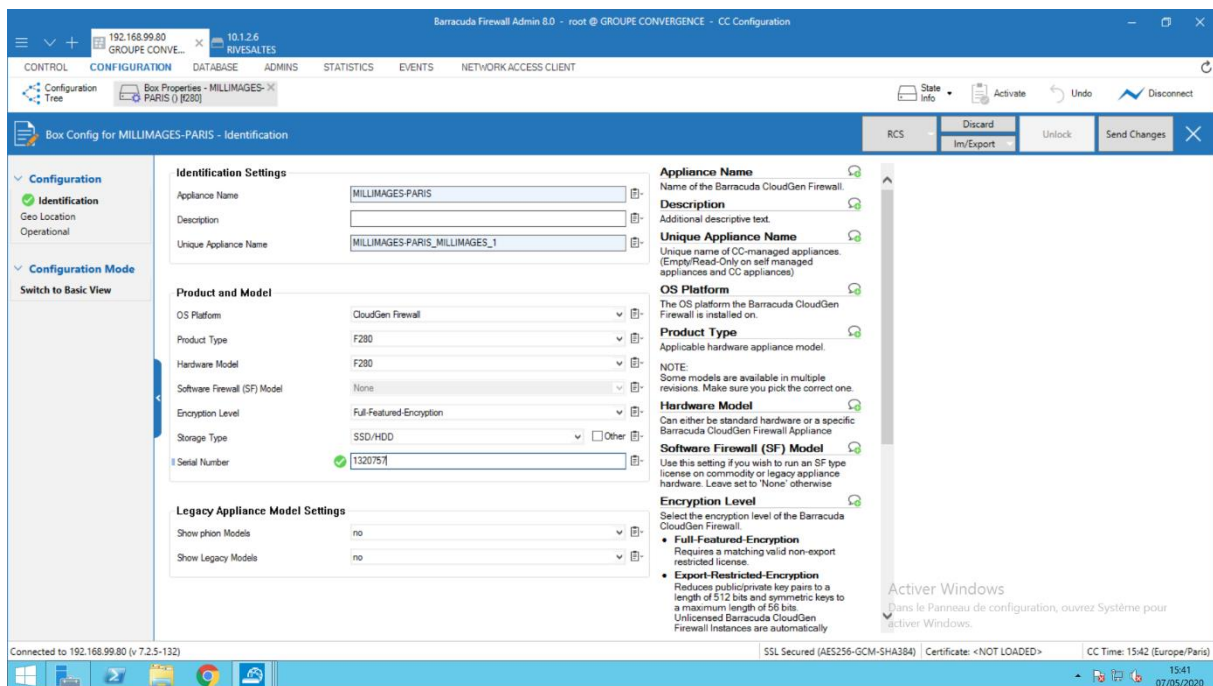


Localisation

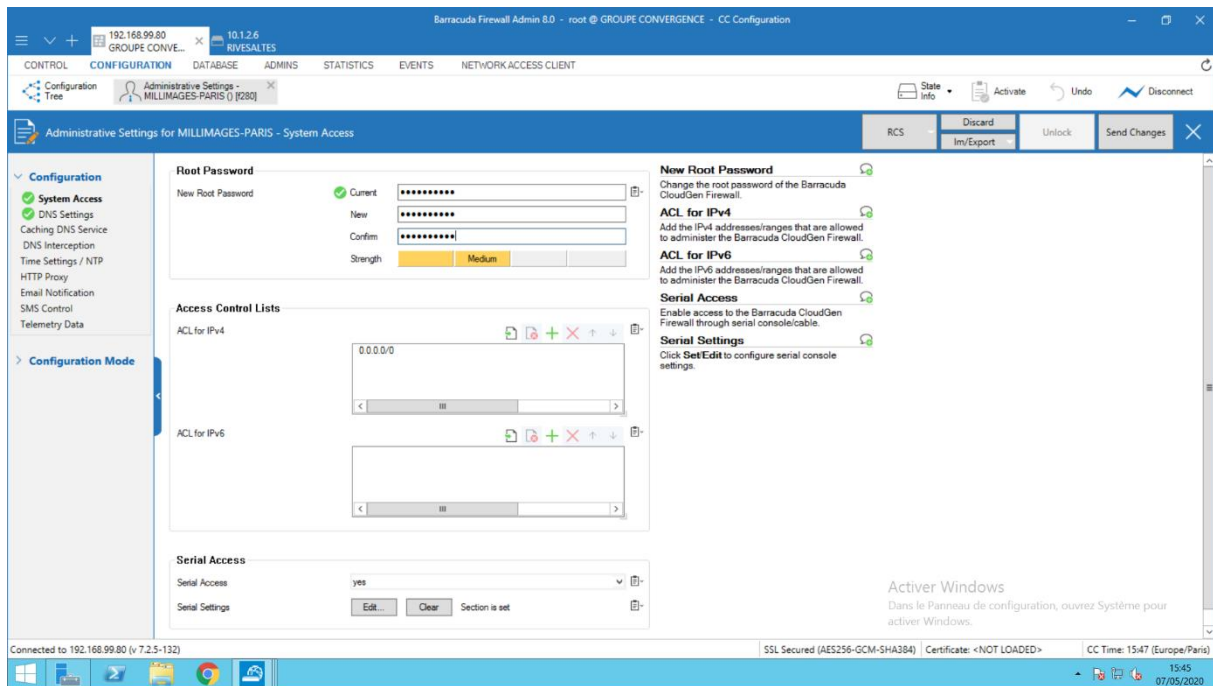




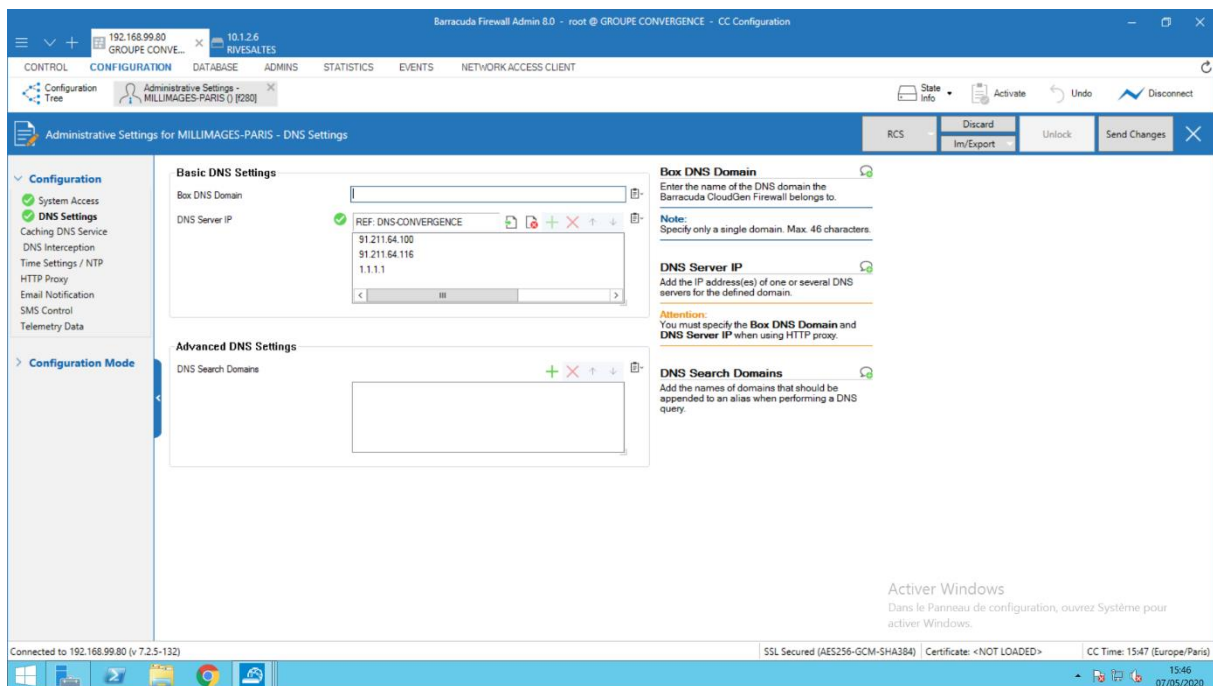
Cliquer sur Activer pour valider la configuration.



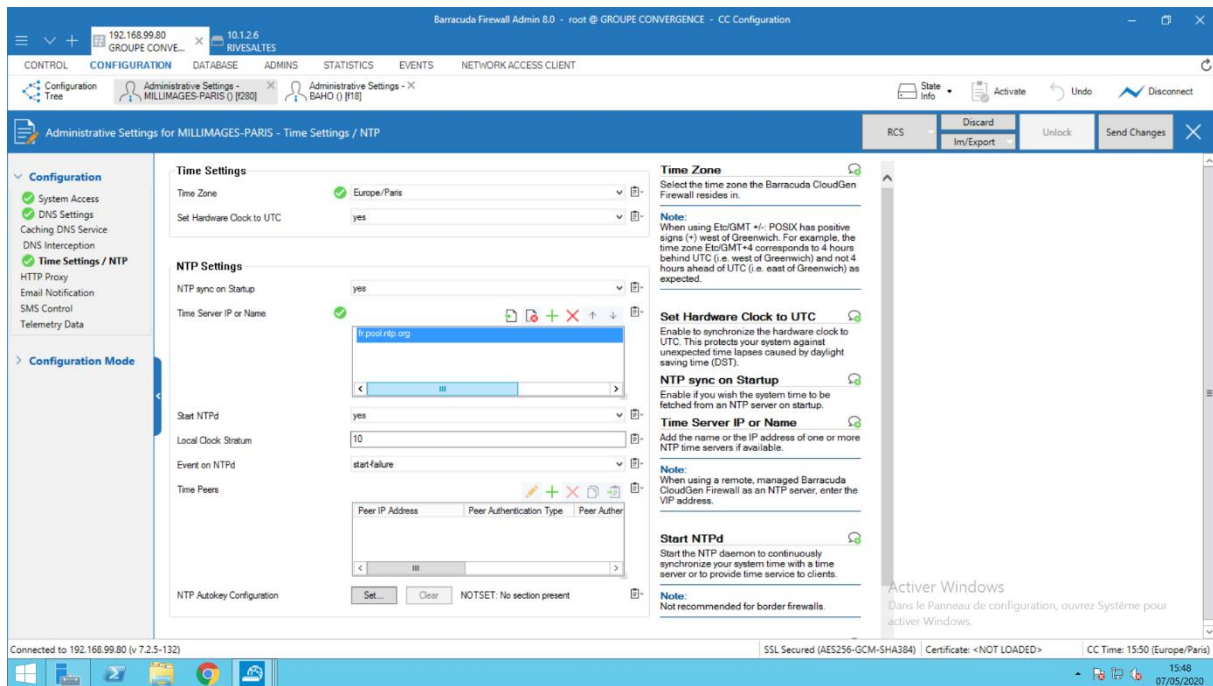
Ne pas oublier de faire Lock en haut à droite pour effectuer une modification.



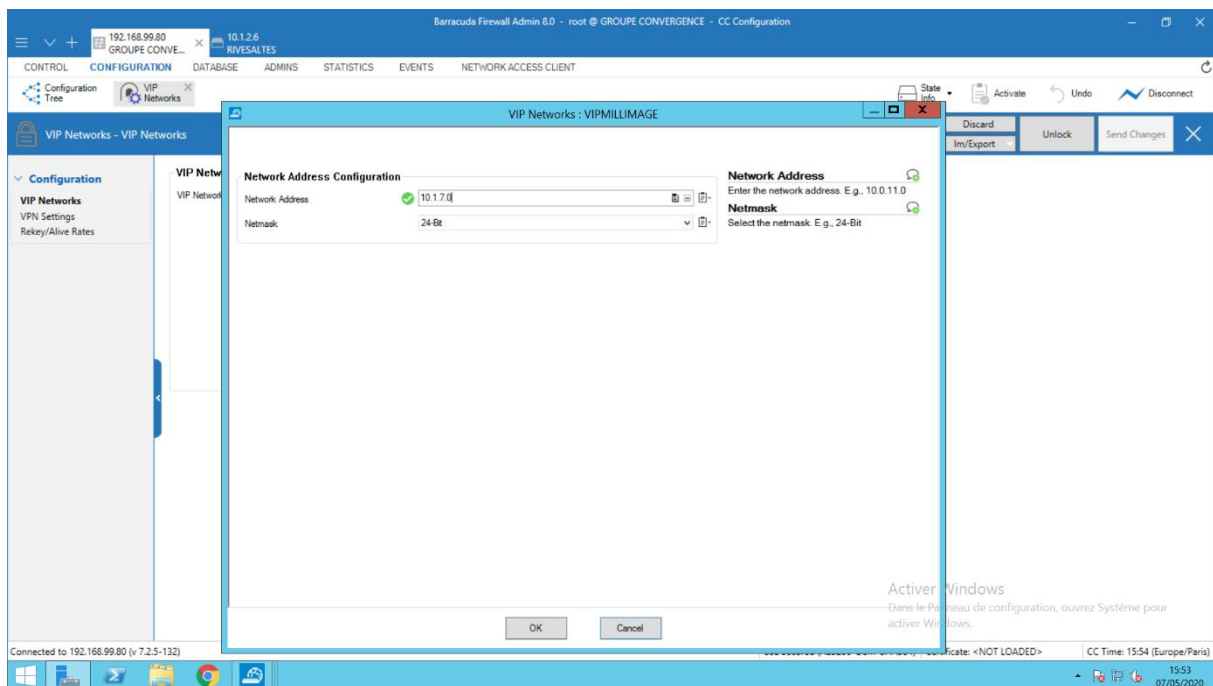
Modification du mot de passe Root si besoin. (mot de passe de base : ngf1r3wall)



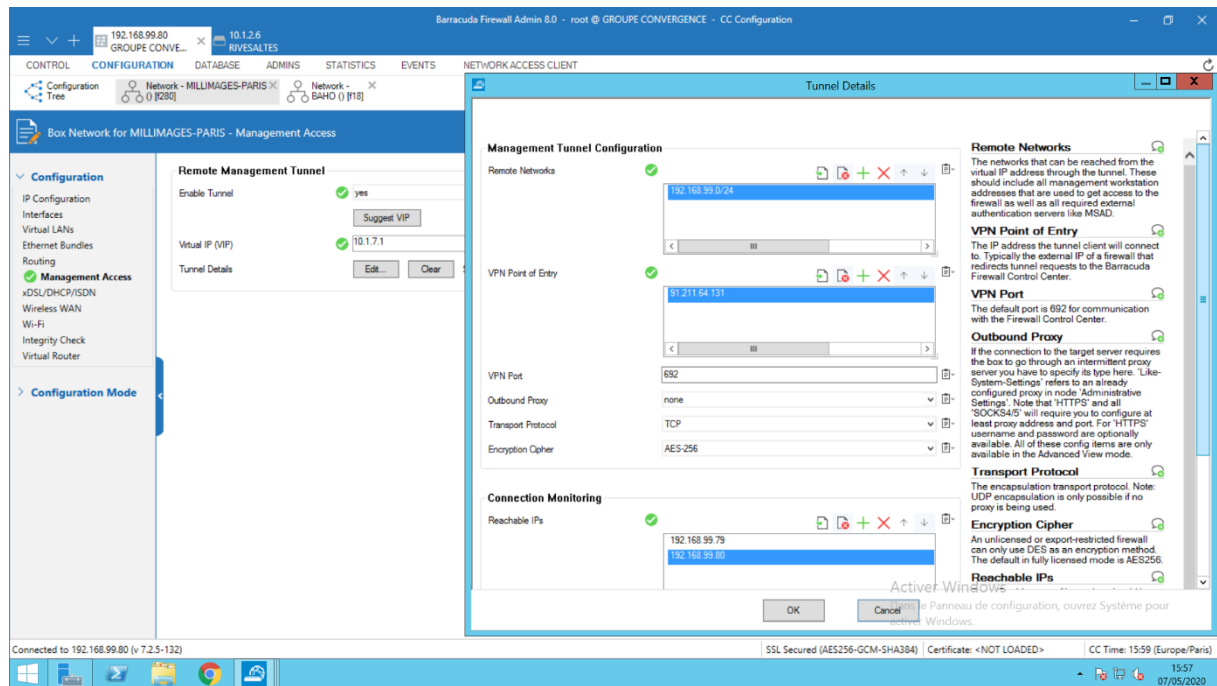
Configuration des DNS. (Il suffit de choisir le groupe préinstallé)



Time zone + NTP



Création du VIP Network. (C'est le réseau avec lequel le CC et le firewall vont discuter)



Et voila nous avons fini la création de la box ici elle sera nommée IDK-ANTHONY

2- Configuration Réseau

- LAN

Dans Configuration>box>IDK-ANTHONY>Network>Virtual LANs

On va pouvoir ajouter un VLAN de notre choix (oubliez pas de cliquer sur LOCK sinon vous ne pourrez pas modifier quoi que se soit)

🔒 VLANs : VLAN01

Virtual LAN Configuration

<input checked="" type="checkbox"/> Physical VLAN Interface	p3	<input type="checkbox"/> Other
<input checked="" type="checkbox"/> VLAN Tag	2900	
<input checked="" type="checkbox"/> Header Reordering	<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> VLAN Description	VLAN2900	

Ensuite dans advance routing on va ajouter la route de configuration :

🔒 IPv4 Routing Table : IPV401

IPv4 Route Configuration

<input checked="" type="checkbox"/> Target Network Address	0.0.0.0/0
<input checked="" type="checkbox"/> Gateway	192.168.11.1
<input checked="" type="checkbox"/> Route Metric	200
<input checked="" type="checkbox"/> Route Type	gateway
<input checked="" type="checkbox"/> Interface	
<input checked="" type="checkbox"/> Trust Level	Unclassified
<input checked="" type="checkbox"/> Default Gateway	
<input checked="" type="checkbox"/> Advertise Route	no
<input checked="" type="checkbox"/> GTI Network	no
<input checked="" type="checkbox"/> Route Origin	User created
<input checked="" type="checkbox"/> Active	yes

- WAN:

Ensuite, on va ajouter une nouvelle connexion PPPoE depuis le menu Network / xDSL/DHCP (menu avancée) :

xDSL Setup

xDSL Enabled

xDSL Links

Name	Link Active	Standby Mode
XDSL01	yes	no

Note: An external DSL modem is required to configure xDSL links.

Ensuite on double clique sur le xDSL Links et lors du choix de l'interface indiquer l'interface avec le tag :

PPPoE Connection Details

Ethernet Interface ☒ Other

Nous continuons par indiquer notre compte PPPoE :

Authentication

Authentication Method

User Access ID

☒ Add SubID

User Access Sub-ID

Access Password

New

Confirm

Strength

☒ Add Provider

Provider Name

PPPoE Acceleration

PPPoE Acceleration à Yes afin d'augmenter les performances (avoir plus de débit).

Nous laissons le reste par défaut (on ajuste la règle de Firewall comme dans le 1.)

3- Ajout du service Firewall

Configuration du service afin que le LAN accède à internet

Bien maintenant que tout cela est mise en place on va se tourner sur faire en sorte que notre LAN accède a internet pour cela on va alors appliquer dans :

Configuration>Box>IDK-ANTHONY>Assigned Services>Forwarding Rules

On va pouvoir alors modifier celle qui concerne notre LAN :

Action	Name	Features	Policy Usage	NAT Mode	Service	Source	Destination	User	Sche.
3 Pass SD-WAN	BOX-LAN-2-INTERNET		All Policy Pr...	N.A.	Any	192.168.11.1	Internet	Any	Always
4 Pass SD-WAN	BOX-LAN-2-LAN		All Policy Pr...	N.A.	Any	Trusted LAN	Trusted LAN	Any	Always
7 Pass SD-WAN	BOX-VPNCLIENTS-2-LAN		All Policy Pr...	N.A.	Any	0.0.0.0/0	Trusted LAN	Any	Always
8 Block	BLOCKALL		N.A.	N.A.	Any	0.0.0.0/0	Any	Any	Always

On clique sur lock puis on va pouvoir modifier de manière a autorisé notre VLAN

(192.168.11.1) à se connecter a des services (ici any) avec pour destination internet :

Views: Rule, Advanced, ICMP Handling

Object Viewer: ☒ Object Viewer

Rule: BOX-LAN-2-INTERNET

Allows Internet access from trusted LAN for typical applications

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
<explicit-src>	Any	Internet
192.168.11.1	Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 169.254.0.0/16 NOT 192.168.0.0/16

Authenticated User: Any

Policies: All Policy Profiles

NAT is configured and applied in the SDWAN Policies

Schedule: Always

OK Cancel

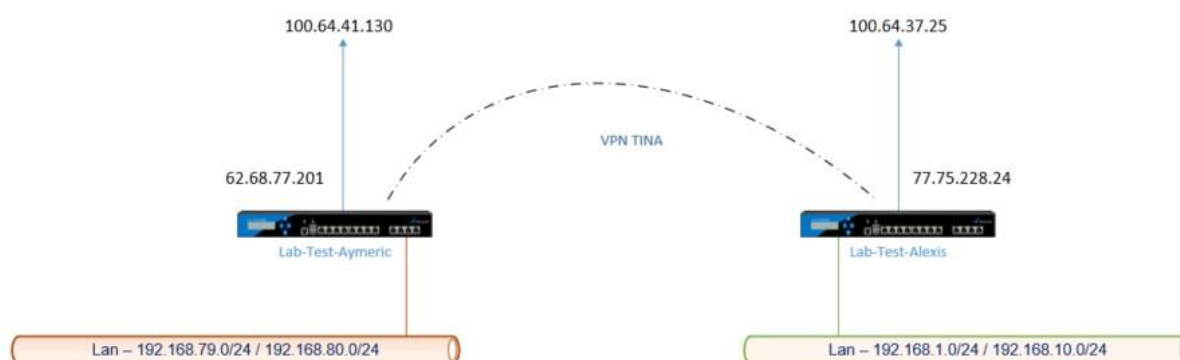
4- Ajout du service VPN

Configuration du service afin de pouvoir se connecter au site distant

Afin d'être le plus clair possible dans la suite de ce tutoriel, voici le plan d'adressage utilisé sur les différents réseaux locaux, ainsi que les IP public afin d'atteindre le service VPN. On utilisera ici des Box préfêtes dans le cadre de se travail

	LAB-TEST-AYMERIC	LAB-TEST-ALEXIS
VPN réseau local	192.168.80.0/24	192.168.10.0/24
VPN réseau distant	192.168.10.0/24	192.168.80.0/24
IP Public (En écoute pour le VPN)	62.68.77.201	77.75.228.24

Pour résumer, voici les IP sur le schéma ci-dessous :



On va appeler « Lab-Test-Aymeric » le site principal, et « Lab-Test-Alexis » le site distant.

Partie réseau

Cette partie va permettre de savoir quel sous réseaux ou souhaite faire passer dans le tunnel.

Premièrement, dans la partie network, on va supprimer les loopback qui ne nous servent pas. Aussi, dans la partie Shared IP, on indique les ip qui doit être partagés, et donc inclus par le VPN.

Management Network and IPs

Interface: ☐ Other

Management IP:

Associated Netmask:

Responds to Ping:

Use for NTPd:

Advertise Route:

Shared IPs in this Network

IP Address	Alias for this IP	Responds to
192.168.79.250	None	yes

Remote Management Tunnel

Enable Tunnel:

Virtual IP (VIP):

Tunnel Details: Section is set

Shared Networks and IPs

Shared Networks and IPs

Name	Interface	Network Address
IPPUB	lo	62.68.77.201/32
test	lo	192.168.80.0/24

Service VPN

On commence par ajouter le service VPN sur les deux Firewalls ...

Ajouter le service VPN sur le FW :

Enable Service	yes	
Service Name	VPN-LAB-AYMERIC	
Description		
Software Module	VPN Service	<input type="checkbox"/> Other

Listening IP Configuration

Listening IP	Explicit	
Explicit IPs		
	<div>62.68.77.201</div> <div>< ></div>	

Dans la partie Listening IP, il faut mettre en Explicit et indiquer l'ip public du FW.
 Dans la capture cidessus, nous sommes sur le premier Firewall donc on met 62.68.77.201. Si le service est déjà créé, il faut se rendre dans « Service Properties »

Faire la même chose sur le second firewall en ajustant l'ip public.

Ensuite, on désactive l'écoute sur le port 443 :

- VPN-LAB-AYMERIC (VPN-Service)
 - SSL-VPN CC Config
 - L2TP/PPTP Settings
 - Service Properties
 - SSL-VPN
 - VPN GTI Tunnels CONVERGENCE-TEST 1
 - VPN GTI Settings
 - VPN Settings**
 - Client to Site
 - Site to Site
 - WAN Optimization

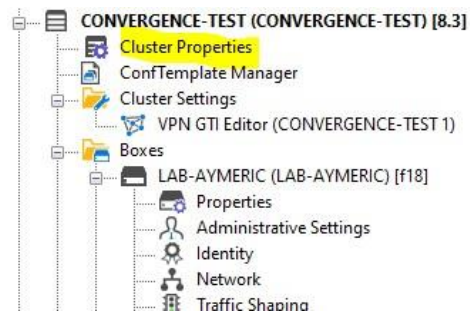
VPN Settings

- General
- IPSec
- Routed VPN
- Client Networks
- Service Keys
- Root Certificates
- Service Certificates

Service

- Listen on port 443** ☐
- Local VPN listen port
- Maximum number of tunnels
- CRL poll time (minutes)
- Site to Site authentication ☒
- Add VPN routes to main routing table
- Allow concurrent user sessions ☒

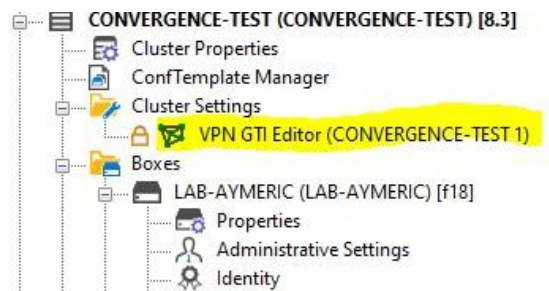
Il faut maintenant créer le service VPN GTI Editor dans cluster properties «
 Logiquement cette étape n'est plus nécessaire depuis la version 9.0) :



Specific Settings

Disable Updates	no
Collect Statistics	like-range
Own Cook Settings	no
Own Event Settings	no
Own Firewall Objects	no
Own VPN GTI Editor	yes
Own Access Control Objects	no
Own Traffic Shaping Settings	no
Own Certificate Store	no

Maintenant on peut commencer la configuration du VPN TINA :



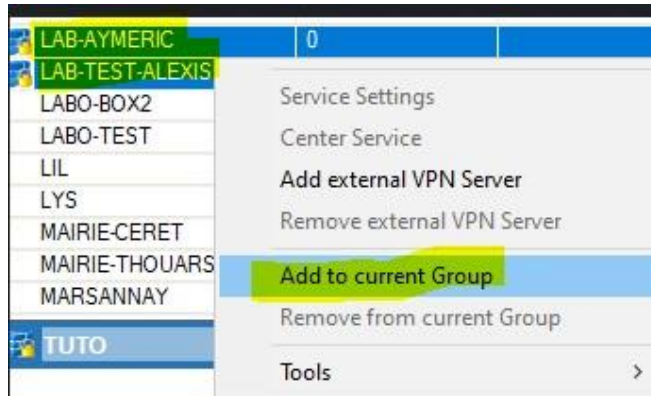
On va créer un nouveau Group via un clic-droit :

Group TINA-THOUARS-CASTLE

TINA Properties		Edit IPSe
Transport	ESP	
Encryption	AES256	
Authentication	SHA256	
Dynamic Mesh	No	
Dynamic Mesh Timeout [sec]	600	
Dynamic Mesh Interface	Static	
Security		
CA Certificate		
X509 Certificate Condition		
Accepted Ciphers	AES, CAST, Blowfish, 3DES, AES256	
SD-WAN		

Maintenant dans l'onglet « Services », on va ajouter nos deux Firewalls dans le Group créé à l'instant.

Pour cela, dans cet onglet, on clique sur Other (au même niveau que le menu service), puis sur les deux Firewalls en question, il suffit de faire un clic droit pour les ajouter dans un group existant :

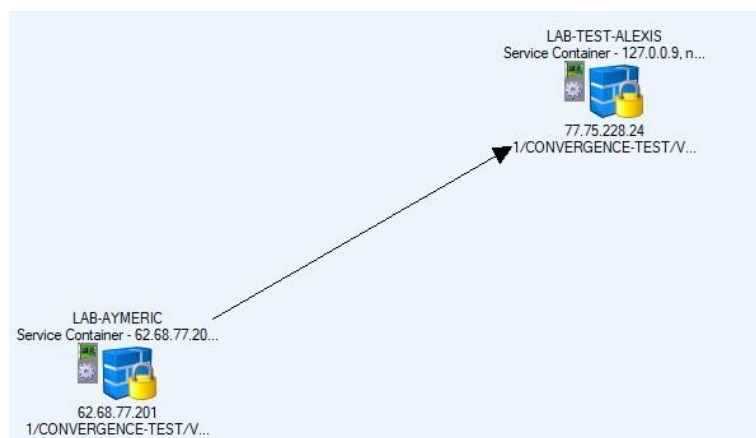


Une fois fait, on peut de nouveau cliquer sur Other, afin d'afficher uniquement les Firewalls dans le Groups « Tuto » :

Groups	Services	WanOpt	Root Certificates						Show	Group	Other
Server			#Groups	Groups	Range	Cluster	Service	Internal Name			
LAB-AYMERIC			1	TUTO	1	CONVERG...	VPN-LAB-AYMERIC	VPN-LAB-AYMERIC_CONVERGENCE-TEST_1			
LAB-TEST-ALEXIS			1	TUTO	1	CONVERG...	VPN-LAB-ALEXIS	VPN-LAB-ALEXIS_CONVERGENCE-TEST_1			

Ensuite, Dans l'espace ci-dessous, il faut relier les deux sites entre eux afin de monter le tunnel. Pour cela, il faut cliquer sur le premier firewall puis diriger la flèche vers le second Firewall.

Nous devons obtenir quelque chose comme ça :



Une fois fait, on va vérifier que les subnets locaux des deux côtés sont bon. Pour cela, il faut cliquer sur la flèche puis sur LAB-AYMERIC_LAB-TEST-ALEXIS. Dans cette fenêtre, on peut ajouter des subnets locaux dans la partie local networks. Sur le premier Firewall, on va modifier la valeur du transport source :

From **LAB-AYMERIC** | Edit GTI Default

VPN-LAB-AYMERIC/CONVERGENCE-TEST/1
Explicit: 62.68.77.201

Direction	active
Transport Source IP/Interface	Explicit
Explicit	62.68.77.201
Transport Listening IP/Hostname	<Use-Transport-Source>
Explicit Listening	62.68.77.201
Local Networks	192.168.80.0/24, 192.168.79.0/24
SD-WAN - Bandwidth Protection	
Advanced	
Proxy	
Security	
Scripts	

Il faut répéter cette action sur le firewall visé.

Règle de Firewall

Maintenant que le tunnel est monté sur le deux sites, on peut le vérifier depuis le CC :

LAB-AYMERIC	LAB-AYMERIC	10.0.0.211	8.3.1-0086	France	F18	1066329	
LAB-TEST-ALEXIS	LAB-TEST-ALEXIS	10.0.0.210	8.3.1-0086	France	F18	1226011	

Ou, depuis les Firewalls dans l'onglet VPN, puis Status :

DASHBOARD	CONFIGURATION	CONTROL	FIREWALL	VPN	LOGS	EVENTS	SSH			
 Site-to-Site	 Client-to-Site	 Status								
Tunnel	Name	Type	Group	Info	User	State	Succ.	Fail	Last Access	Last Peer
 TINA	LAB-AYMERIC-LAB-TEST-ALEXIS			FW Tunnel		ACTIVE	3	0	3h 15m 8s	77.75.228.24

On peut voir que le tunnel est up depuis plus de 3h.

Afin d'autoriser le trafic des différents LAN à travers le tunnel, il faut créer une règle sur chaque Firewall afin d'autoriser le LAN du Firewall vers le LAN distant. Voici la modification qu'il faut appliquer sur les deux Firewalls (capture ci-dessous depuis le FW LAB-AYMERIC). Pour cela, il faut afficher les règles désactivées, puis activer la règle BOX-LAN-2-VPN-SITE (attention au menu Avancée) :

→ Pass

BOX-LAN-2-VPN-SITE

Allows unrestricted communication between the trusted LAN networks and VPN sil ...

☒ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
Trusted LAN	Any	<explicit-dest>
Ref: Trusted LAN Networks	Ref: Any-TCP	192.168.10.0/24
Ref: Trusted Next-Hop Networks	Ref: Any-UDP	192.168.1.0/24
	Ref: ICMP	
	ALLIP	

Authenticated User	Policies	Connection Method
Any	IPS	Original Source IP
	Default	Original Source IP (same port)
	Application Policy	
	AppControl, URL Filter	
	SSL Inspection Policy	
	N.A.	
	Schedule	
	Always	
	QoS Band (Fwd)	
	Business (ID 3)	

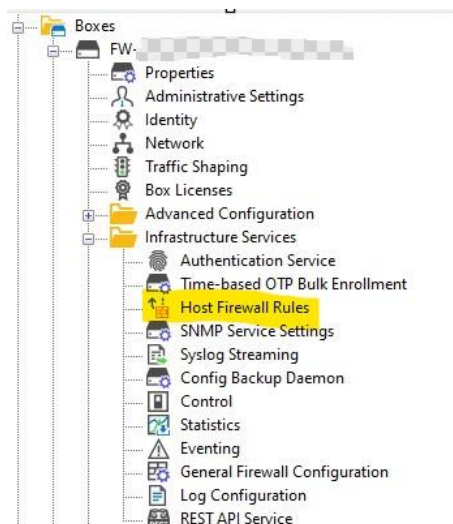
Voici capture pour la version 9 :

Authenticated User	Policies	Connection Method
Any	None	Original Source IP
	NAT	Original Source IP (same port)
	Explicit NAT	
	Schedule	
	Always	
	QoS Band (Fwd)	
	Medium (ID 3)	
	QoS Band (Reply)	
	Like-Fwd	

OK Cancel

On modifie en fonction des subnets distants. Sur le Firewall distant, les subnets de destinations seront les IP Lan du premier Firewall.

On modifie aussi les règles Outbound dans les Host Firewall Rules :



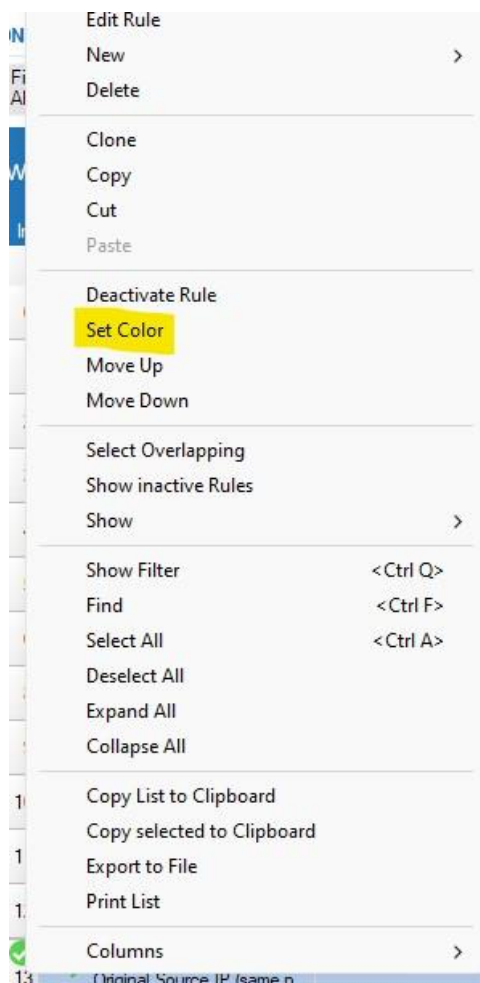
Il vous suffit de cloner la règle OP-SRV-VPN et de jouer avec la destination et la connexion méthode.

Pour la règle copy1 il vous suffit de mettre en destination l'ip pub du distant.

Pour la deuxième règle, il faut natter les flux vers internet avec l'ip pub du site.

→ Pass Original Source IP (same port)	OP-SRV-VPN-INTERNET-Copy1	✕	NGF-OP-VPN ECHO . GRE, IPSEC-AH, IP...	SharedIPs	77.75.228.24
→ Pass Explicit IP 62.68.77.201	OP-SRV-VPN-INTERNET	✕	NGF-OP-VPN ECHO . GRE, IPSEC-AH, IP...	SharedIPs	Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...
→ Pass Original Source IP (same port)	OP-SRV-VPN	✕	NGF-OP-VPN ECHO . GRE, IPSEC-AH, IP...	SharedIPs	Any 0.0.0.0/0

Il est obligatoire de mettre une couleur quand une règle est modifiée dans les host firewall rules afin de retrouver facilement la règle qui a été modifiée. Il faut donc effectuer un clic droit sur la règle et aller sur set color.



Tests

Depuis LAB-AYMERIC, on accède bien aux deux réseaux locaux :

```
[AYMERIC@LAB-AYMERIC:~]$ ping 192.168.1.254 -I 192.168.80.100
PING 192.168.1.254 (192.168.1.254) from 192.168.80.100 : 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=64 time=80.8 ms
64 bytes from 192.168.1.254: icmp_seq=2 ttl=64 time=79.5 ms
^C
--- 192.168.1.254 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 79.527/80.164/80.802/0.697 ms
[2022-08-01 03:47 PDT] [-standard-] [-Barracuda Networks-]
[AYMERIC@LAB-AYMERIC:~]$ ping 192.168.10.100 -I 192.168.80.100
PING 192.168.10.100 (192.168.10.100) from 192.168.80.100 : 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=64 time=62.7 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=64 time=62.1 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=64 time=61.8 ms
^C
--- 192.168.10.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 61.856/62.247/62.747/0.423 ms
```

Depuis LAB-TEST-ALEXIS :

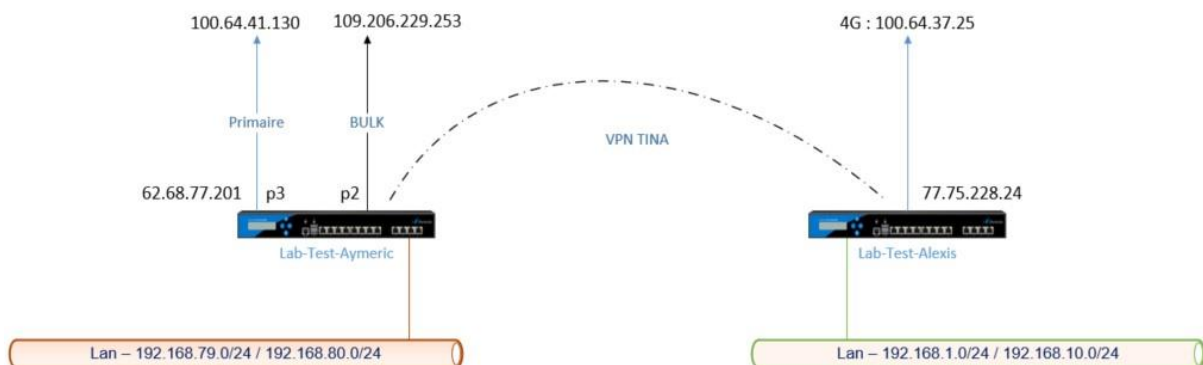
```
[AYMERIC@LAB-TEST-ALEXIS:~]$ ping 192.168.79.250 -I 192.168.10.100
PING 192.168.79.250 (192.168.79.250) from 192.168.10.100 : 56(84) bytes of data.
64 bytes from 192.168.79.250: icmp_seq=1 ttl=64 time=61.2 ms
64 bytes from 192.168.79.250: icmp_seq=2 ttl=64 time=68.7 ms
^C
--- 192.168.79.250 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100lms
rtt min/avg/max/mdev = 61.259/65.013/68.768/3.763 ms
[2022-08-01 12:51 CEST] [-standard-] [-Barracuda Networks-]
[AYMERIC@LAB-TEST-ALEXIS:~]$ ping 192.168.80.100 -I 192.168.10.100
PING 192.168.80.100 (192.168.80.100) from 192.168.10.100 : 56(84) bytes of data.
64 bytes from 192.168.80.100: icmp_seq=1 ttl=64 time=67.7 ms
64 bytes from 192.168.80.100: icmp_seq=2 ttl=64 time=58.6 ms
^C
--- 192.168.80.100 ping statistics ---
3 packets transmitted, 2 received, 33% packet loss, time 200lms
rtt min/avg/max/mdev = 58.624/63.210/67.797/4.593 ms
```

Le ping est ok dans le deux sens, en matchant la règle précédemment ajouté :

AID	IP Proto	Port	Source	Interface	User	Destination	Output-IF	Src NAT	Next Hop	Count	Last	Rule	Info
✓ 393	ICMP		192.168.10.100	vpn0		192.168.80.100	vpn0			2		OP.SRV-VPN	Normal Operation
✓ 384	ICMP		192.168.80.100	vpn0		192.168.10.100				3	5m 59s	OP.SRV-VPN	Normal Operation
✓ 387	ICMP		192.168.80.100	vpn0		192.168.1.254				2	6m 08s	OP.SRV-VPN	Normal Operation
✓ 386	ICMP		192.168.80.100	vpn0		192.168.1.154				1	6m 23s	OP.SRV-VPN	Normal Operation
✓ 382	ICMP		192.168.80.100	vpn0		192.168.1.100				1	7m 06s	OP.SRV-VPN	Normal Operation

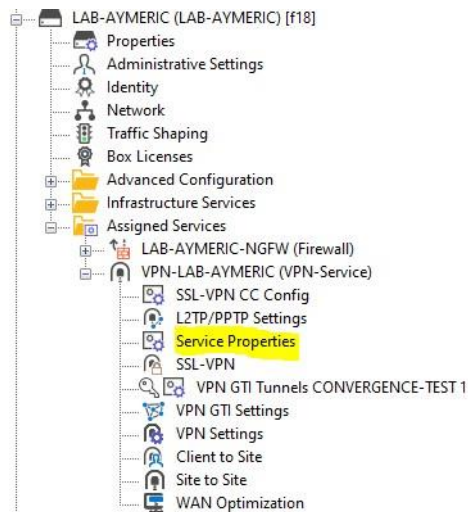
Création du BULK

L'objectif du BULK, est qu'en cas de perte d'un lien, le second lien prenne le relais sur le VPN TINA. Nous avons donc modifié le schéma réseau afin d'avoir un deuxième lien sur le premier Firewall :



Le lien sur p2 est présent pour le BULK. Il s'agit d'un deuxième lien PPPoE (nommé ppp2 sur le Firewall). En cas de coupure du lien primaire, le second prend le relais pour le VPN.

On va maintenant indiquer au service VPN qu'on possède une nouvelle IP public :



On rajoute la nouvelle IP en explicit :

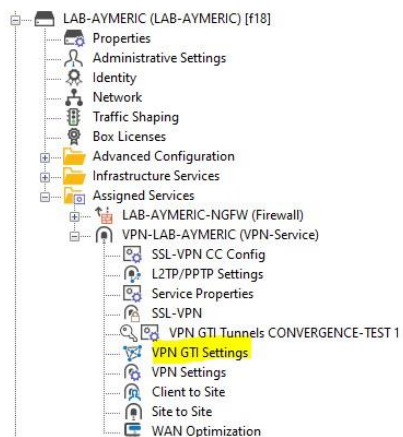
Listening IP Configuration

Listening IP

Explicit IPs

62.68.77.201

109.206.229.253



On rajouter aussi la nouvelle IP public :

IPv4 Transport Settings

Transport Source IP

Explicit Transport Source IP

62.68.77.201

109.206.229.253

Transport Listening IP

Explicit Transport Listening IP

62.68.77.201

109.206.229.253

Ensuite, de la même manière que le premier tunnel, dans la GTI Editor, on tire une flèche du 1^{er} Firewall (LAB-AYMERIC) vers le second (LAB-TEST-ALEXIS).

Ensuite, la configuration va être un peu différente du premier tunnel. Modifier la configuration pour avoir :

Direction	active	IP Version	IPv4	Direction	passive
Transport Source IP/Interface	Explicit	Transport	UDP	Transport Source IP/Interface	Explicit
Explicit	ppp2	Encryption	AES256	Explicit	77.75.228.24
Transport Listening IP/Hostname	<Use-Transport-Source>	Authentication	MD5	Transport Listening IP/Hostname	Explicit
Explicit Listening	109.206.229.253	SD-WAN Classification	Bulk	Explicit Listening	77.75.228.24
SD-WAN - Bandwidth Protection		SD-WAN ID	1	SD-WAN - Bandwidth Protection	
Advanced		Compression	Disabled	Advanced	
Proxy		Dynamic Mesh Interface	Static	Proxy	
Security		SD-WAN		Security	
Scripts		SD-WAN - Bandwidth Protection		Scripts	
		SD-WAN - VPN Envelope Policy			
		Advanced			
		Key Time Limit [min]	10 mins		
		Key Traffic Limit	No Limit		
		Identification Type	Public Key		
		Tunnel Probing [sec]	30 secs		
		Tunnel Timeout [sec]	20 secs		
		Packet Balancing	None		
		High Performance Settings	No		

Dans le menu de gauche, on renseigne l'interface en explicit. Cette interface est le nom donné par le Barracuda sur le second lien. Cette information est disponible depuis le Menu Control / Network :

DASHBOARD	CONFIGURATION	CONTROL	FIREWALL
Services	Network	Resources	Lic
Interfaces/IPs	IPs	Interfaces	Proxy ARPs
dhcp, Speed=-1Mb/s, Duplex=Unknown			
lo			
p1, Speed=1000Mb/s, Duplex=Full			
p3, Speed=1000Mb/s, Duplex=Full			
pppoe1, Speed=1000Mb/s, Duplex=Full			
pppoe2, Speed=1000Mb/s, Duplex=Full			
tap3, Speed=10Mb/s, Duplex=Full			
vpn0			
vpnr0			
xDSL[ppp1]			
100.64.41.130/32			
xDSL[ppp2]			
109.206.229.253/32			

Maintenant, on peut regarder que les tunnels sont monté. En se connectant sur le Firewall, depuis l'onglet VPN, on peut voir le status du tunnel :

DASHBOARD

CONFIGURATION

CONTROL

FIREWALL

VPN

LOGS

EVENTS

SSH

Site-to-Site

Client-to-Site

Status

Tunnel	Name	Type	Group	Info	User	State	Succ.	Fail	Last Access	Last Peer	Last Info
<div><div>TINA</div></div>	LAB-AYMERIC-LAB-TEST-ALEXIS	<div><div></div></div>		FW Tunnel		ACTIVE	11	0	16h 9m 35s	77.75.228.24	Resp. Access Granted
<div><div>TINA</div></div>	LAB-AYMERIC-LAB-TEST-ALEXIS-1	<div><div></div></div>		FW Tunnel		ACTIVE	5	0	16h 9m 35s	77.75.228.24	Resp. Access Granted

⑨ Access Granted, donc le tunnel est up.

De plus, dans site to site, on peut aussi voir depuis quand le tunnel est up :

DASHBOARD CONFIGURATION CONTROL FIREWALL VPN LOGS EVENTS SSH										
Site-to-Site Client-to-Site Status										
Name	Info	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start	
LAB-AYMERIC-LAB-TEST-ALEXIS		TINA						0	01/08/2022 18:14:38	
Bulk (0)		TINA	62.68.77.201:691	77.75.228.24:691	ESP & UDP	AES256	0%	0	01/08/2022 18:14:38	
Bulk (1)		TINA	109.206.229.253:691	77.75.228.24:691	UDP	AES256	0%	0	01/08/2022 18:14:38	

Bulk (0) ⑦ Tunnel primaire

Bulk (1) ⑦ Tunnel secondaire

Enfin, sur le Control Center, on peut voir l'état global du VPN TINA :

