Compte Rendu GRP 4

AP Infra-Site

Girardey Antoine / Lucas Tardy

Sommaire

Présentations des activités

> Planification du projet

> Réalisation du schéma réseau

> Paramétrage du Pare-feu et du SwitchCoeur

> Routage et Liaison Internet

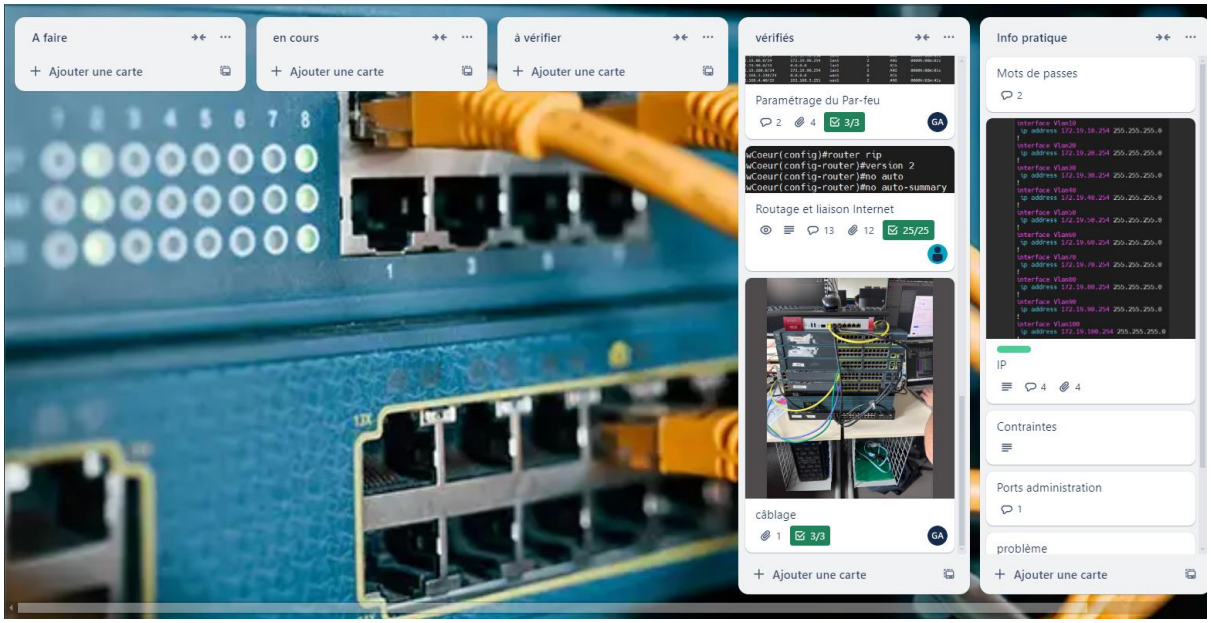
> Administration distante

> Sauvegarde

Planification du projet

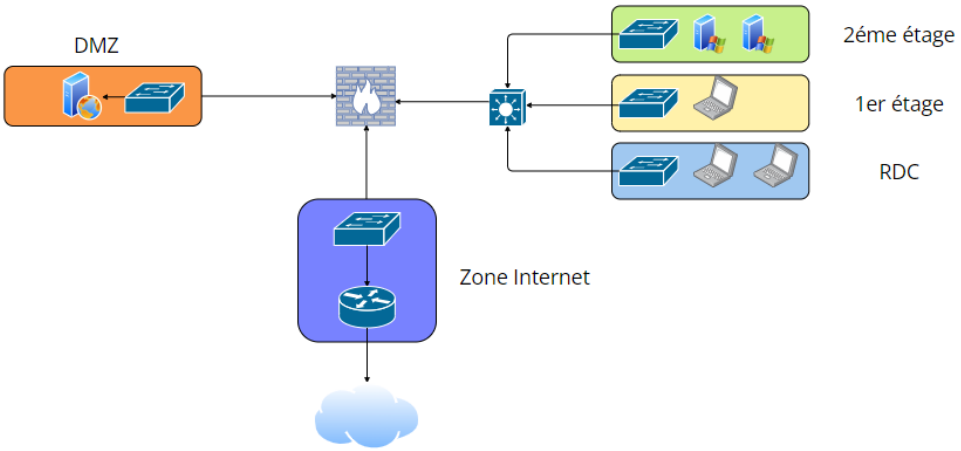
La première phase de ce projet mais néanmoins non négligeable est la planification du projet. Nous entendons par là le recensement de toutes les activités et étapes du projet.

C’est également à cette étape que le Trello est créé et nous suivras tout du long de cette AP. Il faut également créer le GANTT et lui renseigner les premiers temps prévisionnels



Réalisation du schéma réseau

Lors de cette étape l'objectif était d'avoir un schéma clair et précis permettant de pouvoir se repérer visuellement tout en ayant des informations sur les différentes zones qui composent notre AP.



À noter que pour des raisons d'efficacité l'ensemble des adressages IP n'y sont pas répertoriés mais sont présents sur le TRELLO.

Ce schéma réseau logique permet de comprendre le fonctionnement de la maquette ainsi que de mieux pouvoir cibler un problème en cas de défaillance.

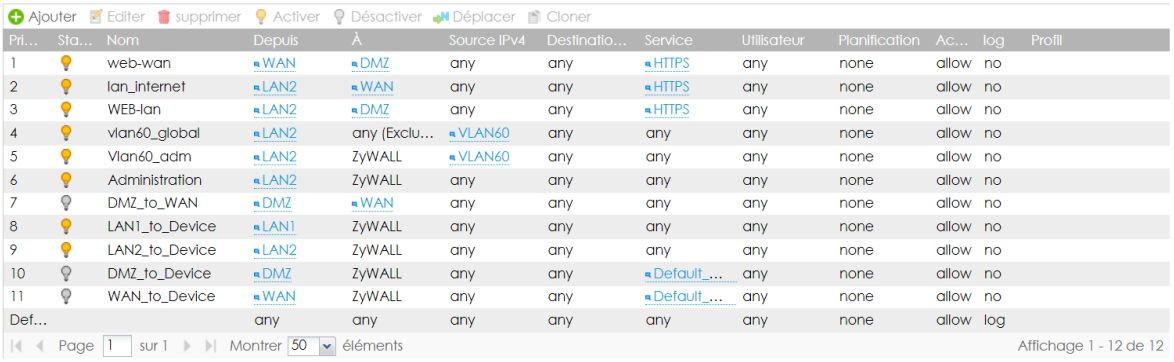
Paramétrage du Pare-feu et du SwitchCoeur

Le paramétrage du SwitchCœur se repose sur les ACL (access-list) qui permettent de définir des règles d'accès pour tous les paquets entrants et sortant de la LAN :

```
ip access-list extended vlanG
 permit ip any host 172.19.100.2
 deny   ip any 172.19.0.0 0.0.255.255
 permit ip any any
```

Voici ci-dessus l'access-list que j'ai paramétrer sur les VLANs de tous les services sauf celui attribué aux administrateurs du LAN, celui attribué au Switchs du LAN, celui qui relie le SwitchCœur et le routeur pare-feu ainsi que celui attribué aux serveurs.

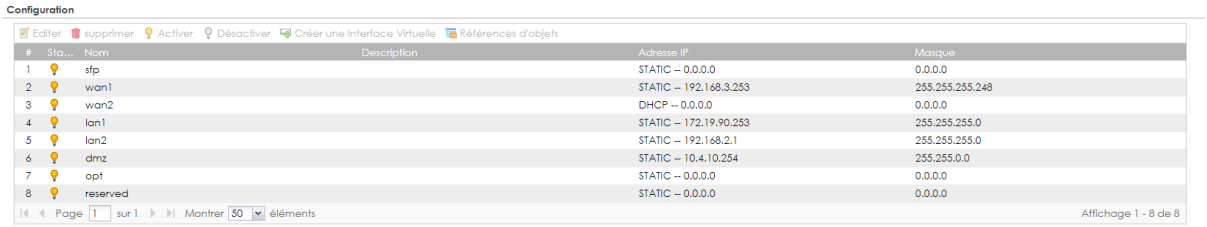
Dans la continuité du switch cœur vient le pare-feu Zyxel, qui comme je le rappelle permet l'interconnexion de la maquette (voir schéma réseau). Par ailleurs étant donné que pour la zone Lan les ACLs sont mise en place au niveau du switch coeur le pare-feu gère lui les règles de filtrage concernant l'entièreté de la maquette comme avec un exemple de règles ci-dessous :


Ajouter Editer supprimer Activer Désactiver Déplacer Cloner

Pri...	Sta...	Nom	Depuis	À	Source IPv4	Destinatio...	Service	Utilisateur	Planification	Ac...	log	Profil
1		web-wan	WAN	DMZ	any	any	HTTPS	any	none	allow	no	
2		lan_internet	LAN2	WAN	any	any	HTTPS	any	none	allow	no	
3		WEB-lan	LAN2	DMZ	any	any	HTTPS	any	none	allow	no	
4		vlan60_global	LAN2	any (Exclu...	VLAN60	any	any	any	none	allow	no	
5		Vlan60_adm	LAN2	ZyWALL	VLAN60	any	any	any	none	allow	no	
6		Administration	LAN2	ZyWALL	any	any	any	any	none	allow	no	
7		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	
8		LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	allow	no	
9		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no	
10		DMZ_to_Device	DMZ	ZyWALL	any	any	Default_...	any	none	allow	no	
11		WAN_to_Device	WAN	ZyWALL	any	any	Default_...	any	none	allow	no	
Def...			any	any	any	any	any	any	none	allow	log	

Page 1 sur 1 Montrer 50 éléments Affichage 1 - 12 de 12

En revanche avant de configurer les règles de filtrages il faut effectuer la configuration et mappage des zones et cela se fait en configurant tout d'abord des ip sur chaque zone :

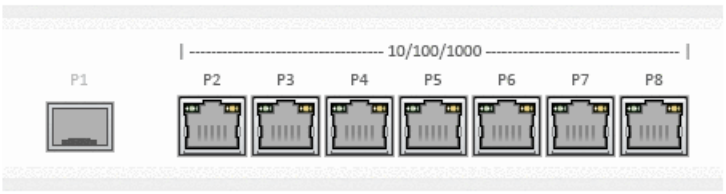

Configuration

Editer supprimer Activer Désactiver Créer une Interface Virtuelle Références d'objets

#	Sta...	Nom	Description	Adresse IP	Masque
1		sfp		STATIC -- 0.0.0.0	0.0.0.0
2		wan1		STATIC -- 192.168.3.253	255.255.255.248
3		wan2		DHCP -- 0.0.0.0	0.0.0.0
4		lan1		STATIC -- 172.19.90.253	255.255.255.0
5		lan2		STATIC -- 192.168.2.1	255.255.255.0
6		dmz		STATIC -- 10.4.10.254	255.255.0.0
7		opt		STATIC -- 0.0.0.0	0.0.0.0
8		reserved		STATIC -- 0.0.0.0	0.0.0.0

Page 1 sur 1 Montrer 50 éléments Affichage 1 - 8 de 8

Puis définir le mappage des ports en fonction de chaque zone :



	P1	P2	P3	P4	P5	P6	P7	P8
sfp	◉							
wan1 (WAN)		◉	○	○	○	○	○	○
wan2 (WAN)		○	◉	○	○	○	○	○
lan1 (LAN1)		○	○	◉	◉	○	○	○
lan2 (LAN2)		○	○	○	○	◉	○	○
dmz (DMZ)		○	○	○	○	○	◉	○
opt (OPT)		○	○	○	○	○	○	◉
reserved		○	○	○	○	○	○	○

Routage et Liaison Internet

Pour pouvoir accès à internet, il faut faire le routage, qui passe sur notre maquette par du routage RIP v2 ainsi que par des routes par défaut, les routes par défaut commencent par 0.0.0.0 0.0.0.0 :

```
SwCoeur#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static rout
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR

Gateway of last resort is 172.19.90.253 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 172.19.90.253
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R        10.0.0.0/8 [120/4] via 172.19.90.253, 00:00:09, Vlan90
R        10.4.0.0/16 [120/1] via 172.19.90.253, 00:00:09, Vlan90
R     172.17.0.0/16 [120/4] via 172.19.90.253, 00:00:09, Vlan90
R     172.18.0.0/16 [120/2] via 172.19.90.253, 00:00:09, Vlan90
      172.19.0.0/16 is variably subnetted, 20 subnets, 2 masks
C        172.19.10.0/24 is directly connected, Vlan10
L        172.19.10.254/32 is directly connected, Vlan10
C        172.19.20.0/24 is directly connected, Vlan20
L        172.19.20.254/32 is directly connected, Vlan20
C        172.19.30.0/24 is directly connected, Vlan30
L        172.19.30.254/32 is directly connected, Vlan30
C        172.19.40.0/24 is directly connected, Vlan40
L        172.19.40.254/32 is directly connected, Vlan40
C        172.19.50.0/24 is directly connected, Vlan50
L        172.19.50.254/32 is directly connected, Vlan50
C        172.19.60.0/24 is directly connected, Vlan60
L        172.19.60.254/32 is directly connected, Vlan60
C        172.19.70.0/24 is directly connected, Vlan70
L        172.19.70.254/32 is directly connected, Vlan70
C        172.19.80.0/24 is directly connected, Vlan80
L        172.19.80.254/32 is directly connected, Vlan80
C        172.19.90.0/24 is directly connected, Vlan90
L        172.19.90.254/32 is directly connected, Vlan90
C        172.19.100.0/24 is directly connected, Vlan100
L        172.19.100.254/32 is directly connected, Vlan100
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
R        192.168.3.0/24 [120/3] via 172.19.90.253, 00:00:09, Vlan90
R        192.168.3.248/29 [120/1] via 172.19.90.253, 00:00:09, Vlan90
R     192.168.4.0/24 [120/2] via 172.19.90.253, 00:00:09, Vlan90
SwCoeur#
```

```
router rip
 version 2
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 passive-interface Vlan40
 passive-interface Vlan50
 passive-interface Vlan60
 passive-interface Vlan70
 passive-interface Vlan80
 passive-interface Vlan100
 network 172.19.0.0
 no auto-summary
```

Ce routage rip est aussi effectué sur le routeur R1 :

```
RNET1>en
Password:
RNET1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.4.254 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.4.254
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
R        10.0.0.0/8 [120/2] via 192.168.4.22, 00:00:17, GigabitEthernet0/1
R        10.4.0.0/16 [120/1] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R     172.17.0.0/16 [120/2] via 192.168.4.22, 00:00:17, GigabitEthernet0/1
R     172.18.0.0/16 [120/1] via 192.168.3.250, 00:00:16, GigabitEthernet0/0
      172.19.0.0/24 is subnetted, 10 subnets
R        172.19.10.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.20.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.30.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.40.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.50.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.60.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.70.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.80.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.90.0 [120/1] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
R        172.19.100.0 [120/2] via 192.168.3.253, 00:00:08, GigabitEthernet0/0
      192.168.3.0/24 is variably subnetted, 3 subnets, 3 masks
R        192.168.3.0/24 [120/1] via 192.168.4.22, 00:00:17, GigabitEthernet0/1
C        192.168.3.248/29 is directly connected, GigabitEthernet0/0
L        192.168.3.251/32 is directly connected, GigabitEthernet0/0
      192.168.4.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.4.0/24 is directly connected, GigabitEthernet0/1
L        192.168.4.42/32 is directly connected, GigabitEthernet0/1
L        192.168.4.43/32 is directly connected, GigabitEthernet0/1
RNET1#
```

```
router rip
 version 2
 passive-interface GigabitEthernet0/1
 network 192.168.3.0
 network 192.168.4.0
 no auto-summary
```

Voici les ip routes qui permet la liaison internet du parfeu :

IP Address/Netmask	Gateway	IFace	Metric	Flags	Persist
0.0.0.0/0	192.168.3.251	wan1	0	ASG	-
10.4.0.0/16	0.0.0.0	dmz	0	ACG	-
127.0.0.0/8	0.0.0.0	lo	0	ACG	-
172.19.10.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.20.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.30.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.40.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.50.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.60.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.70.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.80.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
172.19.90.0/24	0.0.0.0	lan1	0	ACG	-
172.19.100.0/24	172.19.90.254	lan1	2	ARG	0000h:00m:01s
192.168.3.248/29	0.0.0.0	wan1	0	ACG	-
192.168.4.40/29	192.168.3.251	wan1	2	ARG	0000h:02m:41s

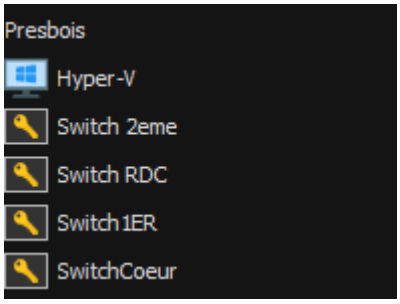
Pour finir le paramétrage de la liaison à internet, il faut faire le NAT sur le routeur qui va faire la liaison entre internet et les réseau LAN et DMZ, ce qui va être fait via une adresse IP publique du routeur qui va être utiliser pour ceux qui veulent se connecter à un élément du LAN, et une autre pour se connecter au serveur Internet :

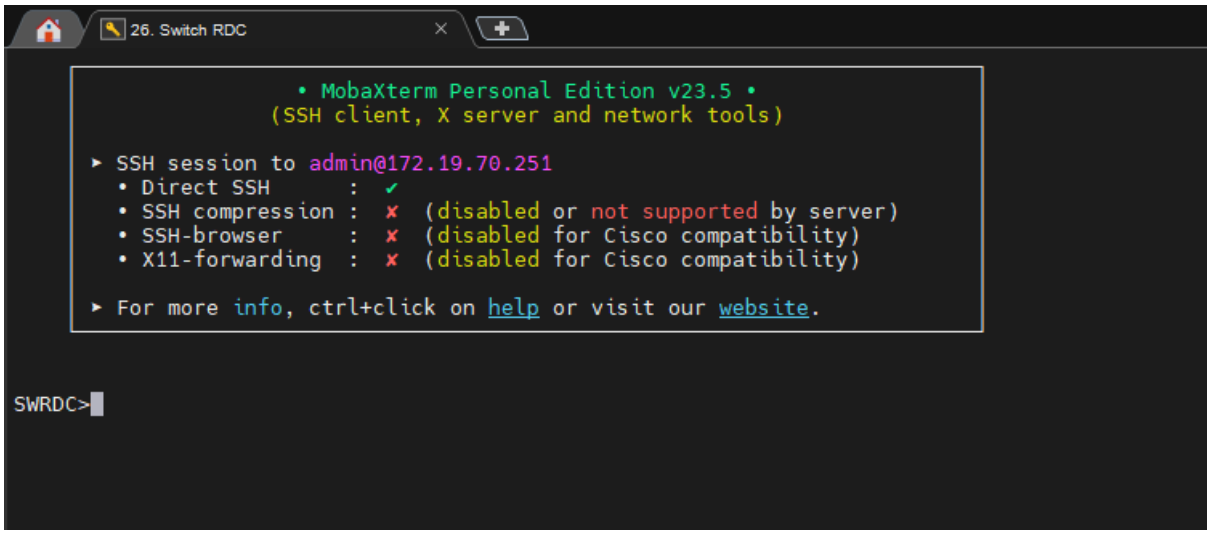
```
!
ip nat inside source list 1 interface GigabitEthernet0/1 overload
ip nat inside source static 10.4.10.1 192.168.4.43
ip route 0.0.0.0 0.0.0.0 192.168.4.254
!
```

Administration à distance

L'administration à distance est un élément essentiel dans le cadre de la gestion et de la maintenance des infrastructures réseau, surtout dans une maquette où différents équipements interagissent.

Tous ces éléments sont administrables sur notre maquette via le logiciel MobaXterm qui permet une sauvegarde des comptes et mots de passe aussi bien en ssh qu'en rdp mais également une sauvegarde des sessions :

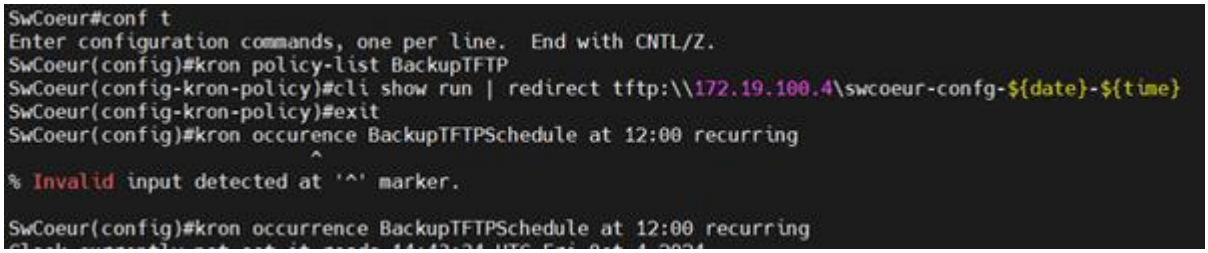


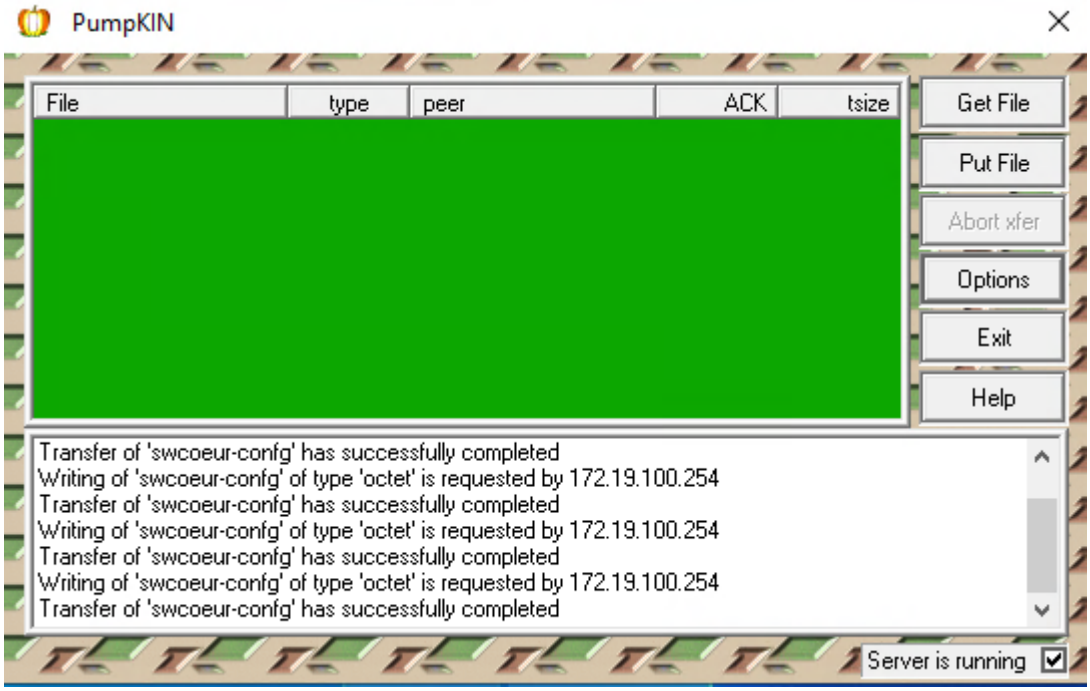


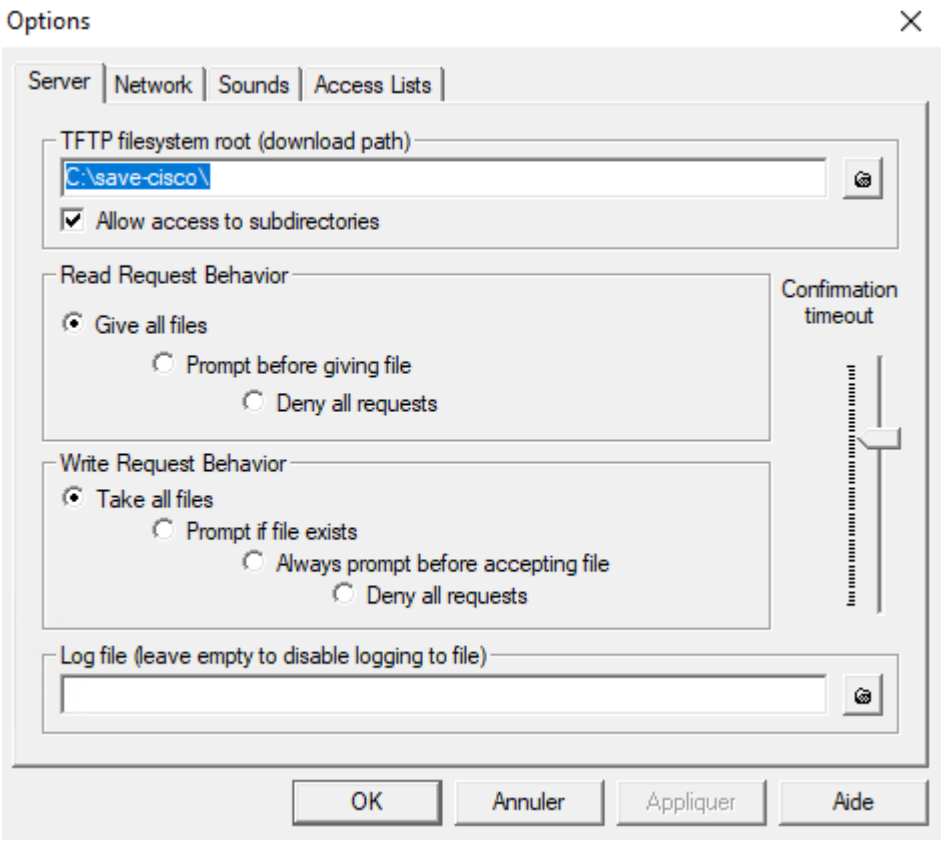
L'utilisation de SSH pour les routeurs et commutateurs ainsi que le Zyxel, combinée aux serveurs Windows en RDP, permet non seulement de simplifier la gestion des systèmes, mais aussi d'augmenter la sécurité et la réactivité face aux problèmes et incidents.

Sauvegarde TFTP

L'automatisation des sauvegardes des configurations des routeurs et switchs via Kron est essentielle pour garantir la continuité et la sécurité des infrastructures réseau. Kron permet de planifier des sauvegardes régulières sans intervention manuelle. Les fichiers de configuration sont envoyés via TFTP (Trivial File Transfer Protocol) vers un poste sous w10 virtualisé sur l'hyper-v du lan, offrant ainsi un environnement sécurisé et facilement gérable. Bien que TFTP soit un protocole non sécurisé, le filtrage d'accès via le parefeu et la restriction d'accès au serveur TFTP assurent une meilleure protection des configurations. Cette solution permet de centraliser les sauvegardes, de simplifier leur gestion et d'assurer une reprise rapide en cas de panne ou d'incident réseau.






Options
Server
Network
Sounds
Access Lists
TFTP filesystem root (download path)
C:\save-cisco\
Allow access to subdirectories
Read Request Behavior
Give all files
Prompt before giving file
Deny all requests
Write Request Behavior
Take all files
Prompt if file exists
Always prompt before accepting file
Deny all requests
Confirmation timeout
Log file (leave empty to disable logging to file)
OK
Annuler
Appliquer
Aide