Nom et Prénom

Colombelle Malone
Bardet Arthur

BTS SIO 2

Document de validation de compétences

AP2-Infra-Site

Dates du projet 04/09->30/09

Equipe 4/20

1. Présentation du contexte d'entreprise

PRESBOIS SAS (société par actions simplifiée), créée en 1998, est une entreprise dont l'activité consiste en la production de panneaux de particules, de panneaux MDF, et à l'offre de solutions pour constructions en ossature bois. Ses besoins en matières premières sont conséquents puisqu'un million de tonnes de bois sont nécessaires à sa production chaque année et en font la plus grosse usine de production de panneaux en fibres de bois en France.

Forte de ses 42 salariés, implantée sur un terrain de 30 hectares, cette entreprise industrielle, connaît depuis sa création une croissance solide et continue. En 2018, elle a vendu 550 000 m3 de panneaux et réalisé un chiffre d'affaires de 133 millions d'euros. Pour 2024, PRESBOIS prévoit des ventes à hauteur de 580 000 m3 pour un chiffre d'affaires estimé à 142 millions d'euros, dont environ 94 % à l'export. Les panneaux vendus en France sont destinés aux grandes surfaces de bricolage, à des clients industriels et à des négociants.
Soucieuse de la qualité de ses produits, l'entreprise l'est aussi quant à la performance et à la sécurité de son réseau informatique.

2. Objectifs attendus

Vous avez mis en œuvre le cloisonnement des services par la mise en place de Vlan. En parallèle un futur projet portant sur la mise en production d'un serveur web sécurisé au sein de la DMZ est à l'étude. Le DSI souhaiterait donc préparer l'infrastructure du réseau en ajoutant à la zone LAN une zone DMZ ainsi qu'une zone Internet afin de répondre aux besoins des salariés de l'entreprise tout en assurant une sécurité maximum du réseau.

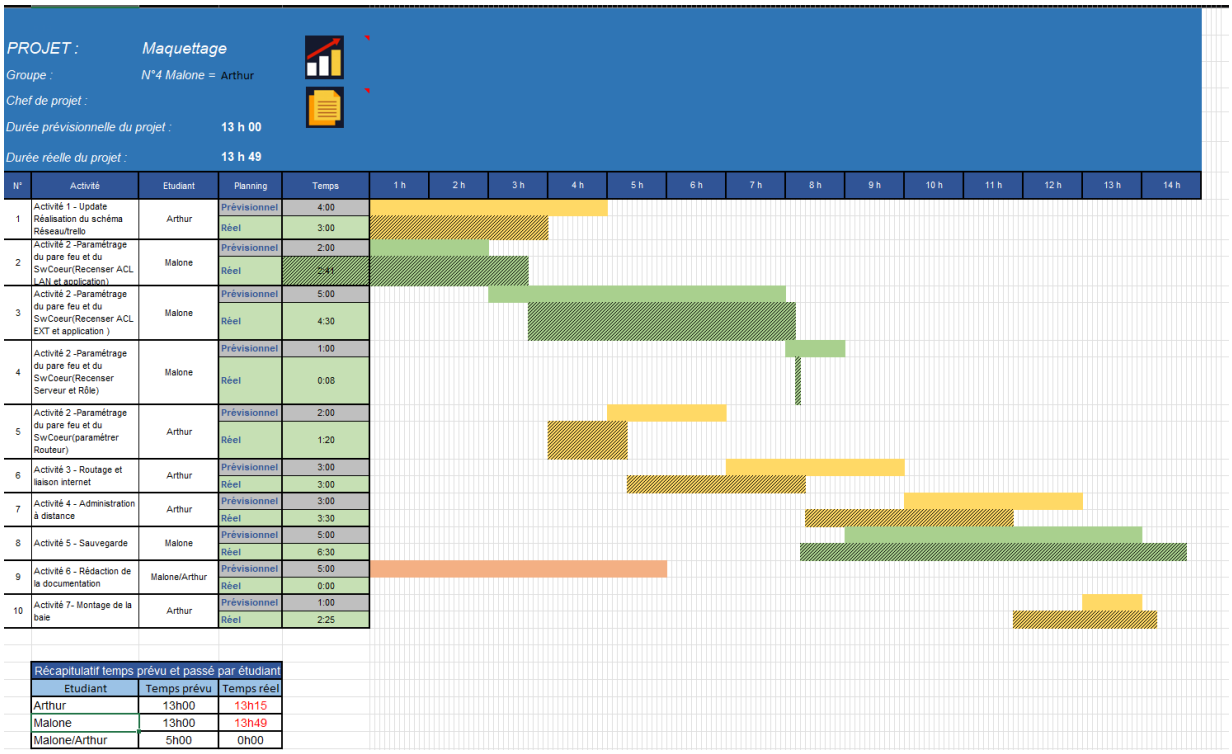
3. Plan de travail

-ACT 0 : Réalisation du Gant
- ACT 1.1 : Réalisation du Trello
- ACT 1.2 : Update Schéma Réseau
- ACT 1.3 : Recenser les nouveaux équipements et leurs rôle
- ACT 1.4 : Mise à jours de la Baie
- ACT 2.1 : Recensement des ACL Lan et les Configurer/Appliquer sur le SW Cœur
- ACT 2.2 : Recenser les ACL Externe au LAN qui seront appliqués sur le Pare feu
- ACT 2.3 : Routage et liaison Internet
- ACT 3 : Paramétrage du Pare Feu
- ACT 4 : Administration à Distance
- ACT 5 : Mise en place de la sauvegarde TFTP pour tous les équipements réseaux.

4. Réalisation

- Activité 0 : Réalisation du GANT

Créer un Gant et organiser nos tâches :



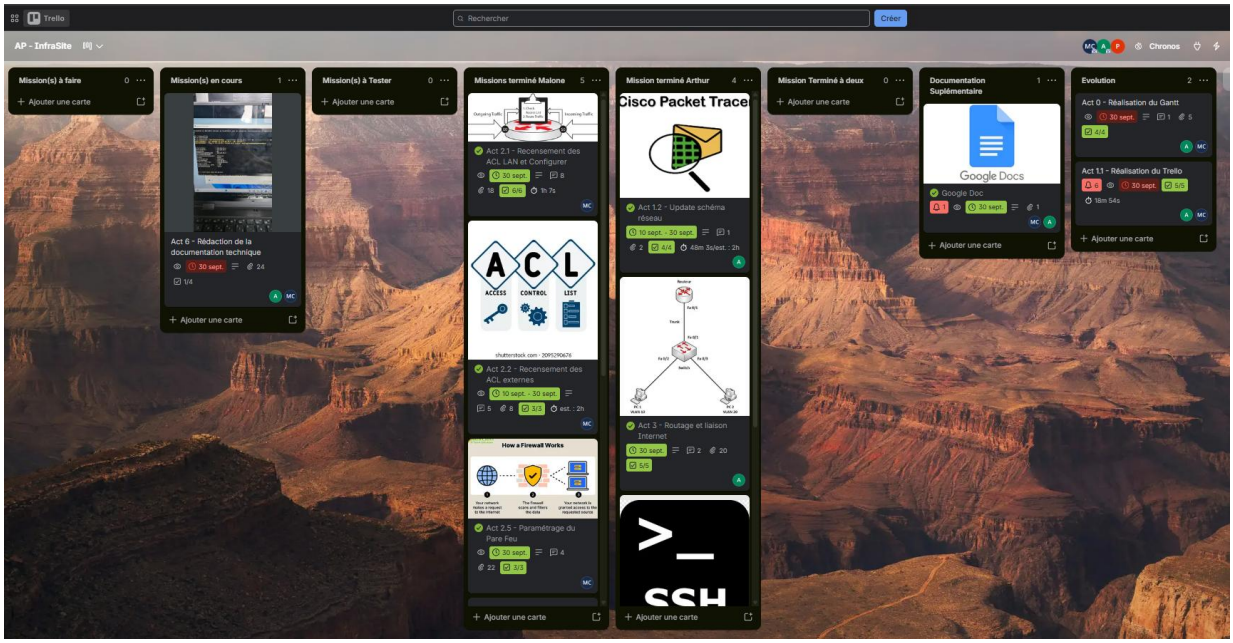
PROJET : Maquettage
Groupe : N°4 Malone = Arthur
Chef de projet :
Durée prévisionnelle du projet : 13 h 00
Durée réelle du projet : 13 h 49

N°	Activité	Etudiant	Planning	Temps
1	Activité 1 - Update Réalisation du schéma Réseau/trello	Arthur	Prévisionnel	4:00
			Réel	3:00
2	Activité 2 -Paramétrage du pare feu et du SwCoeur(Recenser ACL LAN et application)	Malone	Prévisionnel	2:00
			Réel	2:41
3	Activité 2 -Paramétrage du pare feu et du SwCoeur(Recenser ACL EXT et application)	Malone	Prévisionnel	5:00
			Réel	4:30
4	Activité 2 -Paramétrage du pare feu et du SwCoeur(Recenser Serveur et Rôle)	Malone	Prévisionnel	1:00
			Réel	0:08
5	Activité 2 -Paramétrage du pare feu et du SwCoeur(paramétrer Routeur)	Arthur	Prévisionnel	2:00
			Réel	1:20
6	Activité 3 - Routage et liaison internet	Arthur	Prévisionnel	3:00
			Réel	3:00
7	Activité 4 - Administration à distance	Arthur	Prévisionnel	3:00
			Réel	3:30
8	Activité 5 - Sauvegarde	Malone	Prévisionnel	5:00
			Réel	6:30
9	Activité 6 - Rédaction de la documentation	Malone/Arthur	Prévisionnel	5:00
			Réel	0:00
10	Activité 7- Montage de la baie	Arthur	Prévisionnel	1:00
			Réel	2:25

Récapitulatif temps prévu et passé par étudiant		
Etudiant	Temps prévu	Temps réel
Arthur	13h00	13h15
Malone	13h00	13h49
Malone/Arthur	5h00	0h00

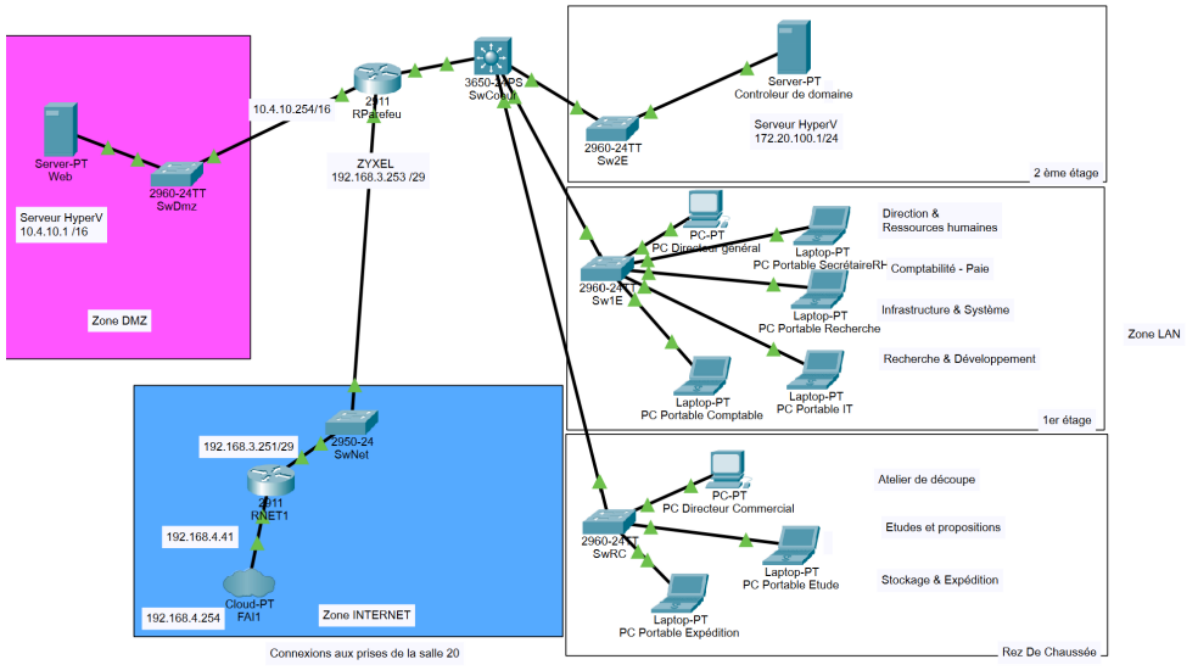
- *Activité 01.1 : Réalisation du Trello*

Ensuite Mise en place du Trello et organisations de nos tâches :

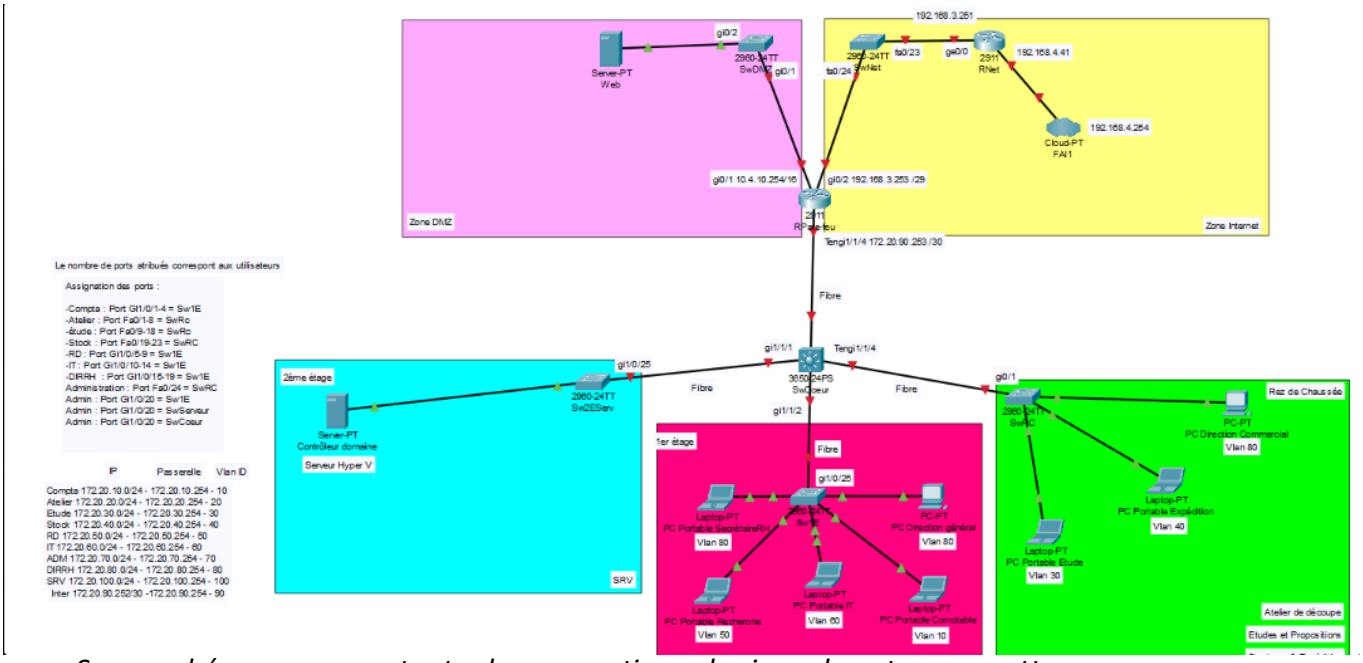


- Activité 1.2 : Réalisation du Schéma Réseau :

Faire un prévisionnel de l'adressage IP que nous allons faire et mettre en place et l'illustrer sur un schéma pour nous aider, sachant qu'un schéma nous ais déjà donné dans la lettre de mission soit :



Après avoir fais un debriefing nous avons fais un adressage et une update du schéma réseau qui au final correspond à ceci :



Sur ce schéma vous avez toutes les connections physique de notre maquette.

- Activité 1.3 : Recenser les nouveaux équipements et leurs rôle

Nous avons des nouveaux équipemenst et avant de les installer dans la Baie, pourquoi ne pas savoir à quoi ils servent ? Pour cela nous avons ces nouveaux équipements avec leur utilité :

- Un serveur WEB : Un serveur WEB qui accueillera des pages nécessaires à l'entreprise Presbois

- Un serveur Active Directory : Permettant la gestion des utilisateurs et des ordinateurs connectés à son domaine, et la gestion des utilisateurs de nos différents services.

- Un Pare Feu : Permettant la gestion des autorisations et des interdictions d'accès de notre infrastructure internet et DMZ servant donc de barrière de sécurité

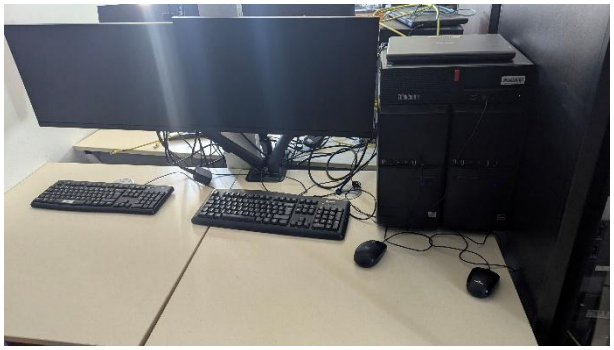
- Un Switch DMZ : Un switch isolé des autres accueillant le serveur Web et un serveur de base de donnée permettant la protection des données internet en cas de piratage , personne n'a accès au Switch Directement hors IT.

- Un Switch pour Internet , Il sert à augmenter le nombre de port ethernet soit de connecter plusieurs appareils si on ne veut pas passer depuis le LAN.

- Un Routeur : Permet de faire la liaison entre le switch et internet s'occupant du routage, du nat etc etc…

- Activité 1.4 : Mise à jours de la Baie

Maintenant que nous avons recenser les équipements et que nous avons notre schéma réseau , nous pouvons l'installer dans la Baie qui a été préalablement monter dans l'AP 0.0 , notre baie ressemble à ça :





- Activité 2.1 : Recenser les ACL Lan et les Configurer / Appliquées sur le SW Cœur :

Nous devons maintenant recenser les Access-lists qui seront mis sur le LAN soit configurer depuis le SwCoeur , dans notre cas nous avons 2 Grandes Access-list hors routage dynamiques soit pour les utilisateurs et l'IT voici l'ordre choisi pour les ACL et les Access-list dédié au LAN :

ACCESS-LIST attribué au LAN donc à paramétrer sur le Switch Cœur :

- Tous les Vlan doivent pouvoir accéder au serveur Active Directory/Serveur Web / internet
- Tous les vlan ne doivent pas communiquer entre eux
- Seul le service IT aura accès au TFTP
- Le service IT devra lui seul pouvoir depuis le LAN et l'extérieur administrer de manière sécurisée l'ensemble des éléments d'interconnexion qui devront bénéficier d'un contrôle d'accès et de messages d'avertissement

Ordre Choisis pour chacune des Access List :

1- Seul le service IT aura accès au TFTP
2- Tous les Vlan doivent pouvoir accéder au serveur Active Directory/Serveur Web
3- Tous les vlan ne doivent pas communiquer entre eux
4- Tous les vlan doivent pour avoir accès à internet
5- Le service IT devra lui seul pouvoir depuis le LAN et l'extérieur administrer de manière sécurisée l'ensemble des éléments d'interconnexion qui devront bénéficier d'un contrôle d'accès et de messages d'avertissement

Et voici désormais l'access-list pour les utilisateurs de n'importe quelle vlan autre que le 60 soit ACLVLANLAN :

Ip access-list extended ACL-VLANLAN

Pour le TFTP :

deny udp any 172.20.100.0 0.0.0.255 eq 69
Test : depuis n'importe qu'elle vlan hors vlan 60 / 70 faire un tftp sur le serveur tftp

Accès au serveur Active Directory :

permit ip any host 172.20.100.2 s
Test : Faire un Ping.

Pour l'accès au vlan serveur en général :

Permit ip any 172.20.100.0 0.0.0.255
Test : Faire un ping sur le vlan serveur

Accès au server Web :

Permit tcp any host 10.4.10.1 eq 80
Permit tcp any host 10.4.10.1 eq 443
Test : accéder à sa page Web

Pour l'accès au vlan serveur en général :

Permit ip any 172.20.100.0 0.0.0.255
Test : Faire un ping sur le vlan serveur

Pour la communication entre eux :

Deny ip any 172.20.0.0 0.0.255.255
Test : tenter de ping les différent vlan , ils ne doivent pas passer.

Pour internet (à la fin) :

Permit ip any any
Test : faire un ping vers internet et le tracert doit s'arrêter après le pare feu si acl pare feu non faite.

Et ensuite nous faisons l'access-list pour l'IT qui a globalement accès à tout soit :

Ensuite nous nous occupons du VLAN 60 soit l'IT pour l'accès TFTP :

ip access-list extended ACLVLANIT
(Tout ce qui est TFTP , Inter-Vlan , Internet)

permit ip any any
test : faire un TFTP depuis l'IT , ping etc)

Faire du SSH :
ip access-list standard PRESBOIS
permit 172.20.60.0 0.0.0.255

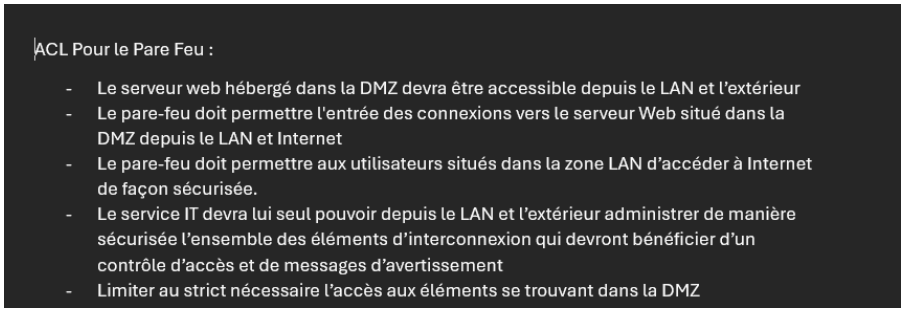
Puis sur la line vty de chacun des équipements :

- Access class PRESBOIS in

Pour les tests veuillez-vous référer au rapport de Test.

- Activité 2.2 : Recenser les ACL Externe au Lan qui seront appliquées sur le Pare Feu :

Idem que pour la 2.1 , nous faisons un recensement des ACL pour le Pare feu sous forme de tableau fidèle à l'interface voici les ACL pour le Pare Feu :



Name	*From*	*TO*	*Ipv4 Source*	*Ipv4 destination*	*Service*	*Device*	*User*	*Schedule*	*Action*	*Log*
SSHEXterne	*LAN1*	*any*	*172.20.60.0*	*any*	*SSH*	*any*	*any*	*none*	*allow*	*No*
SSHEXTERNE1	*WAN*	*any*	*172.20.60.0*	*any*	*SSH*	*any*	*any*	*none*	*allow*	*No*
TFTPWAN	*WAN*	*LAN1*	*172.20.60.0*	*172.20.100.4*	*TFTP*	*any*	*any*	*none*	*allow*	*no*
SSHDENY	*WAN*	*any*	*any*	*any*	*any*	*any*	*any*	*none*	*deny*	*no*
TFTP	*DMZ*	*any*	*any*	*172.20.100.4*	*TFTP*	*any*	*any*	*any*	*allow*	*no*
WanToWeb	*WAN*	*any*	*any*	*any*	*HTTPS*	*any*	*any*	*any*	*allow*	*no*
WanToWeb2	*WAN*	*any*	*any*	*10.4.10.2*	*HTTP*	*any*	*any*	*any*	*allow*	*no*
WantoWeb3	*WNA*	*any*	*any*	*10.4.10.2*	*PING*	*any*	*any*	*any*	*allow*	*no*
WebToLan	*LAN1*	*any*	*any*	*10.4.10.2*	*Mesure(http/S/Ping)*	*any*	*any*	*any*	*allow*	*no*
LanVersInternet	*LAN1*	*any*	*any*	*any*	*Mesure2(DNS-TCP/UDP http/https*	*any*	*any*	*any*	*allow*	*no*
DENYDMZ	*any*	*DMZ*	*any*	*10.4.10.253*	*any*	*any*	*any*	*any*	*deny*	*no*

- Activité 2.3 : Routage et Liaison Internet

Nous allons commencer par Le routage lié au Routeur et au Switch Cœur qui grâce au Protocole RIP leur permettent de faire des routes automatiquement et donc éviter les «ip route » mais si nous allons quand même en faire une seule dans notre cas , soit sur le SwCoeur nous allons mettre ces commandes :

Vous allez en Configure Terminal :

- Router Rip
- Version 2
- network 172.20.0.0
- no auto-summary(permettant de conserver le masque exact d'un sous réseau configuré)

Puis nous allons aller sur le routeur et nous allons mettre ces commandes :

- Router rip
- Version 2
-Network 192.168.4.0
- No auto-summary

Maintenant que le routage est effectué nous allons effectué un nat dynamique qui permettra à notre Lan Privé d'accéder à Internet en utiliser un groupe d'adresses publiques soit nous allons aller sur le routeur et nous allons mettre ces commandes :

Ip nat pool NAT-POOL2 192.168.4.41 192.168.4.49 netmask 255.255.255.224
Access-list 1 permit 172.20.0.0 0.0.255.255
Access-list 1 permit 10.4.10.0 0.0.255.255
Access-list 1 permit 192.168.4.0 0.0.255.255
Ip nat inside source list 1 pool NAT-POOL2 overload

Puis nous allons mettre le « inside » et « outside »

int gi0/1
ip nat inside
int gi0/0
ip nat outside

Puis vous allez faire du nat statique pour qu'un poste extérieur puissent ping votre serveur web

sur le routeur vous allez tapez la commande suivante ip nat source static 10.4.10.10 (hyperviseur du serveur Web) 192.168.4.42 puis quand vous tenterez de ping le serveur web depuis un branchement extérieur ça marchera.

- Activité 3 : Paramétrage du Pare Feu

L'objectif et de paramétrer le pare feu pour que nous puissions contacter ne SwNet / DMZ / Internet en utilisant donc les ACL Externe , premièrement nous allons configurer les Interface du Pare Feu

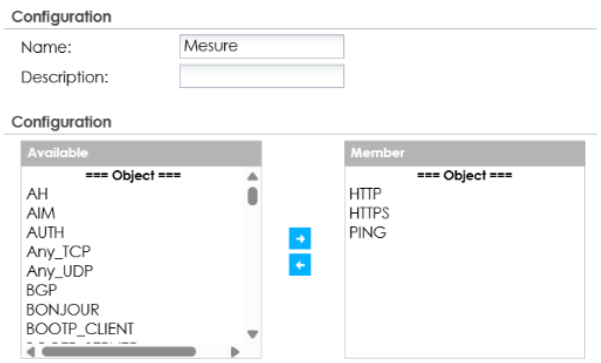
#	Sta...	Name	Description	IP Address	Mask
1		sfp		STATIC -- 172.20.90.253	255.255.255.0
2		wan1		STATIC -- 192.168.3.253	255.255.255.0
3		wan2		DHCP -- 0.0.0.0	0.0.0.0
4		lan1		STATIC -- 192.168.1.1	255.255.255.0
5		lan2		STATIC -- 192.168.2.1	255.255.255.0
6		dmz		STATIC -- 10.4.10.254	255.255.255.0
7		opt		STATIC -- 0.0.0.0	0.0.0.0
8		reserved		STATIC -- 0.0.0.0	0.0.0.0

La Catégorie SFP , nous allons mettre l'adresse 172.20.90.253 conformément au schéma réseau.

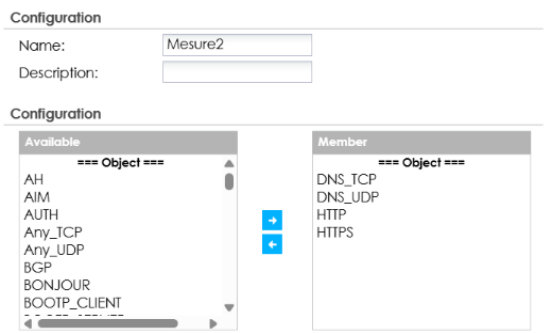
Ensuite nous allons aller dans l'interface du Pare Feu dans Configuration -> Interface là ou nous étions juste avant et en descendant nous actions le « Router Rip » et « RIP V2 ».
Ensuite nous allons dans la console du Pare feu et nous allons taper ces commandes :

Router> enable
Router# Configure Terminal
Router(config) : router rip
Router(config-router) : network sfp
Router(config-router) : network dmz
Router(config-router) : network wan

Ensuite nous allons créer des groupes pour faciliter la création des ACL faire des Groupes de Service soit pour le Serveur web vous allez dans Configuration -> Object -> Address/Geo Ip -> Adress Group puis (Le ping n'est pas demandé mais c'est pour tester):



Et pour Internet créer ce Groupe :



Ensuite nous allons mettre des adresse statiques pour le serveur web par exemple et des adresses réseaux pour le ssh par exemple :

Add Edit Remove References

#	Name	Type	IPv4 Address	Reference
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-10.4.10.0/24	1
2	IP6to4-Relay	HOST	192.88.99.1	0
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24	0
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	0
5	RFC1918_1	SUBNET	10.0.0.0/8	1
6	RFC1918_2	SUBNET	172.16.0.0/12	1
7	RFC1918_3	SUBNET	192.168.0.0/16	1
8	Reseau-SSH-Admin	SUBNET	172.20.60.0/24	2
9	SWDMZADDRESS	HOST	10.4.10.253	0
10	TFTP	HOST	172.20.100.4	2
11	Web	HOST	10.4.10.2	3

Après cela nous pouvons depuis le Pare feu ping le switch DMZ , SwNet

Ensuite nous allons faire les règles de Pare Feu et pour cela vous aller allez dans Configuration -> Security Policy -> Policy Control et vous allez y mettre ces règles préalablement faites :

Pri...	St...	Name	From	To	IPv4 Source	IPv4 Desti...	Service	Device	User	Schedule	Ac...	Log	Profile
1		LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	any	none	all...	no	
2		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	any	none	all...	no	
3		SSHEXTERNE	any	any (Excl...	Reseau-...	any	SSH	any	any	none	all...	no	
4		SSHEXTERNE1	WAN	any (Excl...	Reseau-...	any	SSH	any	any	none	all...	no	
5		TFTPWAN	WAN	LAN1	any	TFTP	TFTP	any	any	none	all...	no	
6		SSHDENY	WAN	any (Excl...	any	any	any	any	any	none	de...	no	
7		TFTP	DMZ	any (Excl...	any	TFTP	TFTP	any	any	none	all...	no	
8		WantoWeb	WAN	any (Excl...	any	any	HTTP	any	any	none	all...	no	
9		Wantoweb2	WAN	any (Excl...	any	Web	HTTPS	any	any	none	all...	no	
10		WantoWeb3	WAN	any (Excl...	any	Web	PING	any	any	none	all...	no	
11		WebtoLan	LAN1	any (Excl...	any	Web	Mesure	any	any	none	all...	no	
12		LanversInternet	LAN1	any (Excl...	any	any	Mesure2	any	any	none	all...	no	
13		DENYDMZ	any	DMZ	any	DMZ_SU...	any	any	any	none	de...	no	

Nous avons fini le paramétrage du Pare Feu.

- Activité 4 : Administration à Distance

Nous avons donc la règle de base pour tous les équipements réseau :

- Le SSH sera à activer sur tous les équipements administrables seulement depuis le VLAN IT
-Le service IT devra lui seul pouvoir depuis le LAN et l'extérieur administrer de manière sécurisée l'ensemble des éléments d'interconnexion qui devront bénéficier d'un contrôle d'accès et de messages d'avertissement.

Soit quand nous parlons de tous les équipements : Routeur , Pare-Feu , Switch. Pour mettre en place le SSH nous allons utiliser un câble console et nous allons nous connectés à chaque équipement grâce à Putty ou nous allons configurer le SSH.

Sur Chaque équipement nous allons donc :

- Nous connecter en console
- Création d'une bannière pour la connexion
- MDP SSH ainsi qu'un nombre de tentative
-Sauvegarde de la Configuration

Donc nous allons mettre ces commandes pour chaque équipement :

Enable

Configure terminal
- banner motd #
-----Nouvelle Session SSH-----#

- Hostname PRESBOIS
- Ip domain-name PRESBOIS.local
- Crypto key generate rsa modulus 2048
- Ip ssh version 2
- username admin privilege 15 secret MonMotDePasse
- Enable secret MotDePasse
- Service password-encryption
- Line vty 0 15
- Login local
- exec-timeout 30 0
- ip ssh authentication-retries 3
- Transport input ssh

End
Write memory

- Activité 5 : Sauvegarde TFTP sur tous les équipements

Premièrement nous devons faire un Serveur TFTP permettant d'accueillir toutes les sauvegardes des switch et des équipements du lan / WAN / DMZ de façon récurrente , tous les mardi à 17h30 , tous les jeudi à 17h30 et tous les vendredis à 12h30. De base faut que les switch aient une adresse IP ce qui a été fait avant pour le SSH et une passerelle. Ensuite sur le serveur TFTP qui sera en 172.20.100.4 et en Ubuntu 26.04 nous allons taper ces commandes :

sudo apt update
sudo apt install tftpd-hpa tftp -y

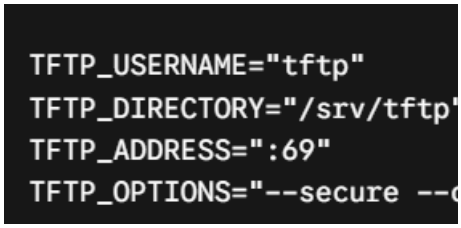
Pour installer les paquets TFTP , Puis nous allons créer le dossier d'accueil des sauvegardes soit :

sudo mkdir -p /srv/tftp (Création du dossier)

Puis nous allons configurer le service TFTP :

sudo nano /etc/default/tftpd-hpa

Nous tombons sur ceci :



Et nous allons rajouter après le « --secure » un « --create »

Puis nous redemarrons le service :

sudo systemctl restart tftpd-hpa

Ensuite nous tentons une sauvegarde manuelle soit les commandes suivantes :

Copy running-config tftp
address : 172.20.100.4
nom de la sauvegarde : ce que vous voulez

Ensuite nous allons configurer l'automatisme des sauvegarde soit :

kron policy-list SAUVEGARDE
cli write
cli copy running-config tftp:// 172.20.100.4/nom.cfg

Puis nous mettons les occurrence :

kron occurrence SAUVEGARDEM at 17:30 Tue recurring

policy-list SAUVEGARDE

exit
kron occurrence SAUVEGARDEJ at 17:30 Thu recurring

policy-list SAUVEGARDE

exit

kron occurrence SAUVEGARDEV at 12:30 Fri recurring

policy-list SAUVEGARDE

exit

et vous avez configure votre sauvegarde automatique , si votre switch n'est pas à l'heure ou la bonne année :

show clock , si c'est c'est le cas :

Clock set 00 :00 :00 jours moi année.

Fin de la sauvegarde des appareils.