INFRASTRUCTURE E6🌐

Contexte :
Schéma Infrastructure :
Organigramme :
Configuration Réseau :
- 🔒 Mots de passe de connexion sur les machines :
- 🔒 Mots de passe de connexion sur les interfaces web & BDD :
- Réseau LAN_SRV :
  - 💻 Configurations Serveurs :
- Réseau LAN_CLT :
  - 💻 Configurations Clients :
- Réseau DMZ :
  - 💻Configurations Serveurs :
  - 📧Adresses mails :
- Les PfSense :
  - 💻Configuration des routeurs :
  - 🔥Les Règles (ACL) :
- Les Switch Physique :
  - 💻 **Configuration Switch :**

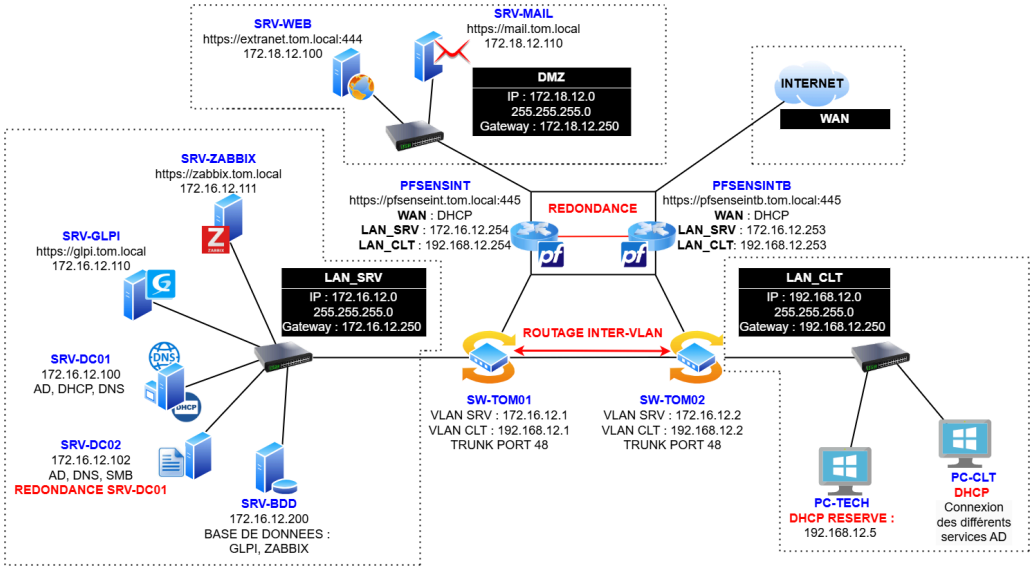
Contexte :

L'entreprise TOM_COMPANY, une entreprise de sacs à main de luxe, a décidé de s'implanter dans le Département du 49 à Angers. Il a fallu créer toute l'infrastructure de cette entreprise avec une condition : garantir la haute disponibilité sur les équipements les plus critiques.

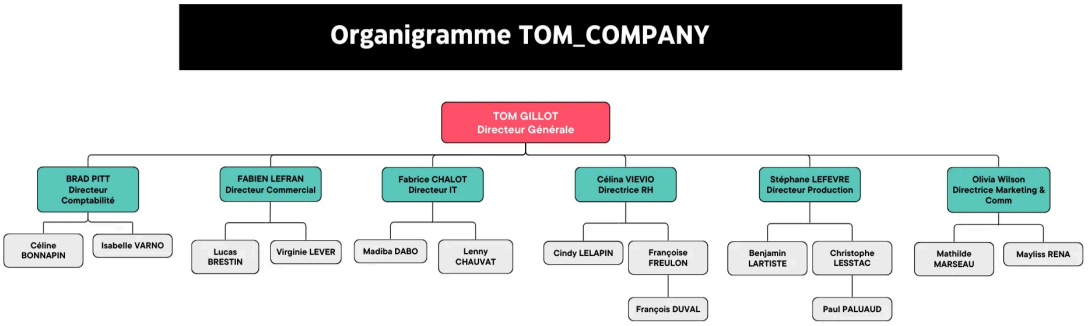
J'ai donc créé un serveur Active Directory avec à l'intérieur le découpage des services (Production, RG, IT, Direction, Communication, Commercial, Comptabilité).

Elle souhaitait avoir les services de messagerie, extranet, qui sont accessibles depuis l'extérieur mais aussi un logiciel de ticketing et de gestion de parc informatique. En plus, il voulait superviser les équipements qui se trouvent dans le réseau serveur plus nos deux switch physiques.

Schéma Infrastructure :



Organigramme :



Configuration Réseau :

🔒 Mots de passe de connexion sur les machines :

Serveurs ou Utilisateurs	Nom d'utilisateur	Mot de passe
SRV-DC01	Administrateur	r5F0p&0m
SRV-DC02	tom.gillot\Administrateur	r5F0p&0m
SRV-GLPI	tom ——————————— root	tom ——————————— root
SRV-ZABBIX	tom ——————————— root	tom ——————————— root
SRV-BDD	tom ——————————— root	tom ——————————— tom

Serveurs ou Utilisateurs	Nom d'utilisateur	Mot de passe
SRV-MAIL	tom root	tom root
SRV-WEB	tom root	tom root
Utilisateurs AD	p.nom	P@ssw0rd
Compte Admin (Windows)	nompc\admin	r5F0p&0m
Switch (SSH)	tom	tom

p.nom = première lettre du prénom.nom de famille

🔒 Mots de passe de connexion sur les interfaces web & BDD :

Serveurs ou Utilisateurs	Nom d'utilisateur	Mot de passe
https://pfsenseint.tom.local:445 https://pfsenseintb.tom.local:445	admin	Jinfot19*
https://glpi.tom.local	admin support	@dmin_company supp0rt_tom
https://zabbix.tom.local	Admin	Z@bbix_company
https://mail.tom.local	postmaster@tom.local p.nom@tom.local	r5F0p&0m P@ssw0rd
serveur BDD (MySQL)	root	password

p.nom = première lettre du prénom.nom de famille

Réseau LAN_SRV :

📌 Réseau Virtuel sur le VMnet 9

💻 Configurations Serveurs :

Nom du Serveur	Adresse IP	Masque (CIDR)	Service	Les +	Accès Web
SRV-DC01	172.16.12.100	24	AD, DNS, DHCP, SNMP	Redondance AD, DNS & DHCP sur SRV-DC02	NON
SRV-DC02	172.16.12.102	24	AD, DNS, SMB, IIS, ADCS, SNMP, HTTP/HTTPS	Redondance AD, DNS & DHCP du SRV-DC01	https://srv-dc02/certsrv
SRV-GLPI	172.16.12.110	24	HTTP/HTTPS, SNMP	Outil de ticketing et de parc Informatique	https://glpi.tom.local
SRV-ZABBIX	172.16.12.111	24	HTTP/HTTPS, SNMP	Outil de supervision des équipements du LAN_SRV	https://zabbix.tom.local
SRV-BDD	172.16.12.200	24	Maria DB, MySQL, SNMP	Stockage des Bases de Données GLPI et Zabbix	NON

ℹ️ L'accès à distance sur les serveurs, que ce soit en SSH ou en bureau à distance, ne peut se faire que depuis le PC-TECH qui se trouve dans le LAN_CLT. Seul ce PC a les droits de prise à distance sur l'ensemble des serveurs.

Réseau LAN_CLT :

📌 Réseau Virtuel sur le VMnet 10

💻 Configurations Clients :

Nom du Serveur	Adresse IP	Masque (CIDR)	Les +
PC-TECH	**DHCP RESERVER** → 192.168.12.5	24	Accès sur tout les serveurs en SSH, RDP, WEB
PC-CLT	172.16.12.102	24	Accès WEB sur les serveurs (GLPI, MAIL, WEB)

ℹ️ Les utilisateurs de l'Active Directory se connectent avec les identifiants de connexion sur le PC-CLT. Seuls les techniciens se connectent sur le PC-TECH car sur celui-ci, nous pouvons prendre en main à distance en RDP et SSH sur l'ensemble des serveurs de l'AD (LAN_SRV & DMZ).

Réseau DMZ :

📌 Réseau Virtuel sur le VMnet 11

💻Configurations Serveurs :

Nom du Serveur	Adresse IP	Masque (CIDR)	Service	Les +	Accès Web
SRV-MAIL	172.18.12.110	24	IMAP(S),POP3(S), SMTP(S), HTTP/HTTPS	Service de MAIL	https://mail.tom.local
SRV-WEB	172.18.12.100	24	HTTP/HTTPS	Extranet de l'entreprise	https://extranet.tom.local:444

📧Adresses mails :

Nom Prénom	Adresses Mails	Mot de passe
postmaster	postmaster@tom.local	r5F0p&0m
GLPI	glpi@tom.local	P@ssw0rd
support_GLPI	support@tom.local	P@ssw0rd
Zabbix	zabbix@tom.local	P@ssw0rd
Benjamin LARTISTE	b.lartiste@tom.local	P@ssw0rd
Brad PITT	b.pitt@tom.local	P@ssw0rd
Célina VIEVO	c.vievo@tom.local	P@ssw0rd
Céline BONNAPIN	c.bonnapin@tom.local	P@ssw0rd
Christophe LESSTAC	c.lesstac@tom.local	P@ssw0rd
Cindy LELAPIN	c.lelapin@tom.local	P@ssw0rd
Fabien LEFRANC	f.lefranc@tom.local	P@ssw0rd
Fabrice CHALOT	f.chalot@tom.local	P@ssw0rd

Nom Prénom	Adresses Mails	Mot de passe
François DUVAL	f.delaval@tom.local	P@ssw0rd
Françoise FREULON	f.freulon@tom.local	P@ssw0rd
Isabelle VARNO	i.varno@tom.local	P@ssw0rd
Lenny CHAUVAT	l.chauvat@tom.local	P@ssw0rd
Lucas BRESTIN	l.brestin@tom.local	P@ssw0rd
Madiba DABO	m.dabo@tom.local	P@ssw0rd
Mathilde MARSEAU	m.marseau@tom.local	P@ssw0rd
Mayliss RENA	m.rena@tom.local	P@ssw0rd
Olivia Wilson	o.wilson@tom.local	P@ssw0rd
Paul PALUAUD	p.paluaud@tom.local	P@ssw0rd
Stéphane LEFEVRE	s.lefevre@tom.local	P@ssw0rd
Tom GILLOT	t.gillot@tom.local	P@ssw0rd
Virginie LEVER	v.lever@tom.local	P@ssw0rd

Les PfSense :

📌 Mes deux PfSense sont accessibles sur internet avec leur adresse IP WAN et sur le port 445 (idem SMB). J'ai choisi ce port car, lorsque j'ai fait mes redirections NAT, j'ai mis une chronologie afin de ne pas être perdu. Mon serveur mail est accessible depuis l'extérieur sur le port 443, mon serveur web est accessible depuis l'extérieur sur le port 444 et mes PfSense sont aussi accessibles depuis l'extérieur sur le port 445.

💻Configuration des routeurs :

Nom du Serveur	Adresse IP	Masque (CIDR)	Service	Les +	Accès Web
Pfsenseint	WAN : DHCP LAN_SRV : 172.16.12.254 LAN_CLT : 192.168.12.254 DMZ : 172.16.12.254	24	CARP, Relay DHCP, SNMP, HTTP/HTTPS	Redondance avec le Pfsenseintb	https://pfsenseint.tom.local:445
Pfsenseintb	WAN : DHCP LAN_SRV : 172.16.12.253 LAN_CLT : 192.168.12.253 DMZ : 172.16.12.253	24	CARP, Relay DHCP, SNMP, HTTP/HTTPS	Redondance avec le Pfsenseint	https://pfsenseintb.tom.local:445

ℹ️ Pour que les serveurs et les clients sachent quelle passerelle ils doivent entrer dans leur configuration, j'ai créé des IP virtuelles qui vont permettre de faire la passerelle sur les deux PfSense. Si un des deux PfSense tombe, l'autre prendra le relais, les serveurs et clients n'auront pas besoin de changer l'adresse IP de leur passerelle.

J'ai donc créé des IP virtuelles :

- LAN_SRV : 172.16.12.250
- LAN_CLT : 192.168.12.250
- DMZ : 172.18.12.250

Les Règles (ACL) :

LAN_SRV :

Règles (Faire glisser pour changer l'ordre)

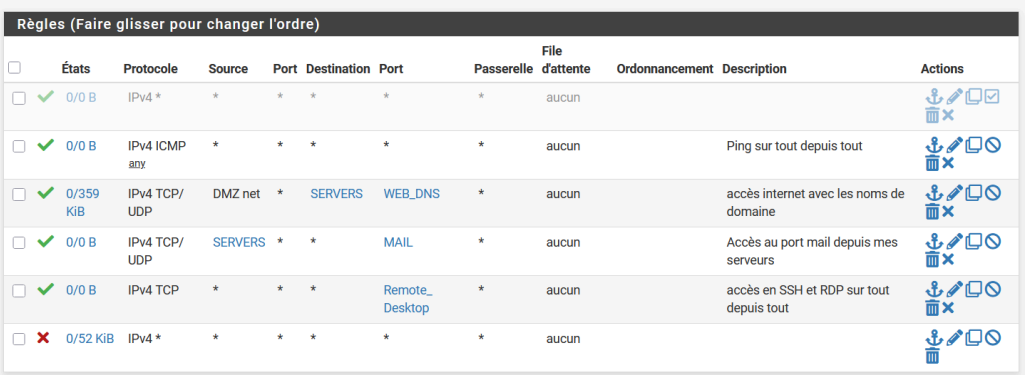
	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	0/0 B	*	*	*	LAN_SERVEUR Address	445 80	*	*		Règle anti-blocage	
	0/0 B	IPv4 TCP/ UDP	*	*	*	*	*	aucun			
	0/72 KiB	IPv4 ICMP any	*	*	*	*	*	aucun		Ping sur tout depuis tout	
	0/0 B	IPv4 TCP	LAN_CLIENT net	*	Server_AD	Active_ Directory	*	aucun		Accepter les requêtes AD du LAN client pour les GPO ...	
	6/177.53 MiB	IPv4 TCP/ UDP	SERVERS	*	*	WEB_DNS	*	aucun		Donne l'accès web à tous les serveurs avec les noms de domaine	
	0/0 B	IPv4 TCP/ UDP	*	*	*	Remote_ Desktop	*	aucun		accès en SSH et RDP sur tout depuis tout	
	0/9 KiB	IPv4 TCP/ UDP	SERVERS	*	*	MAIL	*	aucun		Accès au service de mail sur tous les serveurs	
	0/0 B	IPv4 TCP/ UDP	Zabbix	*	Hotes_SNMP	SNMP	*	aucun		Récupère les informations en SNMP des serveurs	
	0/0 B	IPv4 PFSYNC	*	*	Ce pare-feu	*	*	aucun		Autoriser pfsync pour Redondance	
	0/0 B	IPv4 TCP	*	*	Ce pare-feu	443 (HTTPS)	*	aucun		Autoriser XMLRPC pour redondance	
	0/55 KiB	IPv4 TCP/ UDP	*	*	*	*	*	aucun			

LAN_CLT :

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
	0/0 B	IPv4 *	*	*	*	*	*	aucun			
	0/491 B	IPv4 ICMP any	*	*	*	*	*	aucun			
	25/447 KiB	IPv4 TCP/ UDP	LAN_CLIENT net	*	Server_AD	*	*	aucun		Authentification AD sur PC Clients + ajout PC AD + ajout de GPO	
	0/0 B	IPv4 TCP	PC_Tech	*	SERVERS	Remote_ Desktop	*	aucun		Accès à distance en SSH et RDP sur les Serveurs	
	0/0 B	IPv4 TCP	PC_Tech	*	Zabbix	WEB_DNS	*	aucun		Seul le PC Tech a le droit d'aller sur l'interface web de zabbix	
	0/2 KiB	IPv4 TCP/ UDP	LAN_CLIENT net	*	Zabbix	WEB	*	aucun		Les clients n'ont pas accès à l'interface zabbix sauf le PC Tech	
	0/587 KiB	IPv4 TCP/ UDP	LAN_CLIENT net	*	SERVERS	WEB_DNS	*	aucun		Accès aux sites internet interne et externe avec les noms de domaine	
	113/87.07 MiB	IPv4 TCP/ UDP	LAN_CLIENT net	*	*	WEB	*	aucun		Accès web public	
	0/0 B	IPv4 TCP	*	*	*	Remote_ Desktop	*	aucun		accès en SSH et RDP sur tout depuis tout	
	0/8 KiB	IPv4 *	*	*	*	*	*	aucun			

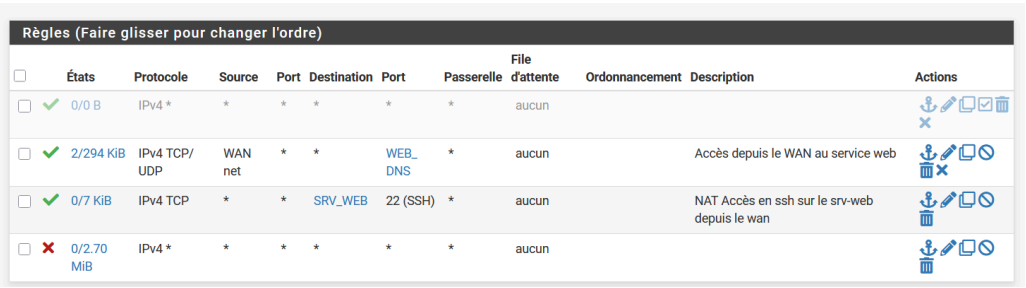
DMZ :



Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓ 0/0 B	IPv4 *	*	*	*	*	*	aucun			
☐	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	aucun		Ping sur tout depuis tout	
☐	✓ 0/359 KiB	IPv4 TCP/UDP	DMZ net	*	SERVERS	WEB_DNS	*	aucun		accès internet avec les noms de domaine	
☐	✓ 0/0 B	IPv4 TCP/UDP	SERVERS	*	*	MAIL	*	aucun		Accès au port mail depuis mes serveurs	
☐	✓ 0/0 B	IPv4 TCP	*	*	*	Remote_Desktop	*	aucun		accès en SSH et RDP sur tout depuis tout	
☐	✗ 0/52 KiB	IPv4 *	*	*	*	*	*	aucun			

WAN :



Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	File d'attente	Ordonnancement	Description	Actions
☐	✓ 0/0 B	IPv4 *	*	*	*	*	*	aucun			
☐	✓ 2/294 KiB	IPv4 TCP/UDP	WAN net	*	*	WEB_DNS	*	aucun		Accès depuis le WAN au service web	
☐	✓ 0/7 KiB	IPv4 TCP	*	*	SRV_WEB	22 (SSH)	*	aucun		NAT Accès en ssh sur le srv-web depuis le wan	
☐	✗ 0/2.70 MiB	IPv4 *	*	*	*	*	*	aucun			

Les Switch Physique :

💻 Configuration Switch :

📌 Les switch sont configurables en SSH depuis un hôte qui se trouve dans le VLAN sur lequel il est connecté via un câble Ethernet. Il suffit d'ouvrir une console d'Administration telle que PuTTY et de renseigner l'adresse IP du VLAN. Le port SSH reste le port par défaut.

Nom du Serveur	VLAN (ID)	Adresse IP	Masque (CIDR)	Ports	Trunk
SW-TOM01	VLAN 10 (LAN_SRV) ———— VLAN 20 (LAN_CLT)	172.16.12.1 ———— 192.168.12.1	24 ———— 24	1 à 10 ————20 à 29	Port 48
SW-TOM02	VLAN 10 (LAN_SRV) ———— VLAN 20 (LAN_CLT)	172.16.12.2 ———— 192.168.12.2	24 ———— 24	1 à 10———— 20 à 29	Port 48