

PROJET CUB
AGENCE
CALIFORNIE



PROJET
CUB

Le projet CUB, mené dans le cadre du BTS SIO, a pour objectif de simuler l'infrastructure complète d'une entreprise. Il vise à mettre en place un réseau sécurisé, intégrant des services essentiels pour assurer un fonctionnement optimal. Pour l'agence Californie, le projet implique le déploiement d'une infrastructure réseau qui garantit une haute disponibilité, une segmentation efficace et la sécurité des flux entre les différentes zones : utilisateurs, administrateurs, serveurs et DMZ.

Ressources matérielles

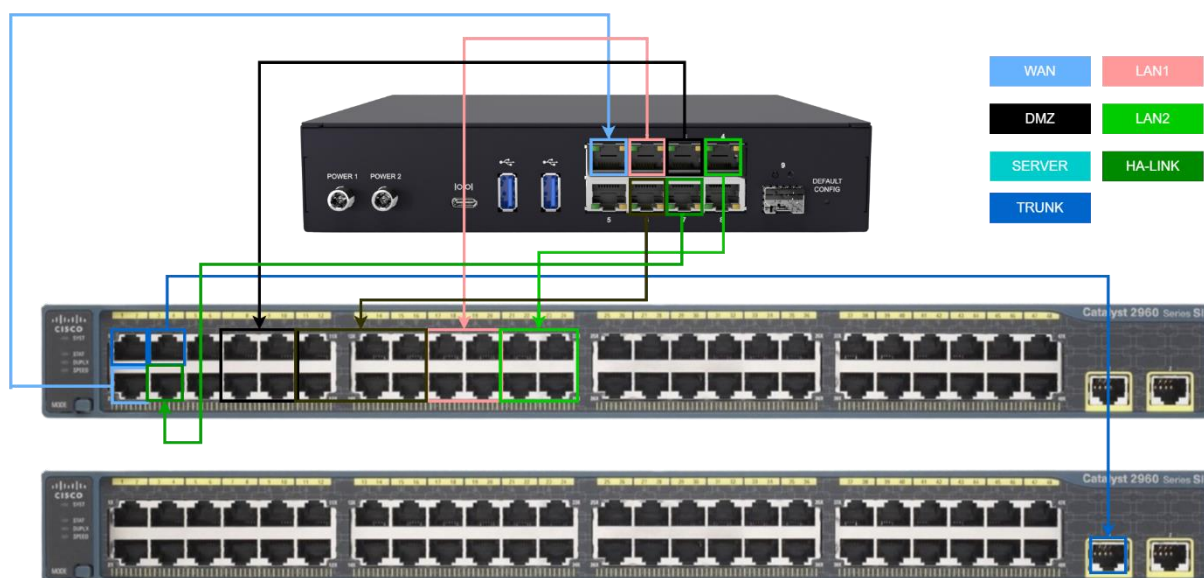
- 1 pare-feu Stormshield SNS-320
- 2 switchs Cisco (SW-L2, SW-L3)
- 1 serveur Proxmox (hyperviseur)
- Postes clients utilisateurs

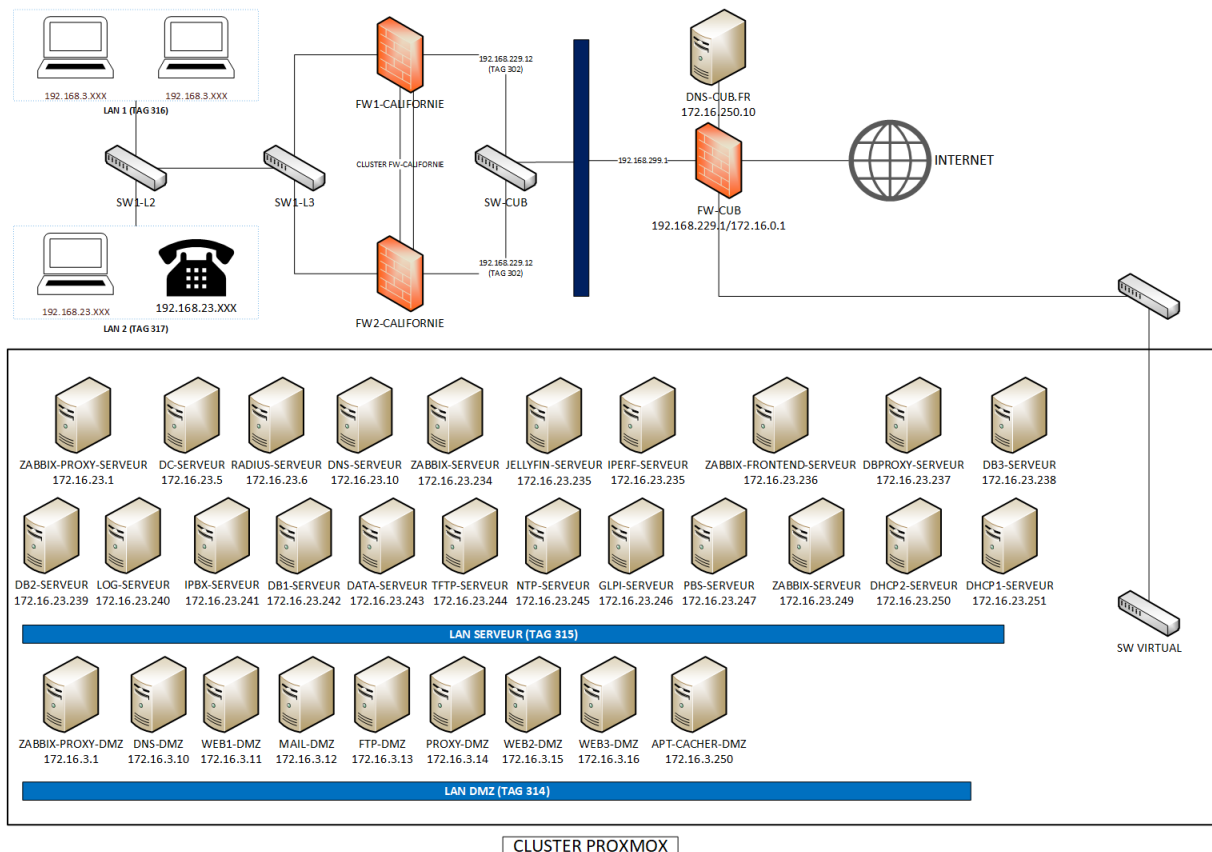
Réseau de l'agence Californie

L'infrastructure de l'agence Californie est divisée en plusieurs réseaux « VLAN » pour séparer les usages DMZ, serveurs, utilisateurs et accès WAN. Chaque VLAN possède un sous-réseau dédié et une interface configurée sur le pare-feu Stormshield.

ID VLAN	RESEAU	IP PARE-FEU
314	DMZ : 172.16.3.0/24	172.16.3.254
315	SERVEUR : 172.16.23.0/24	172.16.23.254
316	LAN 1 : 192.168.3.0/24	192.168.3.254
317	LAN 2 : 192.168.23.0/24	192.168.23.254
134	WIFI	
104	TRANSPORT	

Présentation du schéma physique et logique de l'infrastructure





Services réseau et système de l'agence CALIFORNIE

Infrastructure :

- **Active Directory (AD)** : authentification centralisée des utilisateurs et des machines
- **DNS (Domain Name System)** : résolution des noms interne
- **DHCP (Dynamic Host Configuration Protocol)** : attribution automatique des adresses IP

Supervision / Gestion :

- **Zabbix** : serveur maître qui centralise les données récupérées
- **Zabbix Proxy** : relais de supervision, collecte des données pour un serveur Zabbix maître distant
- **GLPI** : gestion des tickets, suivi d'inventaire et maintenance du parc informatique

Service Web :

- Serveur web 1
- Serveur web 2
- Serveur web 3
- Proxy

Sécurité :

- **Stormshield** : EVA Slave, utilisé pour la haute disponibilité avec le pare-feu physique

ID VLAN	VLAN	SERVICES
314	DMZ	DNS /WEB1/MAIL/FTP/PROXY ZABBIX/WEB2/WEB3 APT-CACHER
315	SERVEUR	DNS/DB PROXY/DB3/DB2/DB1 /GRAYLOG / TFTP/ ZABBIX SERVEUR/ GLPI/NTP/ AD/ DHCP1 / DHCP2/ RADIUS/ DATA
316	LAN 1	Postes utilisateurs
317	LAN 2	Postes utilisateurs
302	WAN	Accès Internet via Stormshield

Configuration du pare-feu Stormshield

Le pare-feu SNS320 est essentiel à la sécurité de l'infrastructure de l'agence. Il impose des règles de filtrage rigoureuses pour gérer les échanges entre les différentes zones du réseau (LAN, DMZ, SERVEURS, WAN). Ces règles assurent la sécurité, la segmentation et le bon fonctionnement des services. Elles sont établies selon les besoins professionnels, le principe de moindre privilège et les recommandations de la CNIL.

Règles de filtrage du pare-feu

Configuration de l'accès à l'application d'administration web. (contient 2 règles, from 1 to 2)									
1				Any	FIREWALL	firewall_srv https			Admin from everywhere
2				Any	firewall_all	Any icmp (Echo request)			Allow Ping from everywhere
Autorisation requête http/https (contient 1 règles, from 3 to 3)									
3				Network_Internals	Internet	http https			Created on 2024-10-25 11:03:05 by admin (172.16.23.5)
DNS (contient 5 règles, from 4 to 8)									
4				DNS-SERVEUR	Internet	dns			Created on 2025-03-18 12:24:12 by admin (172.16.23.5)
5				DNS-DMZ	Internet	dns			Created on 2025-03-18 12:24:12 by admin (172.16.23.5) - Updated on 2025-04-18 10:35:19 by ...
6				DNS-SERVEUR	DNS-DMZ	dns			Created on 2024-11-08 08:13:28 by admin (172.16.23.5)
7				DC-SERVEUR	DNS-SERVEUR	dns			Created on 2025-03-18 09:24:55 by admin (172.16.23.5)
8				Network_LAN1 Network_LAN2 Network_SERVEUR Network_dns1	DC-SERVEUR	dns kerberos ldap ldaps SMB RPC-Endpoint netbios-ns netbios-dgm netbios-ssn ldap-gc ldap-global			Created on 2025-03-18 09:16:25 by admin (172.16.23.5)
SERVEUR WEB (contient 3 règles, from 9 to 11)									
9				Internet	Firewall_WAN	P-PROXY			Crée le 2025-04-18 07:46:30 par admin (192.168.229.132)
10				Internet Interface: WAN	Firewall_WAN PROXY-DMZ	P-PROXY http			Created on 2025-04-18 11:47:20 by admin (192.168.229.132)
11				WEB-DMZ WEB2-DMZ WEB3-DMZ	DBPROXY-SERVEUR	mysql			Created on 2025-03-19 16:09:54 by admin (172.16.23.5)
ADMINISTRATION MSTRC (contient 1 règles, from 12 to 12)									
12				Any Interface: WAN	Firewall_WAN	microsoft-s			Created on 2025-03-18 09:29:50 by admin (172.16.23.5)
VQIP (contient 1 règles, from 13 to 13)									
13				Network_LAN1 Network_LAN2	IPDK-SERVEUR	rip sips			Created on 2025-03-18 10:41:35 by admin (172.16.23.5)
ZABBIX (contient 2 règles, from 14 to 15)									
14				Zabbix-Proxy-DMZ Zabbix-Proxy-SERVEUR	ZABBIX-SERVEUR ZABBIX-SERVEUR2	ZABBIX			Created on 2024-10-23 08:30:30 by admin (172.16.23.5)
15				Zabbix-Proxy-DMZ	DBPROXY-SERVEUR	mysql			Created on 2025-03-24 17:31:56 by admin (172.16.23.5)
TFTP (contient 1 règles, from 16 to 16)									
16				SW1-L3 SW1-L2 FIREWALL	TFTP-SERVEUR	tftp			Created on 2025-03-18 12:48:18 by admin (172.16.23.5)
NTP (contient 2 règles, from 17 to 18)									
17				NTP-SERVEUR	Internet	ntp			Created on 2025-03-18 12:54:11 by admin (172.16.23.5)
18				Network_Internals	NTP-SERVEUR	ntp			Created on 2025-03-18 12:52:44 by admin (172.16.23.5)
GLPI (contient 2 règles, from 19 to 20)									
19				Network_LAN1 Network_LAN2	GLPI-SERVEUR	https http			Created on 2025-03-18 12:58:16 by admin (172.16.23.5)
20				GLPI-SERVEUR	DBPROXY-SERVEUR	mysql			Created on 2025-03-24 17:35:53 by admin (172.16.23.5)
FILES SHARING (contient 1 règles, from 21 to 21)									
21				Network_LAN1 Network_LAN2	DATA-SERVEUR	SMB			Created on 2025-03-18 13:04:01 by admin (172.16.23.5)
SSH (contient 1 règles, from 22 to 22)									
22				Network_SERVEUR	WEB-DMZ WEB2-DMZ WEB3-DMZ	ssh			Created on 2025-03-20 12:51:16 by admin (172.16.23.5)
TFTP Backup (contient 1 règles, from 23 to 23)									
23				FIREWALL	WEBDAV-SERVEUR	HTTP_UPLOAD			TFTPO
Default policy (contient 1 règles, from 24 to 24)									
24				Any	Any	Any			Block all

Règles NAT du pare-feu

	Status	Original traffic (before translation)	Traffic after translation				Protocol	Options	Comments
		Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port	
1		Network_Internals	Internet Interface: WAN	Any	Firewall_WAN	ephemeral	Any		Crée le 2024-01
2		Internet	Firewall_WAN	dns	Any		DNS-DMZ	dns	Crée le 2024-11
3		Any Interface: WAN	Firewall_WAN	microsoft-s	Firewall_SERVEUR	microsoft-s	DC-SERVEUR	microsoft-s	Created on 2023
4		Internet Interface: WAN	Firewall_WAN	P-PROXY	Any		PROXY-DMZ	http	Crée le 2025-04