

Rapport du projet « Refonte Infrastructure Réseaux et Sécurité Sesame »

Préparé par l'équipe technique du Prologic

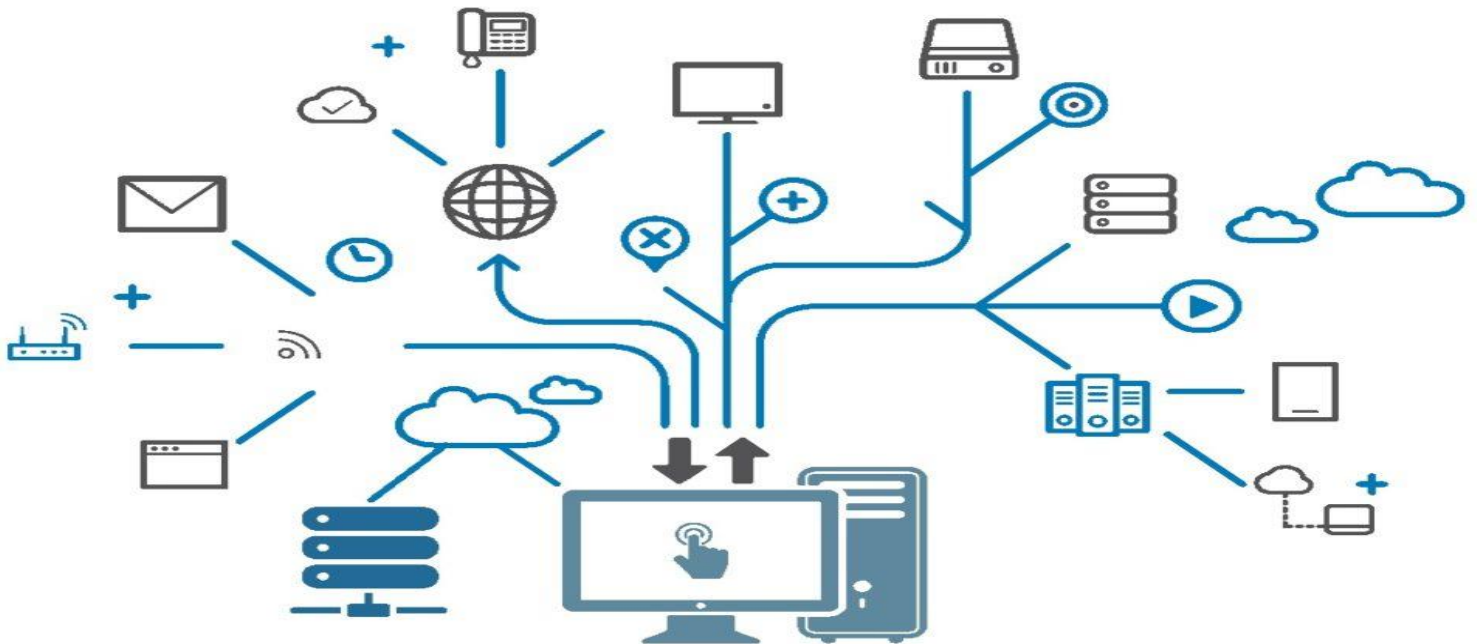


Table des matières

I. Introduction	4
1. Cadre du projet	4
2. Objectif du projet.....	4
3. Liste des tâches	4
4. Equipements acquis.....	5
4.1 Description du switch access Fortiswitch 124F POE.....	5
4.2 Description du FortiAP 231F:	6
4.3 Description du Firewall FortiGate 600E:	6
4.4 FortiAnalyzer:	7
II. High Level Design	8
III. Switch + Controleur	9
1. Configuration des vlans.....	9
2. Configuration initiale	10
IV. Serveur externe.....	11
1. Configuration initiale	12
V. Firewall.....	12
1. Spécifications du Fortigate 600E	13
2. Configuration du service DHCP	13
3. Architecture WAN	13
4. Configuration initiale	14
5. Configuration des interfaces	14
6. Configuration FGT 600E Et Recommandation.....	18
VI. FortiSwitch:	26
VII. Serveur :.....	29
VIII. FortiAnalyzer:	30
Conclusion	33

Liste des tableaux

Tableau 1 : Liste des VLANs du SW partie data	9
Tableau 2 : Liste des VLANs du SW partie serveur.....	9
Tableau 3 : Configuration initiale SW 3com-stack	10
Tableau 4 : Configuration initiale SW access.....	10
Tableau 5 : Configuration initiale du contrôleur	10
Tableau 6 : Les accès WIFI	11
Tableau 7 : Liste des LACP SW-3com.....	11
Tableau 8: Ports du Fortigate 600E.....	13
Tableau 9 : Liste des DHCP	13
Tableau 10 : Configuration initiale des firewall FGT 600 ^E	14

Liste des figures

Figure 1: Switch Fortiswitch 124F POE 4X SFP+.....	6
Figure 2: FortiAP 231F	6
Figure 3: Firewall 600E	7
Figure 4 : FortiAnalyzer	7
Figure 5: Architecture globale	8
Figure 6 : Serveur Proliant ML 350e Gen8	12
Figure 7 : Firewall FGT 600E	12
Figure 8: Architecture WAN	14
Figure 9 : Création du LAG	15
Figure 10 : Création du Vlan.....	15
Figure 11 : Configuration du DHCP	16
Figure 12 : Partie Data	16
Figure 13 : Partie serveur	17
Figure 14 : Interfaces physiques	17
Figure 15 : Zone SD-Wan	17
Figure 16 : WIFI SSID.....	17
Figure 17: Mise à jour.....	18
Figure 18: Upload licence	18
Figure 19: Register code	18
Figure 20: Configuration ACL.....	19
Figure 21: Security profiles	19
Figure 22 : FSSO.....	23
Figure 23 : HA	23
Figure 24 : Configuration du HA.....	24
Figure 25 : Configuration du SD-Wan	24
Figure 26 : Configuration du EMS	25
Figure 27 : Les profiles WIFI	25

Figure 28 : Les SSIDs Créés	26
Figure 29 : Traffic shaping	26
Figure 30 : Dashboard Fortiswitch	26
Figure 31 : Création des Vlans Fortiswitch.....	27
Figure 32 : Config des interfaces.....	27
Figure 33: Association des Vlans aux interfaces	28
Figure 34: Création du LAGs Trk1	28
Figure 35: Association des Vlans au Trk1	29
Figure 36: Ajout du route statique	29
Figure 37: Serveur ESXI	29
Figure 38: login Fortianalyzer.....	30
Figure 39: Dashboard Fortianalyzer.....	30
Figure 40: Ajout des équipements	31
Figure 41: Interface Fabric view	31
Figure 42: Interface Fortiview.....	31
Figure 43: Interface LogView	32
Figure 44 : Interface reports.....	32

I. Introduction

1. Cadre du projet

Prologic Tunisie est un intégrateur du réseau et de sécurité informatique professionnel disposant des compétences, de l'expérience et du personnel qualifié pour exécuter de manière irréprochable les tâches relatives à l'approvisionnement, au pilotage et à la supervision réseau. Il pourra vous fournir des prestations liées à l'intégration, à la virtualisation, à la sauvegarde des données, aux conseils et au support.

Ce présent rapport est rédigé dans le cadre du projet "Refonte de l'infrastructure réseau et sécurité Sesame", pour décrire notre solution proposée par l'équipe technique du Prologic afin de répondre aux besoins d'installation du réseau et de sécurité exigée par l'université Sesame pour assurer le bon fonctionnement dans leur environnement.

2. Objectif du projet

L'objectif du projet consiste en la mise en place d'une nouvelle infrastructure réseau au profit de Sesame dans le cadre de la refonte de son infrastructure. Le but de ce projet est d'avoir un réseau interne/externe consolidé, performant et le plus essentiel sécurisé afin de garantir la confidentialité des données circulant le réseau.

3. Liste des tâches

Le périmètre du projet s'articule autour des prestations demandées au niveau du cahier des charges à savoir :

- La Livraison, l'installation, la configuration et la mise en place de la nouvelle infrastructure réseau qui fait l'objectif de la refonte.
- La mise en rack, l'installation des modules d'alimentation et le câblage des équipements.
- L'implémentation de nouvelles configurations sur les équipements concernés, afin de savoir la configuration du switch core, du firewall et des points d'accès et Intégration Fort Analyzer afin de suivre tous les Différents LOG.
- Effectuer les opérations de tests préventifs des équipements avant et après les interventions en conformité avec les préconisations du constructeur.
- Assurer les mises à jour Software nécessaires afin de garantir toutes évolutions logicielles et matérielles recommandées par les constructeurs.

4. Equipements acquis

Comme première étape dans le projet de “Refonte infrastructure réseau et sécurité sesame”, Prologic s’est déplacé chez Sesame pour mettre en place et installer les nouveaux équipements suivants :

- **6 Fortiswitch 124F FPOE**
- **2 Fortiswitch 148F FPOE**
- **10 Forti-AP 231F**
- **2 FGT 600E**
- **VM FortiAnalyzer GB01**

4.1 Description du switch access Fortiswitch 124F POE

- La série de commutateurs Fortiswitch 124F est conçue pour les clients créer des espaces de travail numériques intelligents optimisés pour utilisateurs mobiles avec une approche filaire et sans fil intégrée.
- La famille FortiSwitch™ Secure Access offre des performances exceptionnelles sécurité, performance et gestion. Sûr, simple, et évolutif, FortiSwitch est le bon choix pour les entreprises conscientes des menaces de toutes tailles Optimisés pour les utilisateurs mobiles ET offrant une approche filaire ET sans fil intégrée, ces commutateurs fiables de couche 3 sont faciles à déployer ET gérer. Commutateurs Ethernet de couche 3.
- Doté d’une gamme de fonctionnalités de classe entreprise incluant routage statique ET RIP, IPv6, ACL, sécurité robuste ET QoS.

Croissance rapide ET simple

- FortiSwitch est généralement géré et déployé via notre FortiGate avec FortiLink mais peut également être déployé et géré dans des environnements non FortiGate.
- Choisissez parmi des commutateurs Ethernet compacts de 8, 12, 24 ET 48 ports avec PoE en option ET liaisons montantes de 10 GbE intégrées.



Figure 1: Switch Fortiswiitch 124F POE 4X SFP+

4.2 Description du FortiAP 231F:

Ce point d'accès intérieur Wi-Fi 6 de classe entreprise fournit trois radios ainsi que Des fonctionnalités tels que OFDMA ET deux ports Ethernet 1 Gbit/s. Le point D'accès peut fournir une analyse 24h/24 et 7j/7 sur les deux bandes tout en offrant UN accès sur les bandes 2, 4 GHz ET 5 GHz. La radio BLE intégrée peut être utilisée pour les balises ET les applications de Localisation.



Figure 2: FortiAP 231F

4.3 Description du Firewall FortiGate 600E:

La série FortiGate 600E fournit un SD-WAN centré sur les applications, évolutif et sécurisé solution avec des capacités de pare-feu de nouvelle génération (NGFW) pour les moyennes et grandes entreprises déployé au niveau du campus ou de la succursale. Protège contre les cybermenaces avec le système sur puce accélération et SD-WAN sécurisé à la pointe de l'industrie dans une solution simple, abordable et facile à déployer.

L'approche Security-Driven Networking de Fortinet offre une intégration étroite du réseau à la nouvelle génération de sécurité.



Figure 3: Firewall 600E

HA FGCP FGT:

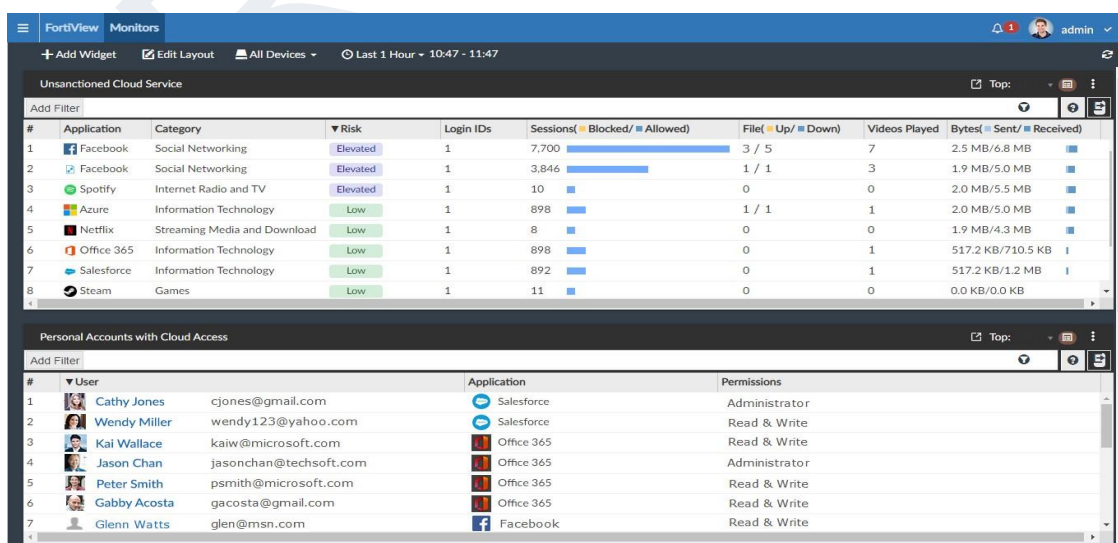
La haute disponibilité est une solution spécifique à FortiGate pour assurer la redondance. HA utilise FGCP. Essentiellement, HA fonctionne de manière similaire à VRRP, mais l'une des principales différences est que vous devez absolument avoir deux mêmes modèles FortiGate pour obtenir HA. Lorsque vous joignez vos pare-feu à un cluster, ils synchroniseront leurs configurations et fonctionneront comme un seul appareil, assurant le basculement et l'équilibrage de charge du trafic si nécessaire.

4.4 FortiAnalyzer:

VMFAZ : espace disque 400 GO

1 GO (Traitement donnée par jour)

- Reporting de conformité
- Visibilité de bout-en-bout grâce à une corrélation d'évènements et une détection des menaces
- Automatisation de la sécurité
- Intégrations optimales (SPLUNK, Qradar, etc.)
- Domaines d'administration (ADOM) et architecture multi-tenant



#	Application	Category	Risk	Login IDs	Sessions (Blocked / Allowed)	File (Up / Down)	Videos Played	Bytes (Sent / Received)
1	Facebook	Social Networking	Elevated	1	7,700	3 / 5	7	2.5 MB / 6.8 MB
2	Facebook	Social Networking	Elevated	1	3,846	1 / 1	3	1.9 MB / 5.0 MB
3	Spotify	Internet Radio and TV	Elevated	1	10	0	0	2.0 MB / 5.5 MB
4	Azure	Information Technology	Low	1	898	1 / 1	1	2.0 MB / 5.0 MB
5	Netflix	Streaming Media and Download	Low	1	8	0	0	1.9 MB / 4.3 MB
6	Office 365	Information Technology	Low	1	898	0	1	517.2 KB / 710.5 KB
7	Salesforce	Information Technology	Low	1	892	0	1	517.2 KB / 1.2 MB
8	Steam	Games	Low	1	11	0	0	0.0 KB / 0.0 KB

#	User	Application	Permissions
1	Cathy Jones	Salesforce	Administrator
2	Wendy Miller	Salesforce	Read & Write
3	Kai Wallace	Office 365	Read & Write
4	Jason Chan	Office 365	Administrator
5	Peter Smith	Office 365	Read & Write
6	Gabby Acosta	Office 365	Read & Write
7	Glenn Watts	Facebook	Read & Write

Figure 4 : FortiAnalyzer

II. High Level Design

High Level Design, dont l'abréviation est HLD, est la conception globale de l'architecture du réseau. Cette norme décrit la relation entre les différents nœuds et le flux de trafic entre eux.

La figure suivante présente la nouvelle architecture mise en place à Sesame.

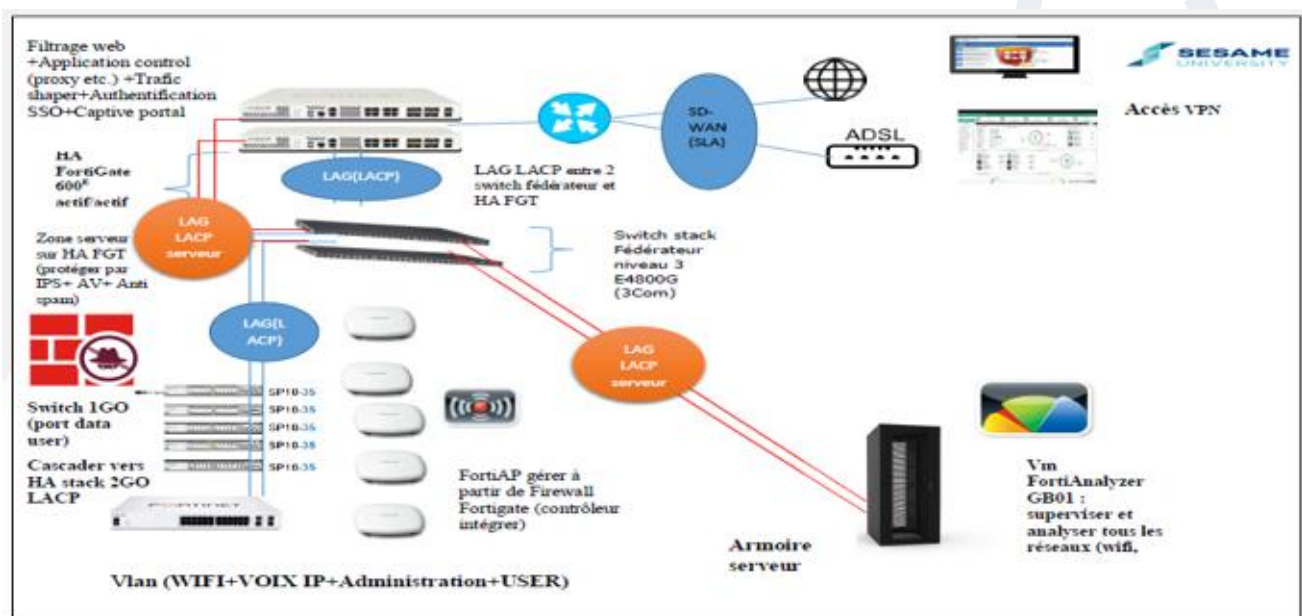


Figure 5: Architecture globale

L'ancien réseau de Sesame était un réseau plat et vulnérable. Il n'était pas segmenté où nous avons trouvé que les serveurs et le réseau LAN étaient dans la même plage réseau. Les équipements réseaux et informatiques étaient obsolètes. Nous avons trouvé un manque au niveau de composants de sécurité et de la documentation qui était insuffisante pour ne pas dire inexistante.

Avec la refonte du réseau, nous avons ajouté une couche de sécurité grâce au Firewall. Nous avons mis en place de nouveaux équipements, que vous trouvez leurs descriptions détaillées ci-dessous, dans le but de segmenter le réseau. Aussi, nous avons fait des liaisons LACP entre les switches Cœur 3com Et les firewalls fortinet 600E afin d'augmenter la capacité et la performance du réseau. Et nous avons installé un réseau Wi-Fi pour les candidats du concours Sopra Au niveau du contrôleur et ajouter d'autres WIFI pour étendre la couverture et faciliter la mobilité entre les différents départements de Sesame.

Nous Avons ajouté une solution FortiAnalyzer afin de suivre tous les événements au niveau des réseaux Sesame par gestion de reporting et Alerting

III. Switch + Contrôleur

1. Configuration des vlans

Le tableau suivant regroupe la liste des VLANs configurés sur le switch 3com.

Partie Data :

Vlan	ID
voix	2
Admin-Thin	5
Student-Thin	15
Wifi-Guest	20
Professeur-Thin	25
takolor	60
ISCI	40
Student PCs	17
Routing	100
Wifi-sopra	34

Tableau 1 : Liste des VLANs du SW partie data

Partie Serveur :

Vlan	ID
Admin	6
Student	16
Professeur	26
Server	30
MGMT	10
Server-new	90
MGMT-server-new	80
ISCI	40

Tableau 2 : Liste des VLANs du SW partie serveur

Le tableau suivant présente la configuration de base du switch 3com STACK, FGT à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

2. Configuration initiale

Attributs du switch à configurer	Valeur
IP management	10.10.255.1
Nom	SW-4800G
Login / Password	manager / se\$amE
Méthodes de management	Terminal / web
Nom	SW-4800G
Login Password	manager / se\$amE
Méthodes de management	Terminal / web

Tableau 3 : Configuration initiale SW 3com-stack

Attributs du switch à configurer	Valeur
IP management	10.10.255.71
Login / Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https
IP management	10.10.255.73
Login Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https
IP management	10.10.255.75
Login / Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https
IP management	10.10.255.78
Login Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https
IP management	10.10.255.81
Login Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https
IP management	10.10.100.86
Login Password	admin / se\$amE2023
Méthodes de management	terminal / SSH / telnet / https

Tableau 4 : Configuration initiale SW access

Attributs du contrôleur à configurer	Valeur
IP management	10.10.255.195
Login Password	huawei / se\$amEHuawei2020
Méthodes de management	Terminal / SSH / telnet / https

Tableau 5 : Configuration initiale du contrôleur

Les interfaces de switch peuvent être configurées en deux modes selon le trafic qui les traversent :

-Mode Access : sert à transporter le trafic d'un seul vlan. Par défaut, ce mode transportera le trafic du vlan natif (VLAN 1). Si les ports du switch sont affectés comme ports access, il peut être considéré comme les ports du switch appartenant à un seul domaine de diffusion. Tout trafic arrivant sur ces ports est considéré comme appartenant au VLAN attribué au port. Une liaison access se fait entre le switch et un périphérique terminal.

- Mode Trunk : sert à acheminer le trafic de plus d'un VLAN. Il fait un grand avantage car pour transporter le trafic de groupe de VLAN, un seul port de switch peut être suffisant et donne une grande utilité si l'utilisateur souhaite échanger du trafic entre plusieurs switches ayant plus d'un vlan configuré. Une liaison trunk s'établit entre le switch et un autre équipement du réseau.

Ce tableau regroupe les différents WIFI

Attributs du switch à configurer		Valeur
SSID		Teach1
Password		\$e\$@mecoNNecTme22
SSID		Studs1
Password		ses@meConnectme2
SSID		ConcourSopra
Password		SopraHR2022

Tableau 6 : Les accès WIFI

Le tableau suivant regroupe toutes les interfaces configurées du switch 3com.

LACP	Vlan ID	interfaces
LACP_server-port7_port_8_FGT	6,16,26,30,10,90,80	1/0/27,2/0/27,1/0/28,2/0/28
LACP_Data_Users_Port_3_4_FGT	2,5,15,20,25,40,60,17,34,100	1/0/29,2/0/29,1/0/30,2/0/30

Tableau 7 : Liste des LACP SW-3com

IV. Serveur externe

Le HPE ProLiant ML350e Gen8 est une plate-forme tour à deux processeurs, qui repose sur les derniers processeurs Intel Xeon E5-2400 pour créer une architecture système unique. Le HPE ProLiant ML350e Gen8 offre la technologie de gestion intégrée la plus puissante du secteur avec HPE Integrated Lights-Out 4 (iLO4), qui permet aux entreprises de gérer les serveurs à tout moment et de n'importe où.

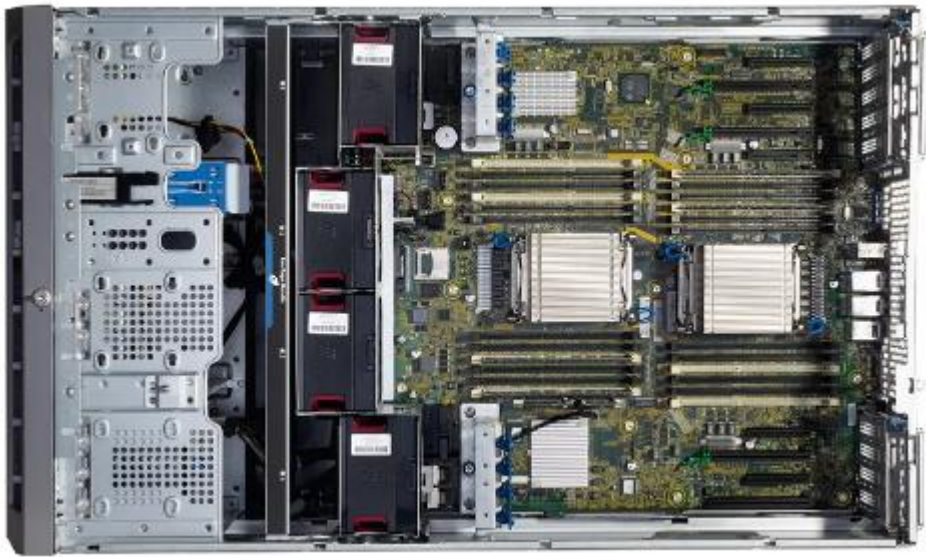


Figure 6 : Serveur Proliant ML 350e Gen8

1. Configuration initiale

On a déployé un serveur ESXI 6.5 u2 sur ce serveur dont les paramètres sont :

Attributs du switch à configurer	Valeur
IP management	10.80.10.40
Login Password	root/ Azerty123###*~
Méthodes de management	Terminal / SSH / telnet / https

Sur ce serveur ESXI on a ajouté 3 VMs EMS, FSSO et FAZ.

Le serveur fonctionne avec 2 cartes Vmnic (Vmnic 0 actif et Vmnic1 en mode standby)

V. Firewall



Figure 7 : Firewall FGT 600E

1. Spécifications du Fortigate 600E

La série FortiGate 600E offre des capacités de pare-feu de nouvelle génération pour les moyennes et grandes entreprises, avec la flexibilité d'être déployé sur le campus ou la branche d'entreprise. Il protège contre les Cyber-menaces avec processeur de sécurité haute performance, efficacité de la sécurité et une grande visibilité.

Dans ce projet, nous avons mis en place un cluster firewall actif /actif de la marque Fortinet et du modèle 600E dont les spécifications comme suit :

Firewall	IPS	NGFW	Threat Protection	Interfaces
36 Gbps	10 Gbps	800 Mbps	700 Mbps	Multiple GE RJ45, GE SFP and 10GE SFP+ slots

Tableau 8: Ports du Fortigate 600E

2. Configuration du service DHCP

Le serveur DHCP sert à attribuer d'une façon dynamique les adresses IP et d'autres informations de configuration réseau (passerelle, DNS) aux utilisateurs finaux. L'utilisateur n'a plus besoin de saisir ces informations manuellement, le serveur s'en charge. Au niveau du HA FGT 600F, nous avons activé le DHCP sur tous les VLANs.

Network Name	Network IP Adress	FG/GW IP	Vlan n ID
Student-Thin	10.15.1.0/20	10.15.1.254	15
Guest	10.20.1.0/16	10.20.1.254	20
Professor-Thin	10.25.1.0/24	10.25.1.254	25
Wifi-Sopra	10.34.1.0/16	10.34.1.254	34
Takolor	10.60.1.0/24	10.60.1.254	60

Tableau 9 : Liste des DHCP

3. Architecture WAN

Pour assurer la sécurité, il est recommandé de séparer l'accès internet du trafic local de Sesame. Pour cela nous avons installé un HA firewall Fortigate 600E entre le réseau

internet et le réseau LAN pour le filtrage du trafic entrant et sortant. Aussi, le firewall Fortigate va assurer la sécurité d'accès vers le serveur WEB et l'accès à distance par les VPNs clients. Une zone SD-WAN est créée pour faire le basculement entre le fibre et l'Adsl.

L'architecture WAN est présentée par la figure suivante :

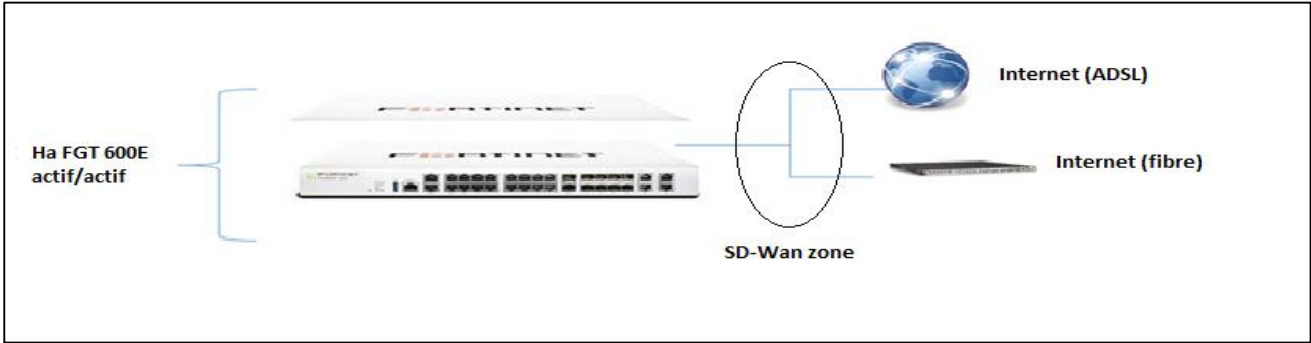


Figure 8:Architecture WAN

4. Configuration initiale

Le tableau suivant présente la configuration de base du firewall Fortigate à savoir son nom, login et mot de passe du compte d'administrateur, son adresse IP de management, etc...

Attributs du switch à configurer		Valeur
Nom		FGT_Master_SESAME
Login / Password		admin / sesame@2022@#*-
Adresse IP de management		10.10.255.254
Méthodes de management		https, SSH, telnet
Nom		FGT_Slave_SESAME
Login / Password		admin / sesame@2022@#*-
Adresse IP de management		10.10.255.254
Méthodes de management		https , SSH, telnet

Tableau 10 : Configuration initiale des firewall FGT 600^E

5. Configuration des interfaces

Cette figure montre comment créer une interface d'agrégation (LAG)

New Interface

Name

LAN_DATA_Sesame

Alias

Type

802.3ad Aggregate

VRF ID

0

Interface members

+

Role

LAN

Addressing mode

Manual DHCP Auto-managed by IPAM

IP/Netmask

0.0.0.0/0.0.0.0

Create address object matching subnet

Name

LAN_DATA_Sesame address

Destination

0.0.0.0/0.0.0.0

Secondary IP address

Administrative Access

IPv4

HTTPS

SSH

SNMP

PING

SNMP

FMG-Access

FTM

OK

Cancel

Figure 9 : Création du LAG

On peut aussi créer des Vlan comme le montre cette figure

Dashboard

Network

Interfaces

DNS

IPAM

SD-WAN

Static Routes

Policy Routes

RIP

OSPF

BGP

Routing Objects

Multicast

Diagnostics

Policy & Objects

Security Profiles

VPN

User & Authentication

System

New Interface

Name

Admin-Thin

Alias

Type

VLAN

VLAN protocol

802.1Q 802.1AD

Interface

VLAN ID

5

VRF ID

0

Role

LAN

Addressing mode

Manual DHCP Auto-managed by IPAM

IP/Netmask

10.5.1.254/24

Create address object matching subnet

Name

Admin-Thin address

Destination


10.5.1.254/24

Secondary IP address

Administrative Access

Figure 10 : Création du Vlan

Il est possible d'activer ou configurer le mode DHCP sur une interface. Dans ce cas on a activé le serveur DHCP sur un VLAN. Il faut spécifier une plage d'adresses pour ce serveur.


DHCP Server

DHCP status

Enabled

Disabled

Address range

10.5.1.1-10.5.1.253

+

Netmask

255.255.255.0

Default gateway

Same as Interface IP

Specify

DNS server

Same as System DNS

Same as Interface IP

Specify

Lease time

604800

second(s)

+

Advanced

Figure 11 : Configuration du DHCP

La capture ci-dessous présente la partie DATA configurée sur le FGT600E

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges
LAN_DATA_Sesame	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0				
Admin_THIN	VLAN		10.5.1.254/255.255.255.0		PING		
MGMT_INFRA_	VLAN		10.10.255.254/255.255.0.0		PING HTTPS Security Fabric Connection		
Professeur_THIN	VLAN		10.25.1.254/255.255.254.0		PING HTTPS	79	10.25.1.1-10.25.1.253
Student_PC	VLAN		10.17.1.254/255.255.0.0		PING		
Student_THIN	VLAN		10.15.1.254/255.255.240.0		PING	1	10.15.0.1-10.15.1.253 10.15.1.255-10.15.15.2
VLAN_Takolor	VLAN		10.60.1.254/255.255.255.0		PING	5	10.60.1.1-10.60.1.253
VOIX_IP	VLAN		10.2.1.254/255.255.240.0		PING HTTPS		
Wifi-Sopra	VLAN		10.34.1.254/255.255.0.0		PING	4	10.34.0.2-10.34.255.25
WIFI_Guest	VLAN		10.20.1.254/255.255.0.0			185	10.20.0.1-10.20.1.253 10.20.1.255-10.20.255.

Figure 12 : Partie Data

La capture ci-dessous présente la partie serveur configurée sur le FGT600E

Zone_server	802.3ad Aggregate	port7 port8	0.0.0.0/0.0.0.0		
Admin	VLAN		10.6.1.254/255.255.255.0	PING HTTPS	
ISCI	VLAN		10.40.255.254/255.255.255.0	PING	
NEW_MGT_SERV	VLAN		10.80.10.254/255.255.255.0	PING	
Prof	VLAN		10.26.1.254/255.255.255.0		
SERV_NEW	VLAN		10.90.10.254/255.255.255.0	PING	
Server	VLAN		10.30.1.254/255.255.255.0	PING HTTPS	
Student	VLAN		10.16.1.254/255.255.255.0	PING	
Student_thin	VLAN		0.0.0.0/0.0.0.0		

Figure 13 : Partie serveur

La capture ci-dessous présente les interfaces physiques du FGT600E

Physical Interface 16					
ADSL_Internet (port6)	Physical Interface	192.168.0.10/255.255.255.0		PING	
Fibre_Topnet (port5)	Physical Interface	41.231.85.167/255.255.255.240			
ha	Physical Interface	0.0.0.0/0.0.0.0			
mgmt	Physical Interface	192.168.1.99/255.255.255.0		PING HTTPS SSH FMG-Access	192.168.1.110-192.168.1.121
port1	Physical Interface	0.0.0.0/0.0.0.0			
port2	Physical Interface	0.0.0.0/0.0.0.0			
port9	Physical Interface	0.0.0.0/0.0.0.0	✓ FORTINET FT...		
port10	Physical Interface	0.0.0.0/0.0.0.0	✓ FORTINET FT...		
port11	Physical Interface	0.0.0.0/0.0.0.0			
port12	Physical Interface	0.0.0.0/0.0.0.0			
s1	Physical Interface	One-Arm Sniffer			
s2	Physical Interface	One-Arm Sniffer			

Figure 14 : Interfaces physiques

La capture ci-dessous présente la zone SD-Wan du FGT600E

SD-WAN Zone 3				
INTERNET	SD-WAN Zone	Fibre_Top... ADSL_Int...	0.0.0.0/0.0.0.0	
SASE	SD-WAN Zone		0.0.0.0/0.0.0.0	
virtual-wan-link	SD-WAN Zone		0.0.0.0/0.0.0.0	

Figure 15 : Zone SD-Wan

La capture ci-dessous présente les SSIDs des FortiAPs sur FGT600E

WiFi SSID 5			
Compétition HUAW...	WiFi SSID	0.0.0.0/0.0.0.0	
Studs1 (Studs2_Brid...	WiFi SSID	0.0.0.0/0.0.0.0	
Teach1 (Teach_bridge)	WiFi SSID	0.0.0.0/0.0.0.0	

Figure 16 : WIFI SSID

6. Configuration FGT 600E Et Recommandation

Pour mettre à jour les équipements il faut aller sous Fabric Management et appuyer sur Fabric upgrade

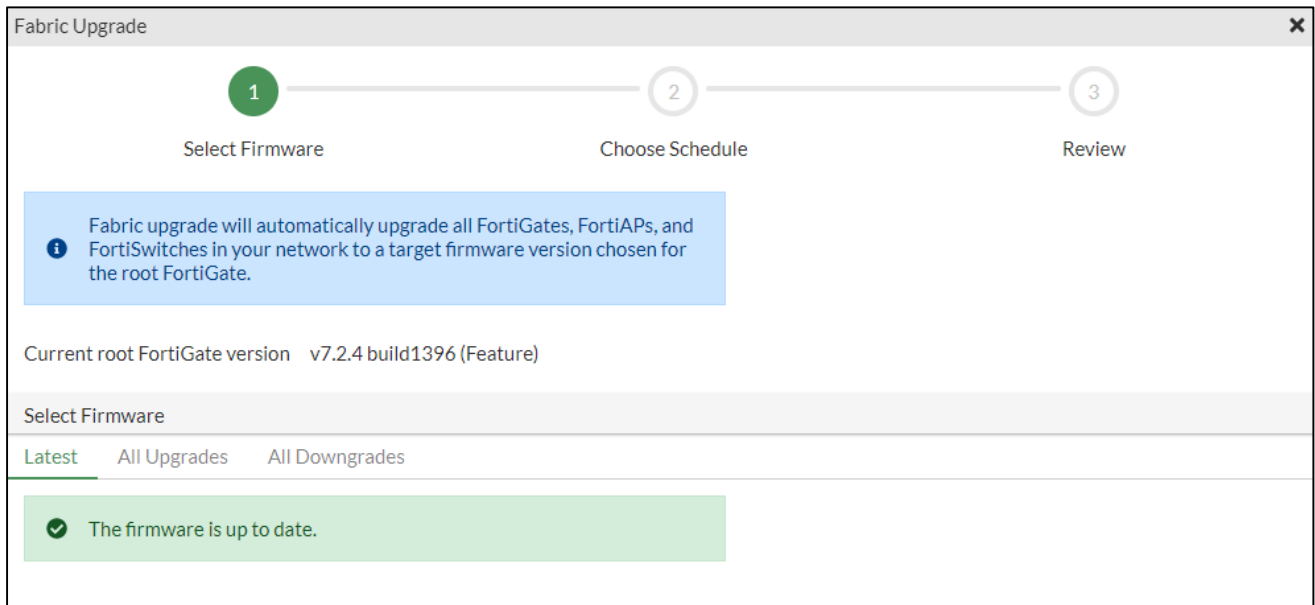


Figure 17: Mise à jour

Pour ajouter une licence il faut aller sous System → Fortiguard

On peut ajouter le fichier directement.

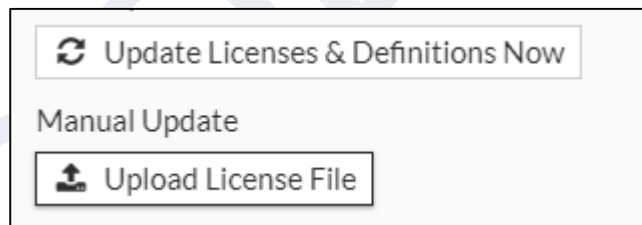


Figure 18: Upload licence

Ou il suffit de taper le code de la licence.

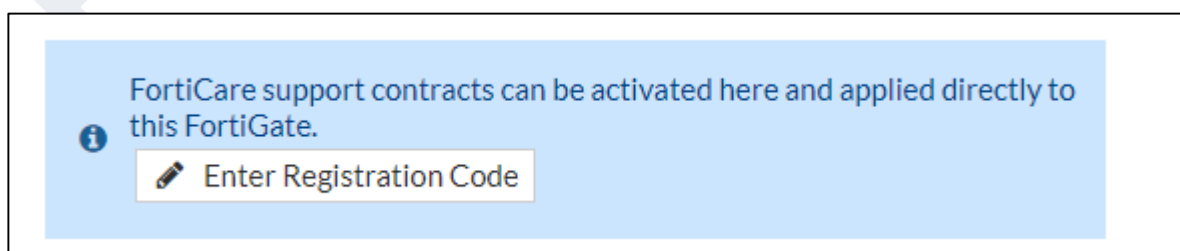
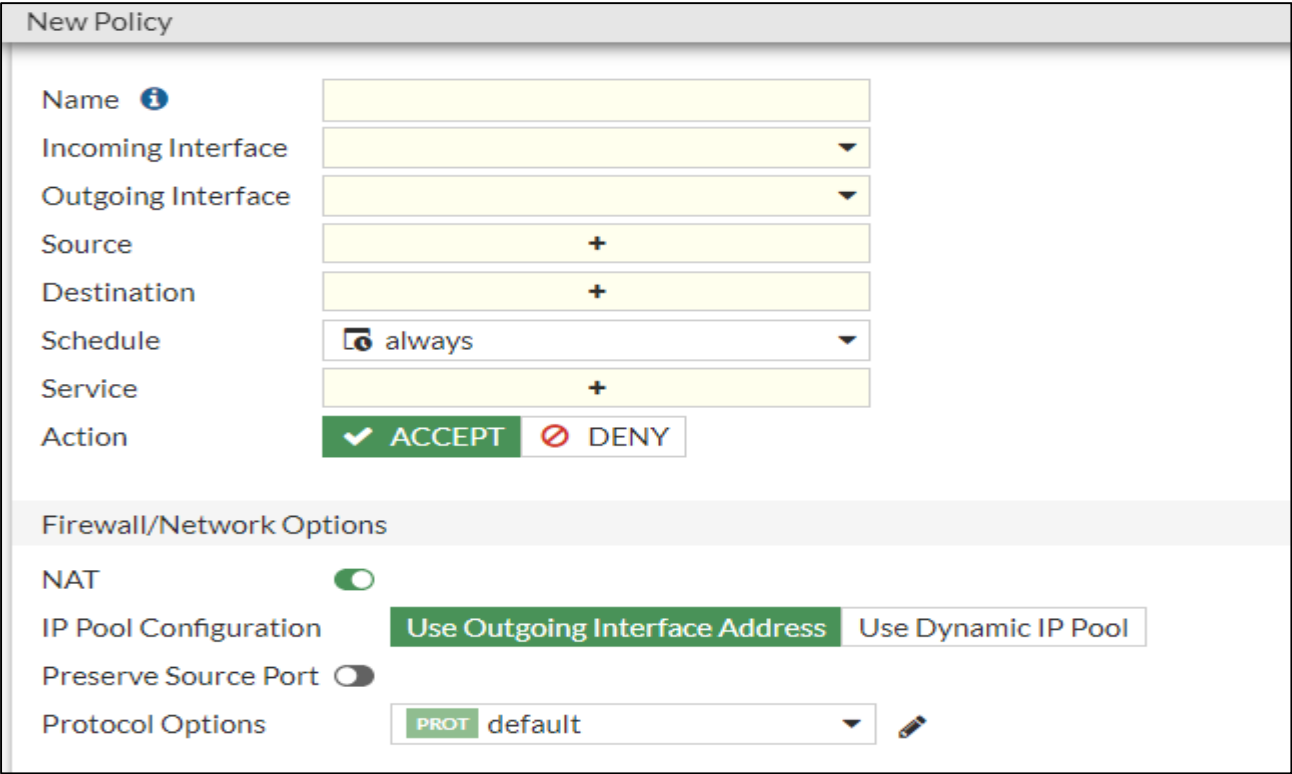


Figure 19: Register code

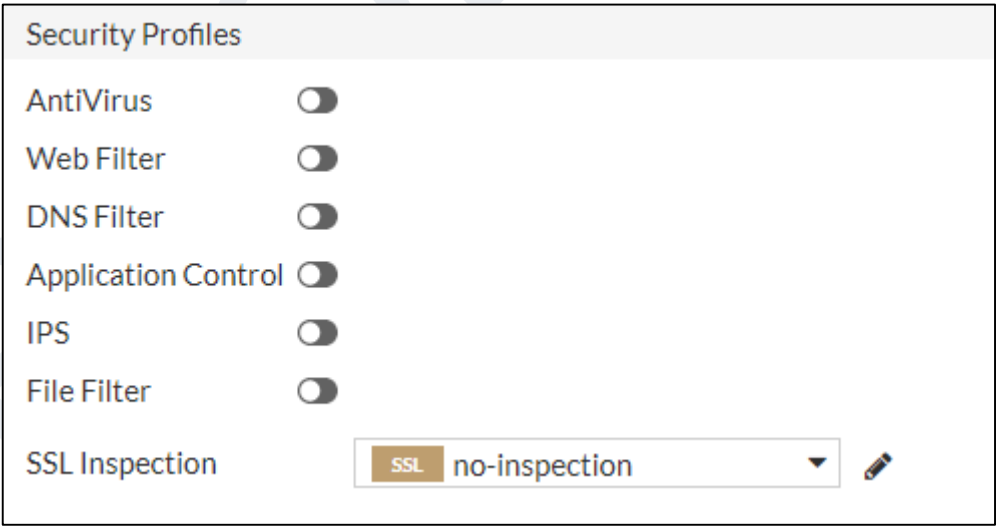
Pour créer une acces list il faut aller sous Policy & Objects → Firewall Policy



The 'New Policy' window is divided into two main sections. The top section contains fields for 'Name', 'Incoming Interface', 'Outgoing Interface', 'Source', 'Destination', 'Schedule' (set to 'always'), 'Service', and 'Action' (set to 'ACCEPT'). The bottom section, titled 'Firewall/Network Options', includes a 'NAT' toggle (checked), 'IP Pool Configuration' (set to 'Use Outgoing Interface Address'), 'Preserve Source Port' toggle (unchecked), and 'Protocol Options' (set to 'default').

Figure 20: Configuration ACL

On peut ajouter des options des profils de sécurités aux accès listes.



The 'Security Profiles' window lists several security features with toggle switches: 'AntiVirus', 'Web Filter', 'DNS Filter', 'Application Control', 'IPS', and 'File Filter', all of which are currently disabled. At the bottom, 'SSL Inspection' is set to 'no-inspection' via a dropdown menu.

Figure 21: Security profiles

Les figures ci-dessous indiquent la liste des règles de la sécurité

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Admin → Admin_THIN 1									
Admin_To_Admin_THIN	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	225.68 MB
Admin → INTERNET 2									
email-Internet	Admin	all	always	Email Access	ACCEPT	Enabled	no-inspection	UTM	69.41 MB
Admin_To_Internet	Admin	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	26.56 GB
Admin → ISCI 1									
Admin_To_ISCI	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Admin → MGMT_INFRA 1									
admin_to_mgmt	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	501.02 kB
Admin → Server 1									
Admin	Admin	AD_1 AD_2 SRV_3 SRV_TSE	always	Windows AD RDP	ACCEPT	Disabled	no-inspection	UTM	10.72 GB
Admin → Student_THIN 2									
Student_THIN_To_Admin	Student_THIN	Admin address	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
Admin_to_student_thin	Admin address	Student_THIN	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
Admin_THIN → Admin 1									
Admin_THIN_TO_Admin	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	153.78 GB

Admin_THIN → INTERNET 2									
email_To_Internet	Admin_THIN address	all	always	Email Access	ACCEPT	Enabled	no-inspection	UTM	8.07 MB
Admin_THIN_To_Internet	Admin_THIN address	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	6.65 GB
Admin_THIN → Server 1									
Admin_THIN_To_server	all	all	always	Windows AD RDP	ACCEPT	Disabled	no-inspection	UTM	9.67 MB
administration (ADMINISTRATION) → INTERNET 1									
WiFi-administration-to-NET	all	all	always	Windows AD	ACCEPT	Enabled	no-inspection	UTM	0 B
direction (DIRECTION) → INTERNET 1									
WiFi-Direction-to-NET	all	all	always	Windows AD	ACCEPT	Enabled	no-inspection	UTM	0 B
Etudiant (Etudiant) → INTERNET 1									
WiFi-etudiant-to-NET	all	all	always	Windows AD	ACCEPT	Enabled	no-inspection	UTM	0 B
Guest (Guest) → INTERNET 1									
Wifi-Guest-to-NET	all	all	always	Windows AD	ACCEPT	Enabled	no-inspection	UTM	0 B
ISCI → Admin 1									
ISCI_To_Admin	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
ISCI → Server 1									
ISCI_To_Server	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
MGMT_INFRA → Admin 1									
MGMT_to_admin	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	4.72 MB

MGMT_INFRA → INTERNET 2									
Email_TO_INTERNET	MGMT	all	always	Email Access	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	1.33 MB
MGMT_TO_Internet	MGMT	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	8.84 GB
MGMT_INFRA → ISCI 1									
MGMT_INFRA → NEW_MGT_SERV 1									
MGMT_INFRA_TO_MGMT_NEW_SRV	MGMT	ESXI_6.5 SRV_ESXI	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	960 B
MGMT_INFRA → SERV_NEW 1									
MGMT_INFRA_TO-VM_SRV	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	480 B
MGMT_INFRA → Server 1									
MGMT_INFRA_TO_server	all	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	31.91 MB
NEW_MGT_SERV → SERV_NEW 1									
MGT-serv_TO_serv-new	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
Professeur_THIN → Admin 1									
Professeur_THIN → INTERNET 2									
Email_TO_INTERNET	Prof_THIN	all	always	Email Access	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	313.71 MB
Prof_THIN_To_Internet	Prof_THIN	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	135.42 GB
Professeur_THIN → MGMT_INFRA_ 1									
WIF_THIN_to_MGMT_infra	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	561.62 MB

+ Create New		Edit	Delete	Policy Lookup	Search	Q	Export	Interface Pair View	By Sequence
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Professeur_THIN → NEW_MGT_SERV 1									
WIFI_TO_VLAN80	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	184.79 MB
Professeur_THIN → SERV_NEW 1									
WIFI_TO_NEW_VLAN_MGT	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	822.95 MB
Professeur_THIN → Server 2									
Professeur_THIN_To_Server	all	AD_1 AD_2	always	Windows AD	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	86.60 MB
wifi_to_server	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	3.38 MB
Professeur_THIN → Student_THIN 1									
test-pro-stud	Prof_THIN	Student_THIN	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	162.39 MB
SERV_NEW → INTERNET 1									
SERV-NEW-TO-Internet	IT_PROLOGIC SERV_NEW address	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	387.36 MB
SERV_NEW → NEW_MGT_SERV 1									
SERV_TO_MGMT-serv	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B
SERV_NEW → Server 1									
Server_new_to_ancien_server	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	36.77 GB
Server → Admin 1									
server_to_admin	all	AD_1 AD_2	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	0 B

Server → Admin_THIN 1									
server_to_Admin_THIN	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Server → INTERNET 2									
Email_to_internet	Server	all	always	Email Access	ACCEPT	Enabled	SSL no-inspection	UTM	95.19 MB
Server_To_Internet	AD_1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	63.33 MB
	AD_2								
	SRV_3								
	SRV_TSE								
Server → ISCI 1									
server_to_ISCI	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Server → MGMT_INFRA 1									
Server_TO_MGMT_INFRA	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	49.25 kB
Server → Student_THIN 2									
server_thin	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
Server_To_Student_THIN	all	all	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Student_THIN → Admin 1									
Student_Thin	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	1.36 GB
Student_THIN → INTERNET 2									
Email_To_Internet	Student_THIN	all	always	Email Access	ACCEPT	Enabled	SSL no-inspection	UTM	22.13 MB
Student_THIN_To_Internet	Student_THIN	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	37.54 GB

+ Create New Edit Delete Policy Lookup <input type="text"/> <input type="button" value="Q"/> <input type="button" value="Export"/> Interface Pair View By Sequence									
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Student_THIN → INTERNET 2									
Email_To_Internet	Student_THIN	all	always	Email Access	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	22.13 MB
Student_THIN_To_Internet	Student_THIN	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	37.54 GB
Student_THIN → Server 1									
Student_THIN_To_Server	all	AD_1 AD_2 SRV_TSE	always	Windows AD RDP	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	167.12 MB
VLAN_Takolor → INTERNET 3									
Email_To_Internet	Tkolor	all	always	Email Access	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	50.99 MB
Tkolor_To_Internet	Tkolor	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	112.40 GB
✗	Tkolor	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	0 B
WIFI_Guest → Admin 1									
WIFI-to-Admin	all	all	always	ALL	✓ ACCEPT	✗ Disabled	SSL no-inspection	UTM	56.81 MB
WIFI_Guest → INTERNET 2									
email_To_Internet	Wifi_Guest	all	always	Email Access	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	3.85 GB
Wifi_Guest_To_Internet	Wifi_Guest	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	337.66 GB
Wifi-Sopra → INTERNET 1									
Wifi-Sopra-to-internet	Wifi-Sopra address	all	always	ALL	✓ ACCEPT	✓ Enabled	SSL no-inspection	UTM	49.86 GB
Implicit 1									
Implicit Deny	all	all	always	ALL	✗ DENY			✗ Disabled	86.93 MB

La figure ci-dessous montre l'Intégration du FSSO avec firewall.

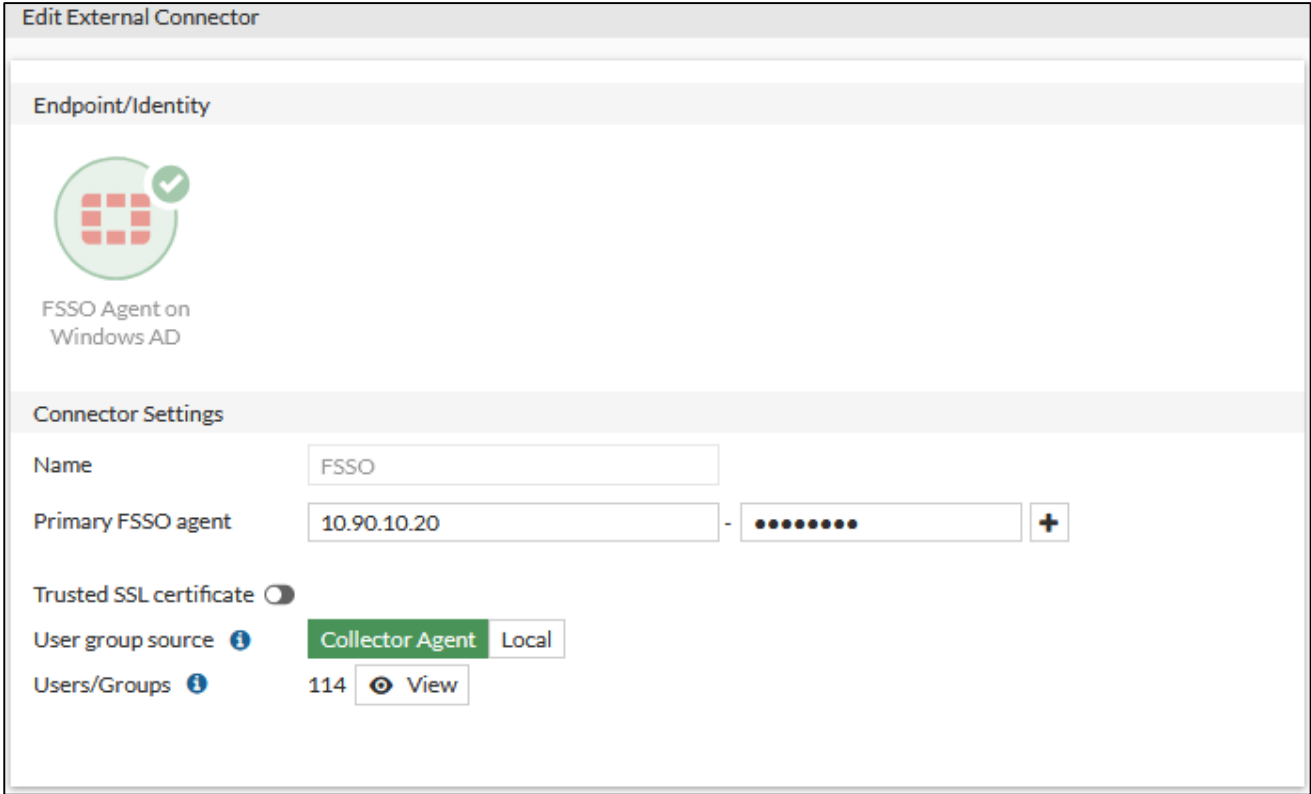
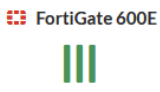


Figure 22 : FSSO

Les figures ci-dessous montrent la configuration du HA cluster FGT600E.



HA

1 3 5 7 9 11

S1 VW1 X1

MGMT 2 4 6 8 10 12

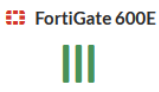
S2 VW2 X2

FGT_Master_SESAME (Primary)

Refresh

Edit

Remove device from HA cluster



HA

1 3 5 7 9 11

S1 VW1 X1

MGMT 2 4 6 8 10 12

S2 VW2 X2

FGT_Slave_SESAME (Secondary)

Figure 23 : HA

High Availability

Mode: Active-Active

Device priority: 128

Cluster Settings

Group name: Cluster-sesame

Password: Change

Session pickup: ☒

Monitor interfaces

- LAN_DATA_Sesame
- port3
- port4
- Fibre_Topnet (port5)
- ADSL_Internet (port6)
- port7
- port8
- Zone_server

Heartbeat interfaces

- port9
- port10

Heartbeat Interface Priority

port9: 150

port10: 150

☐ Management Interface Reservation

OK Cancel

Figure 24 : Configuration du HA

La figure ci-dessous montre la configuration SD-Wan

SD-WAN Zones SD-WAN Rules Performance SLAs

Bandwidth Volume Sessions

Download

Upload

2 Total

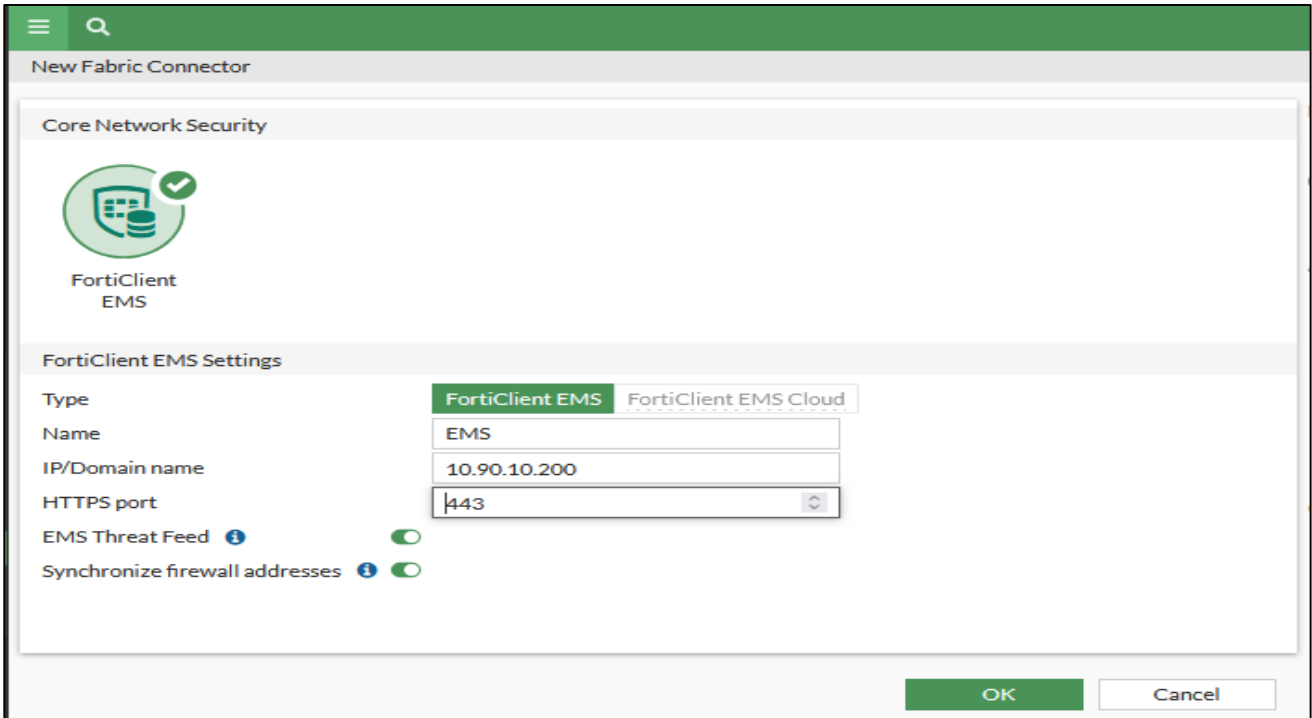
2 Total

+ Create New Edit Delete

Interfaces	Gateway	Cost	Download	Upload
virtual-wan-link				
SASE				
INTERNET				
Fibre_Topnet (port5)	41.231.85.161	0	15.46 Mbps	2.89 Mbps
ADSL_Internet (port6)	192.168.0.1	0	1.08 kbps	1.35 kbps

Figure 25 : Configuration du SD-Wan

La figure ci-dessous montre l'association du EMS avec FGT600E



New Fabric Connector

Core Network Security

FortiClient EMS

FortiClient EMS Settings

Type: **FortiClient EMS** | FortiClient EMS Cloud

Name: EMS

IP/Domain name: 10.90.10.200

HTTPS port: 443

EMS Threat Feed: ☒

Synchronize firewall addresses: ☒

OK Cancel

Figure 26 : Configuration du EMS

Partie WIFI :

La figure ci-dessous montre les profiles WiFi

Name	Platform(s)	Radio Mode	Band	SSIDs	Comments
FAP231F-default	FAP-231F	R1 Access Point R2 Access Point R3 Dedicated Monitor	R1 2.4GHz 802.11ax/n/g R2 5GHz 802.11ax/ac/n/a R3 N/A	R1 None R2 None R3 N/A	
Forti-AP-Sesame	FAP-231F	R1 Access Point R2 Disabled R3 Dedicated Monitor	R1 2.4GHz 802.11ax/n/g R2 N/A R3 N/A	R1 AP Studs1 (Studs2_Bridge) AP Teach1 (Teach_bridge) R2 N/A R3 N/A	
Forti-AP-salle-reunion	FAP-231F	R1 Access Point R2 Disabled R3 Dedicated Monitor	R1 2.4GHz 802.11ax/n/g R2 N/A R3 N/A	R1 AP Compétition HUAWEI (Accréditation) AP Studs1 (Studs2_Bridge) AP Teach1 (Teach_bridge) R2 N/A R3 N/A	

Figure 27 : Les profiles WIFI

La figure ci-dessous affiche les différents SSIDs

SSID 4					
Accréditation	AP Compétition HUAWEI (Accréditation)	Local Bridge	WPA2 Personal	always	Up
Studs2_Bridge	AP Studs1 (Studs2_Bridge)	Local Bridge	WPA2 Personal	always	Up
Teach_bridge	AP Teach1 (Teach_bridge)	Local Bridge	WPA2 Personal	always	Up

Figure 28 : Les SSIDs Créés

La figure ci-dessous comporte les profiles traffic shaping.

Traffic Shapers						
Traffic Shaping Policies						
Traffic Shaping Profiles						
+ Create New Edit Clone Delete <input type="text" value="Search"/>						
Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
Shared 1						
Traffic_TAKOLOR		20.00 Mbps	0 bps		High	0

Figure 29 : Traffic shaping

VI. FortiSwitch:

Voilà le dashboard du Fortiswitch.

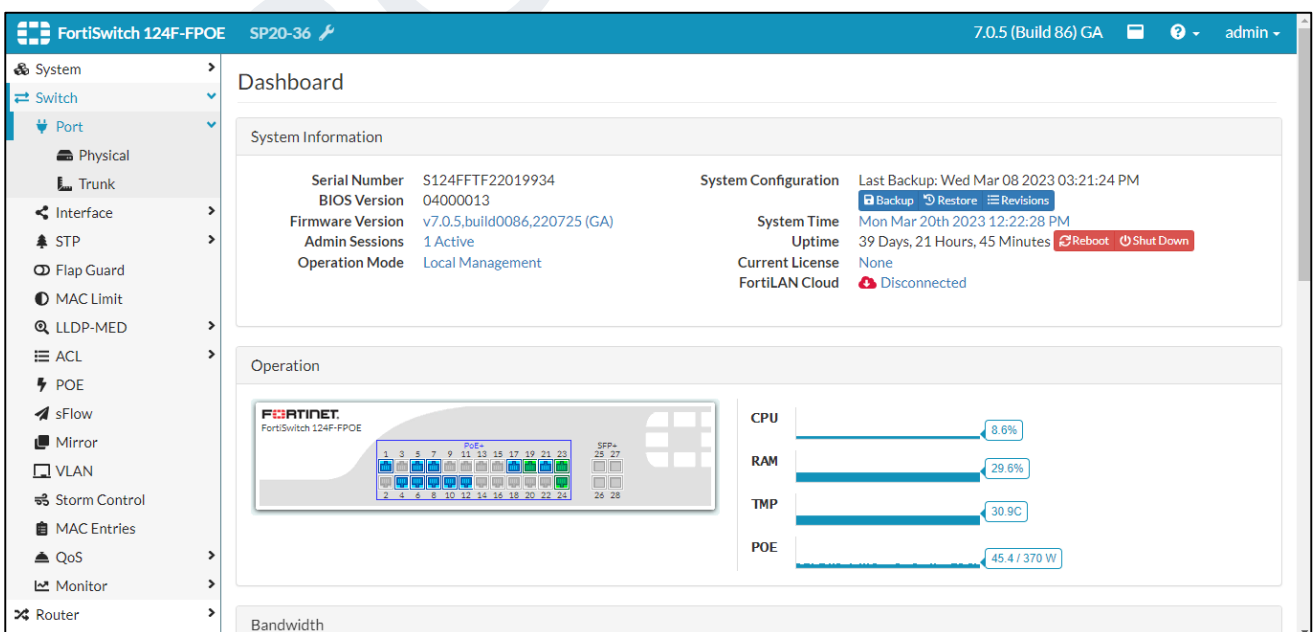


Figure 30 : Dashboard Fortiswitch

La creation des vlans se fait au niveau du menu network puis vlan

Physical	Name	Alias	VLAN ID	IP Address	Access	Features	Enabled	Link Status	Manage
VLAN	Student		15	0.0.0.0/0			↑	↑	Edit Delete
Loopback	Studs		20	0.0.0.0/0			↑	↑	Edit Delete
DNS	TAKOLOR		60	0.0.0.0/0			↑	↑	Edit Delete
Settings	VLAN5		5	0.0.0.0/0			↑	↑	Edit Delete
Config	VLAN10		10	10.10.255.78/24	HTTP HTTPS PING SSH TELNET		↑	↑	Edit Delete
Admin	guest		21	0.0.0.0/0			↑	↑	Edit Delete
User	professeur		25	0.0.0.0/0			↑	↑	Edit Delete
Authentication	sopra		34	0.0.0.0/0			↑	↑	Edit Delete
Certificate									
Link Monitor									
FortiLAN Cloud									
Locations									
Packet Capture									
Switch									
Router									
Log									

Figure 31 : Création des Vlans Fortiswitch

Pour configurer les interfaces physiques il faut accéder au menu switch.

Name	Traffic (Last Day)	VLAN(s)	Security Mode	STP	Edge Port	Packet Sampler
internal	17.78kbps	1 / 1-2, 5, 10, 15, 20-21, 25, 34, 60	None	—	✓	—
port1	61.34kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port2	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port3	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port4	3.129kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port5	3.049kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port6	1.370kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port7	808.2kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port8	1.327kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port9	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port10	55.88kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port11	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port12	3.027kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port13	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port14	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port15	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port16	0.000bps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—
port17	55.05kbps	10 / 15, 20-21, 25, 34 / 10	None	—	✓	—

Figure 32 : Config des interfaces

Il faut associer les vlans aux interfaces.

Edit Physical Port Interface

Name	port14		
Native VLAN	<input type="text" value="10"/>	(1-4094)	
Allowed VLANs	<input type="text" value="15,20-21,25,34"/>	(1-4094)	
Untagged VLANs	<input type="text" value="10"/>	(1-4094)	

Spanning Tree

☐ Enable

Figure 33: Association des Vlans aux interfaces

On peut créer des lag (dans notre cas on a crée une seule lag TRK1 comporte les ports 23,24,27,28)

Port Trunks

☒ Select All ☐ Deselect All

Search:

Name	Members	Mode	PSC	References	Manage
Trk1	port23, port24, port27, port28	Static	N/A	0	<input type="button" value="Edit"/>

Showing 1 to 1 of 1 entries

Figure 34: Création du LAGs Trk1

Il faut aussi associer les Vlan au Trk1

Trunk Interfaces					
<input checked="" type="checkbox"/> Select All <input type="checkbox"/> Deselect All <button>Edit</button>		Search: <input type="text"/>			
Name	Traffic (Last Day)	VLAN(s)	Native / Allowed / Untagged	STP	Edge Port
Trk1	997.3kbps	10 / 1-2, 5, 10, 15, 20-21, 25, 34, 60		—	✓

Figure 35: Association des Vlan au Trk1

Il faut ajouter une route static vers Firewall.

Static Routes						
<input checked="" type="checkbox"/> Select All <input type="checkbox"/> Deselect All <button>Delete</button>		Show 25 entries				
ID	Enabled	Destination IP / Mask	Device	Blackhole	Gateway	Dynamic Gateway
1	✓	0.0.0.0/0.0.0	VLAN10	—	10.10.255.254	—

Showing 1 to 1 of 1 entries

Figure 36: Ajout du route statique

VII. Serveur :

Cette parite présente le serveur ESXI installé sur un serveur.

Fortianalyzer est installé sur ce serveur.

- Adresse management du serveur est sur vlan 80 (10.80.10.X/24)
- Les Vms sont sur le vlan 90 (10.90.10.X/24)

Hôte	Machine virtuelle	Statut	Espace utilisé	SE invité	Nom d'hôte
Gérer	FSSO	✓ Nor...	400 Go	Microsoft Windows Serv...	Inconnu
Surveiller	EMS	✓ Nor...	100 Go	Microsoft Windows Serv...	Inconnu
Machines virtuelles 11	Serveur Linux	✓ Nor...	104,99 Go	Ubuntu Linux (64 bits)	ubuntu-info
Stockage 1	FAZ	✓ Nor...	511,9 Go	Autre Linux 2.6.x (64 bits)	Inconnu
Mise en réseau 5	FAC_	✓ Nor...	2,17 Go	Autre Linux 3.x ou versi...	Inconnu
	TSE2	✓ Nor...	240,11 Go	Microsoft Windows Serv...	Inconnu
	UBUNTU1	✓ Nor...	100 Go	Ubuntu Linux (64 bits)	Inconnu
	TSE	✓ Nor...	200 Go	Microsoft Windows Serv...	Inconnu
	FAZ_PROD	✓ Nor...	230,78 Go	Autre Linux 2.6.x (64 bits)	Inconnu
	SrvFile	✓ Nor...	993,68 Go	Microsoft Windows Serv...	Inconnu
	G.soud	✓ Nor...	75,11 Go	Microsoft Windows 10 (6...	Inconnu

Figure 37: Serveur ESXI

VIII. FortiAnalyzer:

Voici l'interface du login de fortianalyzer.

Adresse IP fortianalyzer est 10.90.10.65.

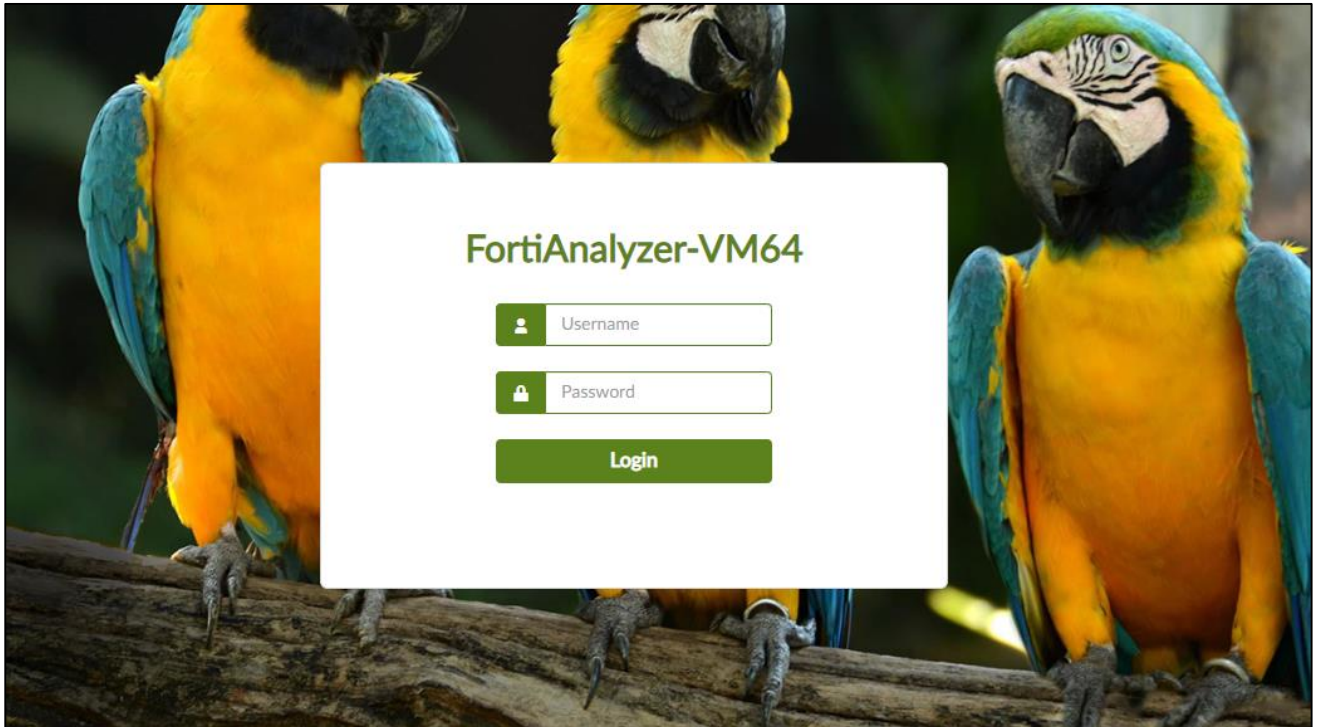


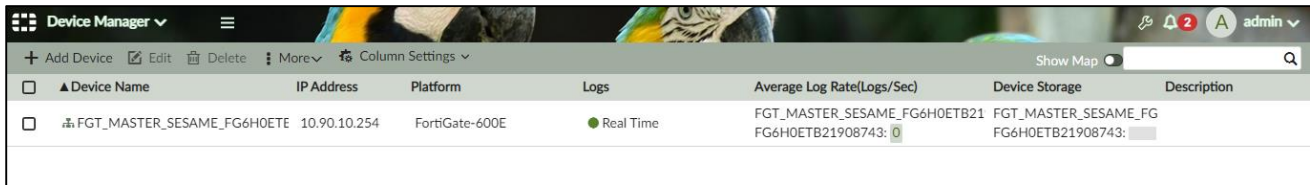
Figure 38: login Fortianalyzer

Après avoir saisir le login voici le dashboard qui s'affiche.



Figure 39: Dashboard Fortianalyzer

On peut ajouter l'équipement qu'on va surveiller à travers l'interface Device Manager.



Device Name	IP Address	Platform	Logs	Average Log Rate(Logs/Sec)	Device Storage	Description
FGT_MASTER_SESAME_FG6H0ETE	10.90.10.254	FortiGate-600E	Real Time	FGT_MASTER_SESAME_FG6H0ETB21 FG6H0ETB21908743: 0	FGT_MASTER_SESAME_FG FG6H0ETB21908743:	

Figure 40: Ajout des équipements

Voici l'interface Fabric View contient les différents devices connectés.

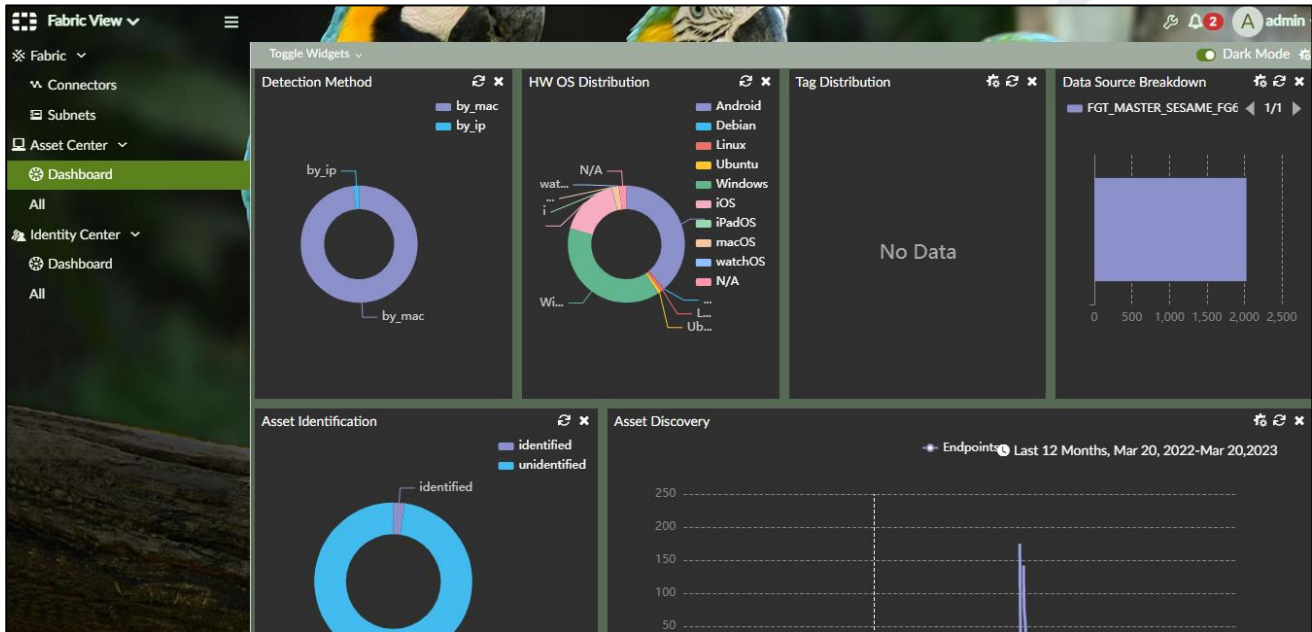


Figure 41: Interface Fabric view

Cette interface est l'interface est FortiView.

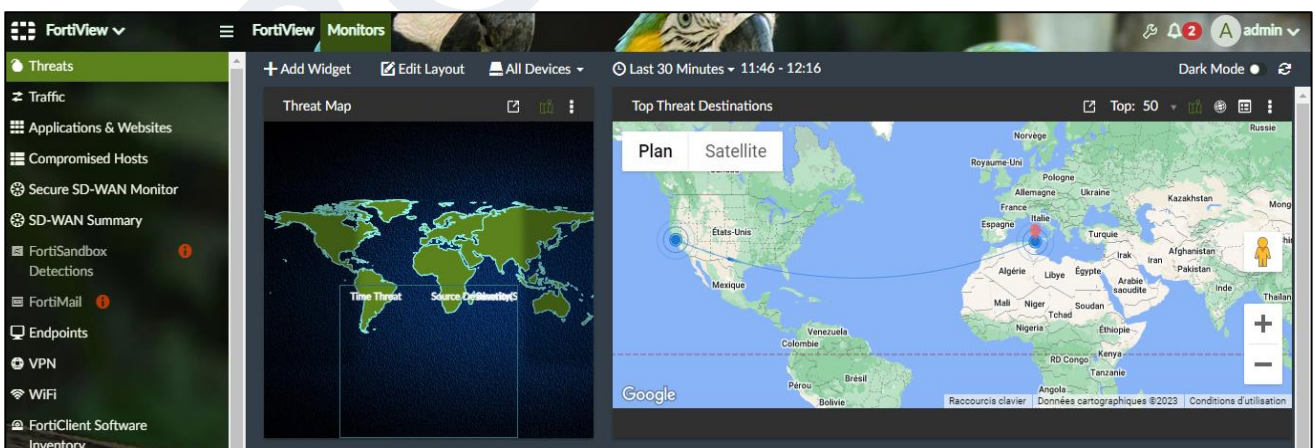
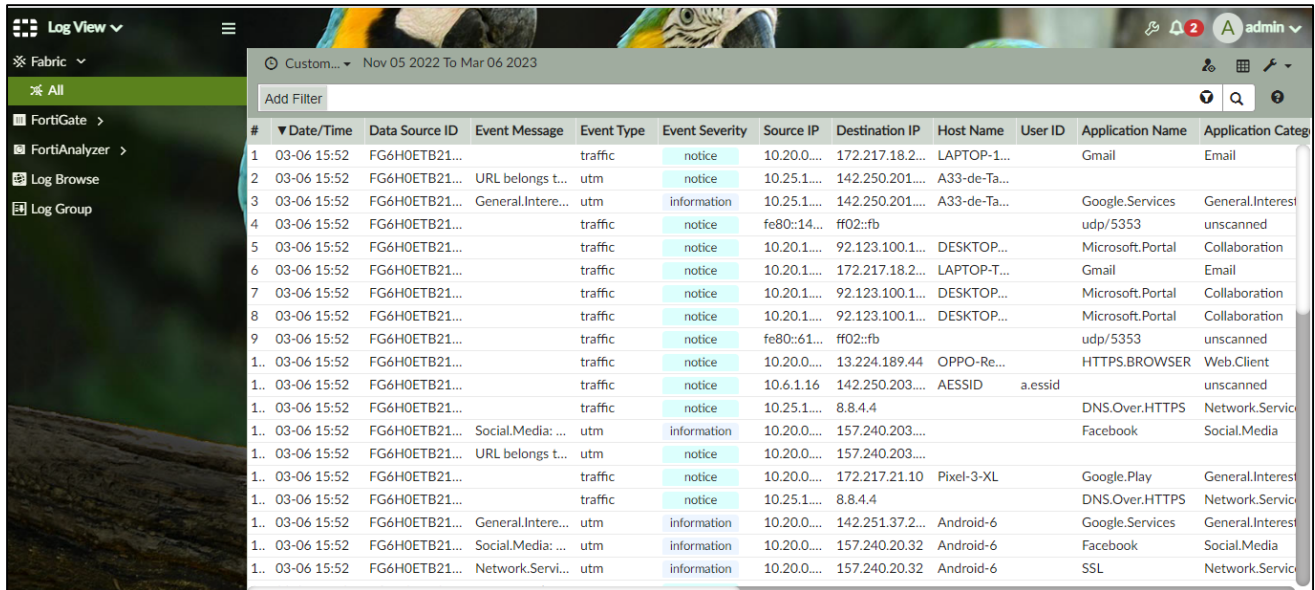


Figure 42: Interface Fortiview

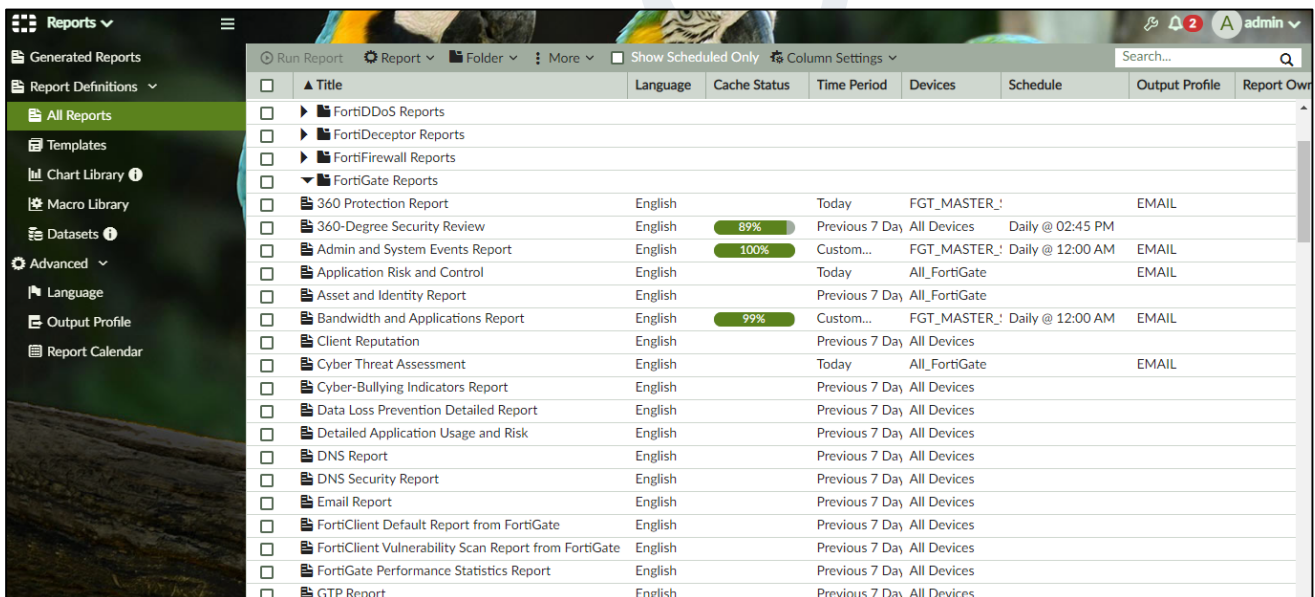
Cette figure présente l'interface log view qui contient les différents logs.



#	Date/Time	Data Source ID	Event Message	Event Type	Event Severity	Source IP	Destination IP	Host Name	User ID	Application Name	Application Category
1	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.0...	172.217.18.2...	LAPTOP-1...		Gmail	Email
2	03-06 15:52	FG6H0ETB21...	URL belongs t...	utm	notice	10.25.1...	142.250.201...	A33-de-Ta...			
3	03-06 15:52	FG6H0ETB21...	General.Intere...	utm	information	10.25.1...	142.250.201...	A33-de-Ta...		Google.Services	General.Interest
4	03-06 15:52	FG6H0ETB21...		traffic	notice	fe80::14...	ff02::fb			udp/5353	unscanned
5	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.1...	92.123.100.1...	DESKTOP...		Microsoft.Porta...	Collaboration
6	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.1...	172.217.18.2...	LAPTOP-T...		Gmail	Email
7	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.1...	92.123.100.1...	DESKTOP...		Microsoft.Porta...	Collaboration
8	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.1...	92.123.100.1...	DESKTOP...		Microsoft.Porta...	Collaboration
9	03-06 15:52	FG6H0ETB21...		traffic	notice	fe80::61...	ff02::fb			udp/5353	unscanned
1..	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.0...	13.224.189.44	OPPO-Re...		HTTPS.BROWSER	Web.Client
1..	03-06 15:52	FG6H0ETB21...		traffic	notice	10.6.1.16	142.250.203...	AESSID	a.essid		unscanned
1..	03-06 15:52	FG6H0ETB21...		traffic	notice	10.25.1...	8.8.4.4			DNS.Over.HTTPS	Network.Service
1..	03-06 15:52	FG6H0ETB21...	Social.Media: ...	utm	information	10.20.0...	157.240.203...			Facebook	Social.Media
1..	03-06 15:52	FG6H0ETB21...	URL belongs t...	utm	notice	10.20.0...	157.240.203...				
1..	03-06 15:52	FG6H0ETB21...		traffic	notice	10.20.0...	172.217.21.10	Pixel-3-XL		Google.Play	General.Interest
1..	03-06 15:52	FG6H0ETB21...		traffic	notice	10.25.1...	8.8.4.4			DNS.Over.HTTPS	Network.Service
1..	03-06 15:52	FG6H0ETB21...	General.Intere...	utm	information	10.20.0...	142.251.37.2...	Android-6		Google.Services	General.Interest
1..	03-06 15:52	FG6H0ETB21...	Social.Media: ...	utm	information	10.20.0...	157.240.20.32	Android-6		Facebook	Social.Media
1..	03-06 15:52	FG6H0ETB21...	Network.Servi...	utm	information	10.20.0...	157.240.20.32	Android-6		SSL	Network.Service

Figure 43: Interface LogView

Cette interface présente l'interface de reporting.



	Title	Language	Cache Status	Time Period	Devices	Schedule	Output Profile	Report Owner
<input type="checkbox"/>	FortiDDoS Reports							
<input type="checkbox"/>	FortiDeceptor Reports							
<input type="checkbox"/>	FortiFirewall Reports							
<input type="checkbox"/>	FortiGate Reports							
<input type="checkbox"/>	360 Protection Report	English		Today	FGT_MASTER_!		EMAIL	
<input type="checkbox"/>	360-Degree Security Review	English	89%	Previous 7 Day	All Devices	Daily @ 02:45 PM		
<input type="checkbox"/>	Admin and System Events Report	English	100%	Custom...	FGT_MASTER_!	Daily @ 12:00 AM	EMAIL	
<input type="checkbox"/>	Application Risk and Control	English		Today	All_FortiGate		EMAIL	
<input type="checkbox"/>	Asset and Identity Report	English		Previous 7 Day	All_FortiGate			
<input type="checkbox"/>	Bandwidth and Applications Report	English	99%	Custom...	FGT_MASTER_!	Daily @ 12:00 AM	EMAIL	
<input type="checkbox"/>	Client Reputation	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	Cyber Threat Assessment	English		Today	All_FortiGate		EMAIL	
<input type="checkbox"/>	Cyber-Bullying Indicators Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	Data Loss Prevention Detailed Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	Detailed Application Usage and Risk	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	DNS Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	DNS Security Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	Email Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	FortiClient Default Report from FortiGate	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	FortiClient Vulnerability Scan Report from FortiGate	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	FortiGate Performance Statistics Report	English		Previous 7 Day	All Devices			
<input type="checkbox"/>	GTP Report	English		Previous 7 Day	All Devices			

Figure 44 : Interface reports

Conclusion

Pendant ce projet, on a fait une étude détaillée du réseau informatique de Sesame afin de relever les différentes insuffisances présentées par le dit réseau. L'architecture, que nous avons mis à la place de l'ancienne architecture, fait face à ces insuffisances permettant de rendre le réseau beaucoup plus sécurisé et performant.

Tout au long de nos interventions, nous avons pris en compte les besoins du notre client, Sesame, pour obtenir enfin un réseau bien segmenté et sécurisé assurant le bon fonctionnement des équipements et des logiciels et favorisant une transmission rapide et sécurisée des données qui répond aux besoins et aux priorités de la société et ses employés.