

Documentation technique

1. Présentation du Projet	2
2. Schéma réseau	2
3. Zones SD WAN	2
4. FORTIGATE 100F - SITE [REDACTED]	3
4.1. Configuration IP	3
4.2. VPN [REDACTED]	3
4.3. Zones SD-WAN	3
4.4. Règles de routage	3
4.5. Règles de sécurités	4
5. FORTIGATE 40F - SITE [REDACTED]	5
5.1. Configuration IP	6
5.2. Zones SD-WAN	6
5.3. Règles de routage	6
5.4. Règles de sécurité	7
6. FORTIGATE 40F - SITE [REDACTED]	7
6.1. Configuration IP	7
6.2. Zones SD-WAN	8
6.3. Règles de routage	8
6.4. Règles de sécurité	8
7. FORTIGATE 40F - SITE [REDACTED]	9
7.1. Configuration IP	9
7.2. Zones SD-WAN	9
7.3. Règles de routage	10
7.4. Règles de sécurité	10
8. FORTIGATE 40F - SITE [REDACTED]	10
8.1. Configuration IP	10
8.2. Zones SD-WAN	10
8.3. Règles de routage	11
8.4. Règles SD-WAN	11
8.5. Règles de sécurité	11
9. FORTIGATE 40F - SITE [REDACTED]	12
9.1. Configuration IP	12
9.2. Zones SD-WAN	13
9.3. Règles de routage	13
9.4. Règles SD-WAN	13
9.5. Règles de sécurité	13
10. FORTIGATE 40F - SITE [REDACTED]	14
10.1. Configuration IP	14
10.2. Zones SD-WAN	15
10.3. Règles de routage	15
10.4. Règles SD-WAN	15
10.5. Règles de sécurité	15

1. Présentation du Projet

Le présent projet a pour objectif d'assurer une continuité de service dans le cadre du remplacement de l'actuel fournisseur internet suite à une cyber-attaque. Les sites devront être interconnectés à travers un réseau SD WAN qui délimitera les sites en fonction des MPLS et des accès propre à chaque marque. La solution s'appuie sur des boîtiers de la marque Fortinet.

2. Schéma réseau



3. Zones SD WAN

3.1. Globale

La zone globale a pour objectif d'interconnecter tous les sites entre eux et de les superviser et de les administrer pour la partie informatique.

3.2. VKS

La zone [REDACTED] est quant à elle une zone permettant aux différents sites équipés d'un routeur MPLS [REDACTED] de leur permettre en cas de perte de leurs liens MPLS [REDACTED] de pouvoir se connecter aux autres liens afin d'assurer une continuité de service.

3.3. [REDACTED]

La zone [REDACTED] est pour l'instant inactive.

3.4. [REDACTED]

La zone [REDACTED] permet au site partenaire de [REDACTED] de communiquer avec les différents équipements présent sur le site de [REDACTED]

4. FORTIGATE 100F - SITE [REDACTED]

4.1. Configuration IP

WAN :

IP Publique : [REDACTED] non porté par le fortigate, porté par le routeur linktr en [REDACTED]/30

IP WAN : [REDACTED]/30

LAN :

Réseau : 10.[REDACTED]/24

Passerelle : [REDACTED]

4.2. VPN [REDACTED]

4.3.

[REDACTED]

4.4. Zones SD [REDACTED]

Zone [REDACTED] : permet de donner accès au LAN [REDACTED] et au réseau [REDACTED]

Cinq zones SD-WAN :

Zone "Virtual Wan Link" qui est la zone reliant le Site [REDACTED] avec un accès [REDACTED]










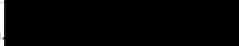

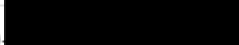

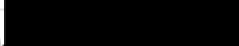




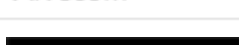


Zone "[REDACTED]"

Zone "[REDACTED]"

Zone "[REDACTED]"






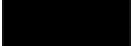
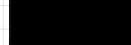
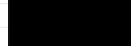
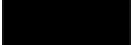

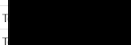
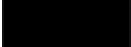

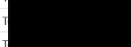
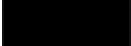
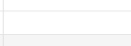

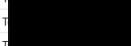


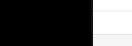









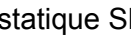






Zone "Alvecom" qui permettra la supervision depuis notre réseau

[REDACTED]

	Interfaces
	virtual- 
	VPNSD- 
	
	VPNSD- 
	VPNSD- 
	VPNSD- 
	VPNSD- 
	
	Alvecom
	
	VPNSD- 

4.5. Règles de routage

Les routes sont faites à partir des zones SD-WAN pour laisse le SD-WAN gérer le routage entre les potentiels plusieurs liens à l'intérieur.

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0		wan1	Enabled	Default
			Enabled	
		LAN	Enabled	
		LAN	Enabled	
		VPNSD-AU-PI-4G	Enabled	
		VPNSD- 	Enabled	
		VPNSD- 	Enabled	
		Alvecom	Enabled	
			Enabled	
			Enabled	
			Enabled	

Route statique SD-WAN vers LAN 

4.6. Règles de sécurités

Règles Bidirectionnelle : [] | [] <-> [] []

Autorisation du LAN vers le WAN avec un filtrage WEB, APPLICATIF, inspection antivirus et IPS

Autorisation du LAN vers le LAN ***** via zone SD-WAN

Autorisation des zones ***** et ***** vers le LAN

Autorisation de ***** vers le LAN *****ine + routes, ainsi que l'autorisation d'accès à tous les sites

Autorisation du trafic SSL vers le LAN, les sites et les routes

Autorisation du trafic ***** double sens ainsi que ***** vers les routes

5. FORTIGATE 40F - SITE *****

5.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction aucune solution fixe n'est en place. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : *****_*****.dyndns.org

IP WAN : 192. [REDACTED] /24

LAN :

Reseau : 192. [REDACTED] /24

Passerelle : 192. [REDACTED]

5.2. Zones SD-WAN

Zone par défaut reliant ***** ET *****INE

5.3. Règles de routage

[REDACTED]

5.4. Règles de sécurité

Autorisation du LAN vers le WAN avec un filtrage WEB, APPLICATIF, inspection antivirus et IPS

Autorisation du LAN vers le LAN ***** et Routes

6. FORTIGATE 40F - SITE [REDACTED]

6.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction la fibre n'est pas déployée. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : *****-████████.dyndns.org
IP WAN : ████████/24

LAN :
Reseau : ████████/27
Passerelle : ████████

6.2. Zones SD-WAN

Zone SD-WAN par défaut permettant la connexion avec le site de *****ine.
Deux VPN y sont présents : l'un sur le lien fibre (pas déployé pour l'instant) et l'autre sur le lien 4G/5G.

6.3. Règles de routage

À noter que la route vers le routeur VGF est monitoré afin de vérifier la bonne disponibilité du service.

6.4. Règles de sécurité

Autorisation du LAN vers les deux sorties WAN avec un filtrage WEB, APPLICATIF, inspection antivirus et IPS

Autorisation du lan vers le LAN *****INE et les ROUTES *****

7. FORTIGATE 40F - SITE [REDACTED]

7.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction la fibre n'est pas déployée. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : *****-[REDACTED].dyndns.org

IP WAN : 192.[REDACTED]/24

LAN :

Reseau : 10.[REDACTED]/25

Passerelle : 10.[REDACTED]

7.2. Zones SD-WAN

Zone SD-WAN par défaut permettant la connexion avec le site de *****ine.
Deux VPN y sont présents : l'un sur le lien fibre (pas déployé pour l'instant) et l'autre sur le lien 4G/5G.

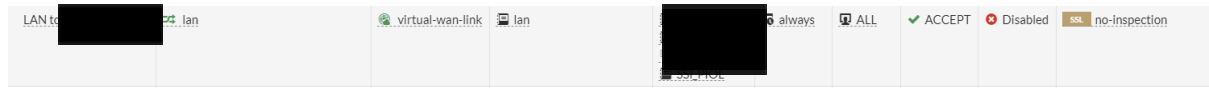
7.3. Règles de routage

[REDACTED]

7.4. Règles de sécurité

[REDACTED]

Autorisation du LAN vers les deux sorties WAN avec un filtrage WEB, APPLICATIF, inspection antivirus et IPS



Autorisation du lan vers le LAN *****INE et les ROUTES *****

8. FORTIGATE 40F - SITE [REDACTED]

8.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction la fibre n'est pas déployée. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : *****-[REDACTED].dyndns.org

IP WAN : [REDACTED]

LAN :

Reseau : 192.168.4.0/24

Passerelle : 10.x.x.x.x

8.2. Zones SD-WAN

Deux SD-WAN :

[REDACTED]

Zone Virtual-wan-Link permettant le fail-over/loadbalancing des deux liens WAN (fibre et 5G)

Zone ***** permettant la connexion avec le site de *****ine et via routage le réseau *****

Deux VPN y sont présents : l'un sur le lien fibre (pas déployé pour l'instant) et l'autre sur le lien 4G/5G.

8.3. Règles de routage

Quatre routes statiques SD-WAN

Deux routes pour les sous-réseaux *****

Une route pour le sous-réseau *****

Ainsi que, la route par défaut

8.4. Règles SD-WAN

Une règle SD-WAN pour le choix entre les deux WAN établi sur la latence vers GMAIL

Une règle SD-WAN pour le choix entre les deux VPN fibre et 5G vers ***** basé sur la latence vers un serveur ***** et le DNS *****

8.5. Règles de sécurité

Une première règle pour la Sortie vers le WAN : Elle est établie sur la zone SD-WAN, elle s'applique donc au deux liens WAN. Un filtrage classique NSFW est appliqué.

Puis deux règles Miroir permettant la communication du LAN vers ***** et ***** et de ***** et ***** vers le LAN

Enfin, la règle implicite permettant le DROP de tout autre trafic non voulu.

9. FORTIGATE 40F - [REDACTED]

9.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction la fibre n'est pas déployée. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : *****-[REDACTED].dyndns.org

IP WAN : [REDACTED]

LAN :

Reseau : 192.168.20.0/24

Passerelle : 192.168.20.254

9.2. Zones SD-WAN

Deux SD-WAN :

Zone Virtual-wan-Link permettant le fail-over/loadbalancing des deux liens WAN (fibre et 5G)

Zone ***** permettant la connexion avec le site de *****ine et via routage le réseau *****

Deux VPN y sont présents : l'un sur le lien fibre (pas déployé pour l'instant) et l'autre sur le lien 4G/5G.

9.3. Règles de routage

Quatre routes statiques SD-WAN

Deux routes pour les sous-réseaux *****

Une route pour le sous-réseau *****

Ainsi que, la route par défaut

9.4. Règles SD-WAN

Une règle SD-WAN pour le choix entre les deux WAN établi sur la latence vers GMAIL

Une règle SD-WAN pour le choix entre les deux VPN fibre et 5G vers ***** basé sur la latence vers un serveur ***** et le DNS *****

9.5. Règles de sécurité

La première règle permet un accès en VPN SSL au Forti.

La deuxième règle est là pour autoriser le trafic vers le 3CX.

Une troisième règle pour la Sortie vers le WAN : Elle est établie sur la zone SD-WAN, elle s'applique donc au deux liens WAN. Un filtrage classique NSFW est appliqué.

Puis deux règles Miroir permettant la communication du LAN vers ***** et ***** et de ***** et ***** vers le LAN

Enfin, la règle implicite permettant le DROP de tout autre trafic non voulu.

10. FORTIGATE 40F - SITE *****

10.1. Configuration IP

La solution s'appuie sur un équipement 5G et à l'heure de cette rédaction la fibre n'est pas déployée. L'équipement 5G se voit attribuer une adresse dynamique dyndns afin de permettre l'interconnexion au site principal de *****.

IP Publique : [REDACTED]

IP WAN :

LAN :

Reseau : 192.168.21.0/24

Passerelle : 192. [REDACTED]

10.2. Zones SD-WAN

Deux SD-WAN :

Zone Virtual-wan-Link permettant le fail-over/loadbalancing des deux liens WAN (fibre et 5G)

Zone ***** permettant la connexion avec le site de *****ine et via routage le réseau *****

Deux VPN y sont présents : l'un sur le lien fibre (pas déployé pour l'instant) et l'autre sur le lien 4G/5G.

10.3. Règles de routage

Quatre routes statiques SD-WAN

Deux routes pour les sous-réseaux *****

Une route pour le sous-réseau *****

Ainsi que, la route par défaut

10.4. Règles SD-WAN

Une règle SD-WAN pour le choix entre les deux WAN établi sur la latence vers GMAIL

Une règle SD-WAN pour le choix entre les deux VPN fibre et 5G vers ***** basé sur la latence vers un serveur ***** et le DNS *****

10.5. Règles de sécurité

La première règle permet un accès en VPN SSL au Forti.

La deuxième règle est là pour autoriser le trafic vers le 3CX.

Une troisième règle pour la Sortie vers le WAN : Elle est établie sur la zone SD-WAN, elle s'applique donc au deux liens WAN. Un filtrage classique NSFW est appliqué.

Puis deux règles Miroir permettant la communication du LAN vers ***** et ***** et de ***** et ***** vers le LAN

Enfin, la règle implicite permettant le DROP de tout autre trafic non voulu.