BTS SIO – Services Informatiques aux Organisations

30 Janvier 2026
Option SISR

François Oscar
Henry Stephane

SOMMAIRE

Cahier des charges

Le projet consiste en la migration des services de sécurité d'un environnement virtuel pfSense vers un équipement physique Cisco ASA 5506. Les objectifs définis sont les suivants :

- Accès sécurisé : Assurer la prise de main à distance sécurisée sur le pare-feu (SSH ou accès administrateur HTTPS/ASDM).
- Migration des règles : Transposer l'ensemble des règles de filtrage et de NAT de pfSense vers l'ASA.
- Services critiques : Configurer et tester les services réseau essentiels comme le DHCP relay et le NTP.
- Segmentation : Garantir la séparation stricte du réseau via les interfaces logiques (inside, outside).
- Pérennité : Assurer la sauvegarde et la capacité de restauration de la configuration de l'ASA.

• Moyens techniques

La migration repose sur l'utilisation des outils suivants :

- Infrastructure Source : Firewall pfSense sur une machine virtuelle.
- Infrastructure Cible : Firewall physique Cisco ASA.
- Administration : Logiciel Cisco ASDM pour la gestion graphique et terminal pour la ligne de commande (CLI).

Tableau d’adressage

Nom de l'équipement	Adresse IP	Masque	Passerelle
DEBIAN CLIENT	192.168.1.30	255.255.255.0	192.168.1.254
DEBIAN SRV	192.168.1.20	255.255.255.0	192.168.1.254
Oscar-GLPI	192.168.1.223	255.255.255.0	192.168.1.254
PC-CLIENT 1	192.168.2.10	255.255.255.0	192.168.1.254
PFsense	192.168.1.254	255.255.255.0	192.168.1.254
WIN-SRV-FICHIER	192.168.1.2	255.255.255.0	192.168.1.254
WinSRV	192.168.1.10	255.255.255.0	192.168.1.254
Switch Externe	192.168.1.1	255.255.255.0	192.168.1.254

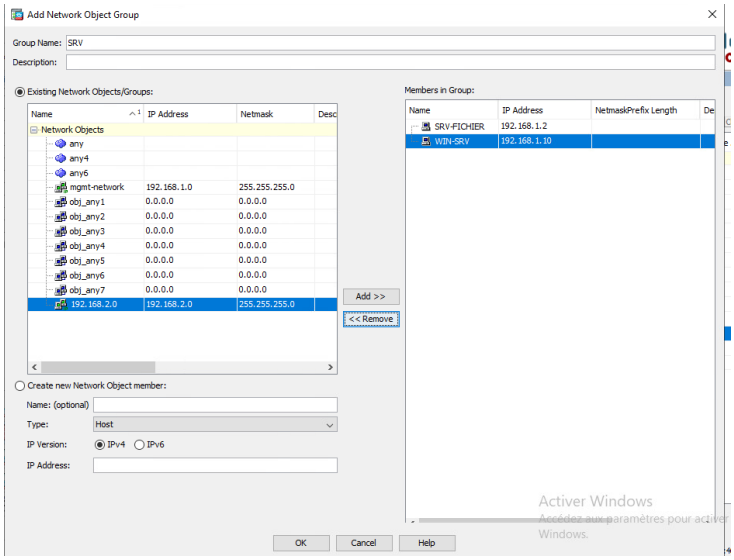
Solutions Techniques

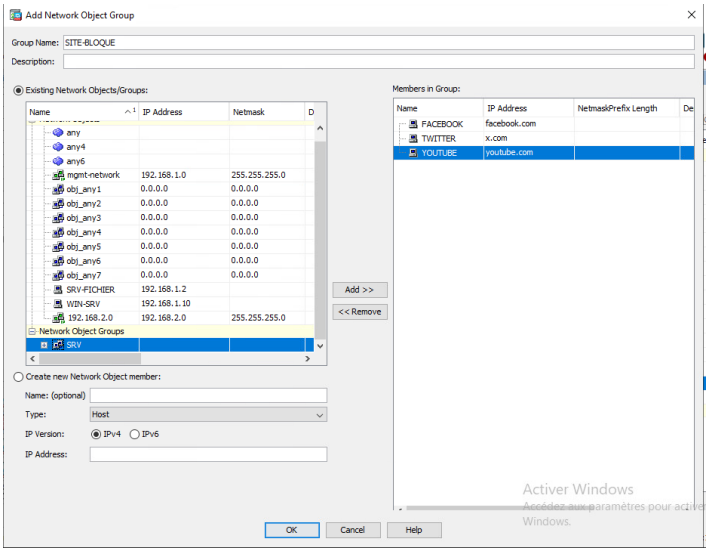
Les alias IP du pfSense ont été recréés sous forme de Network Objects.

SERVEURS : Regroupe les hôtes `192.168.1.10` et `192.168.1.2`.
FQDN Objects : Création d'objets pour `facebook.com`, `youtube.com`, etc., pour permettre un filtrage par nom de domaine.

Firewall Aliases IP

Name	Type	Values	Description	Actions
Bloque_ytb	Host(s)	youtube.com, www.youtube.com, ytimg.com, i.ytimg.com, youtube.googleapis.com	bloquer l'acces a youtube	
SERVEURS	Host(s)	192.168.1.10, 192.168.1.2	serveurs	
site_bloque	Host(s)	facebook.com, www.facebook.com, twitter.com, x.com, youtube.com, www.youtube.com, amazon.com, www.amazon.com	site bloqué	



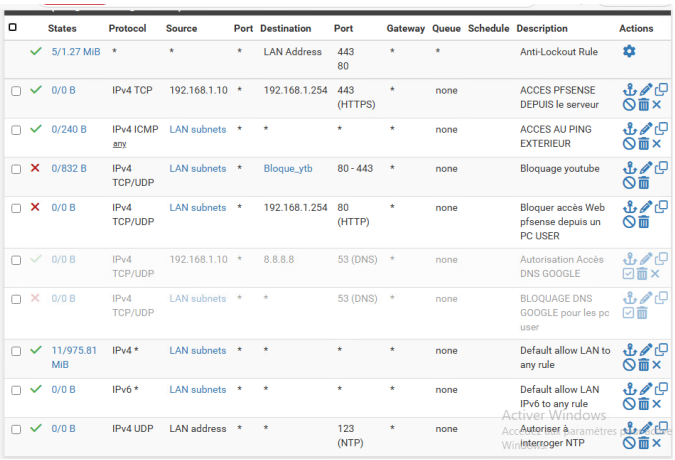


Conformément au cahier des charges, l'ASA a été configuré comme client DNS sur l'interface `outside` pour permettre la résolution des objets FQDN. Le service NTP a été activé pour garantir l'exactitude de l'horodatage des logs de sécurité.

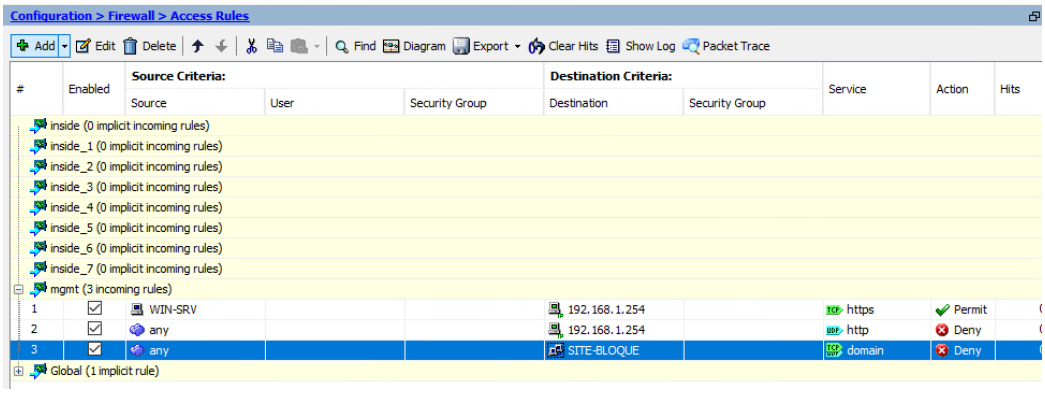
Le filtrage a été appliqué sur l'interface `inside` selon une logique de priorité haute vers basse :

Blocage Web : Les groupes `Bloque_ytb` et `site_bloque` sont interdits en tête de liste.

Accès Management : Autorisation du flux HTTPS (443) du serveur vers l'ASA.
Flux DNS/NTP : Autorisation des requêtes vers les serveurs de temps et les résolveurs DNS.
NAT Sortant : Mise en place d'une règle de Dynamic PAT pour l'accès internet global.



	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	5/1.27 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
	0/0 B	IPv4 TCP	192.168.1.10	*	192.168.1.254	443 (HTTPS)	*	none		ACCES PFSENSE DEPUIS le serveur	
	0/240 B	IPv4 ICMP any	LAN subnets	*	*	*	*	none		ACCES AU PING EXTERIEUR	
	0/832 B	IPv4 TCP/UDP	LAN subnets	*	Bloque_ytb	80 - 443	*	none		Bloquage youtube	
	0/0 B	IPv4 TCP/UDP	LAN subnets	*	192.168.1.254	80 (HTTP)	*	none		Bloquer accès Web pfsense depuis un PC USER	
	0/0 B	IPv4 TCP/UDP	192.168.1.10	*	8.8.8.8	53 (DNS)	*	none		Autorisation Accès DNS GOOGLE	
	0/0 B	IPv4 TCP/UDP	LAN subnets	*	*	53 (DNS)	*	none		BLOQUAGE DNS GOOGLE pour les pc user	
	11/975.81 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	
	0/0 B	IPv4 UDP	LAN address	*	*	123 (NTP)	*	none		Autoriser à interroger NTP	



Configuration > Firewall > Access Rules

Add | Edit | Delete | Find | Diagram | Export | Clear Hits | Show Log | Packet Trace

#	Enabled	Source Criteria: Source	User	Security Group	Destination Criteria: Destination	Security Group	Service	Action	Hits
inside (0 implicit incoming rules)									
inside_1 (0 implicit incoming rules)									
inside_2 (0 implicit incoming rules)									
inside_3 (0 implicit incoming rules)									
inside_4 (0 implicit incoming rules)									
inside_5 (0 implicit incoming rules)									
inside_6 (0 implicit incoming rules)									
inside_7 (0 implicit incoming rules)									
mgmt (3 incoming rules)									
1	☑	WIN-SRV			192.168.1.254		https	Permit	
2	☑	any			192.168.1.254		http	Deny	
3	☑	any			SITE-BLOQUE		domain	Deny	
Global (1 implicit rule)									

La migration vers le Cisco ASA 5506 répond à toutes les exigences du cahier des charges. La segmentation réseau est effective et les services critiques (DHCP/NTP) sont opérationnels. La configuration a été sauvegardée dans la mémoire `startup-config` de l'équipement, garantissant la restauration du service en cas de redémarrage.