

FICHE PROCEDURE

Extension du Proxy Squid au Site B via Tunnel IPsec

Champ	Valeur
Auteur	CHADHOULI EL-Anrif — BTS SIO SISR, 2ème année
Établissement	MEWO Metz
Date	Mars 2026
Version	1.0
Objet	Routage du trafic web des clients Site B vers le proxy Squid DMZ Site A
Durée estimée	30 à 45 minutes

Contexte et objectif

Le proxy Squid (avec SSL Bumping) est hébergé sur SRV-WEB-01 (10.11.3.2, DMZ Site A). Les clients du Site B doivent utiliser ce proxy pour accéder à Internet, tout en passant par le tunnel IPsec Site-à-Site déjà opérationnel.

Prérequis

- Tunnel IPsec IKEv2 Site A / Site B en état Established
- SRV-WEB-01 opérationnel — Squid actif sur 10.11.3.2:3127
- Certificat racine « Squid Proxy CA » exporté en .cer
- Accès administrateur à pfSense-01, pfSense-02 et SRV-WEB-01
- Poste CL-WIN11-02 (Site B) sous Windows 11

ARCHITECTURE — FLUX CIBLE

Élément	Réseau / IP	Rôle
pfSense-01	LAN : 10.11.3.17 — DMZ : 10.11.3.1	Pare-feu principal Site A
SRV-WEB-01	10.11.3.2 (DMZ)	Proxy Squid — port TCP 3127
pfSense-02	LAN : 10.11.4.17	Pare-feu Site B
CL-WIN11-02	LAN Site B — 10.11.4.16/28	Poste client Site B
Tunnel IPsec	IKEv2 AES-256 déjà en place	Transport chiffré inter-sites

Flux cible : CL-WIN11-02 → pfSense-02 → Tunnel IPsec → pfSense-01 → DMZ → 10.11.3.2:3127 (Squid) → Internet

ÉTAPE 1 — AJOUT DE LA PHASE 2 IPSEC (LAN SITE B ↔ DMZ SITE A)

Le tunnel existant couvre uniquement LAN Site A ↔ LAN Site B. Il faut ajouter un second sélecteur de trafic (Phase 2) pour couvrir le flux LAN Site B (10.11.4.16/28) ↔ DMZ Site A (10.11.3.0/28).

1.1 Sur pfSense-01 (Site A)

- Aller dans : VPN > IPsec > Tunnels
- Ouvrir le tunnel existant puis cliquer sur « Show Phase 2 Entries »
- Cliquer sur « Add P2 » pour ajouter une nouvelle entrée Phase 2
- Remplir les champs :

Mode	: Tunnel IPv4
Local Network	: 10.11.3.0/28 (DMZ Site A)
Remote Network	: 10.11.4.16/28 (LAN Site B)
Encryption	: AES 256 bits
Hash	: SHA256
PFS Key Group	: 14 (2048 bits)

- Sauvegarder → Apply Changes
- Vérifier dans Status > IPsec que les deux Phase 2 sont en Established

Status / IPsec / Overview							
Overview Leases SADs SPDs							
IPsec Status							
ID	Description	Local	Remote	Role	Timers	Algo	Status
con1 #319	IPsec Bât A vers Bât B	ID: 10.10.101.3 Host: 10.10.101.3:500 SPI: 729c4bc3cd02f810	ID: 10.10.101.4 Host: 10.10.101.4:500 SPI: 5903b87b304da600	IKEv2 Initiator	Rekey: 10802s (03:00:02) Reauth: Disabled	AES_CBC (256) HMAC_SHA2_256_128 PRF_HMAC_SHA2_256 MODP_2048	Established 15101 seconds (04:11:41) ago
ID	Description	Local	SPI(s)	Remote	Times	Algo	Stats
con1: #236	Multiple	10.11.3.16/28	Local: c053da53 Remote: cb3b5d4b	10.11.4.16/28	Rekey: 2155s (00:35:55) Life: 2751s (00:45:51) Install: 849s (00:14:09)	AES_CBC (256) HMAC_SHA2_256_128 MODP_2048 IPComp: None	Bytes-In: 593,466 (580 KiB) Packets-In: 6,818 Bytes-Out: 1,184,684 (1.13 MiB) Packets-Out: 8,709
							Installed

1.2 Sur pfSense-02 (Site B)

- Aller dans : VPN > IPsec > Tunnels
- Ouvrir le tunnel existant puis cliquer sur « Show Phase 2 Entries »
- Cliquer sur « Add P2 »
- Remplir les champs (miroir de pfSense-01) :

```

Mode                : Tunnel IPv4
Local Network       : 10.11.4.16/28      (LAN Site B)
Remote Network      : 10.11.3.0/28       (DMZ Site A)
Encryption          : AES 256 bits
Hash                : SHA256
PFS Key Group       : 14 (2048 bits)
  
```

- Sauvegarder → Apply Changes

IPsec Tunnels									
	ID	IKE	Remote Gateway	Auth/Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
☐	1	V2	WAN 10.10.101.3	Mutual PSK -	AES (256 bits)	SHA256	14 (2048 bit)	Tunnel vers bât A	
	ID	Mode	Local Subnet	Remote Subnet	P2 Protocol	P2 Transforms	P2 Auth Methods	Description	P2 actions
☐	1	tunnel	10.11.4.16/28	10.11.3.16/28	ESP	AES (256 bits)	SHA256	Routage AD vers AD	
☐	2	tunnel	LAN	10.11.3.0/28	ESP	AES (256 bits)	SHA256	Site B → Proxy Squid DMZ	

ÉTAPE 2 — RÈGLES DE PARE-FEU (ONGLET IPSEC)

Les règles IPsec sont évaluées après le déchiffrement du tunnel. Sans règle explicite, pfSense bloque le flux même si le tunnel est actif. Ces règles doivent être placées EN HAUT de l'onglet IPsec (avant toute règle générale).

2.1 Sur pfSense-01 (Site A) — Firewall > Rules > IPsec

- Cliquer sur « Add » (flèche vers le haut pour insérer en tête de liste)
- Configurer la règle principale :

Champ	Valeur
Action	Pass
Interface	IPsec
Protocole	TCP
Source	10.11.4.16/28 (LAN Site B)
Destination	10.11.3.2 (SRV-WEB-01)
Port destination	3127
Description	Site B → Proxy Squid DMZ

- Ajouter une seconde règle pour autoriser le DNS depuis la DMZ vers AD1 :

Champ	Valeur
Action	Pass
Interface	IPsec
Protocole	TCP/UDP
Source	10.11.3.2 (SRV-WEB-01)
Destination	10.11.3.18 (AD1)
Port destination	53
Description	Squid DMZ → DNS AD1

Floating	WAN	DMZ	LAN	IPsec	OpenVPN
----------	-----	-----	-----	-------	---------

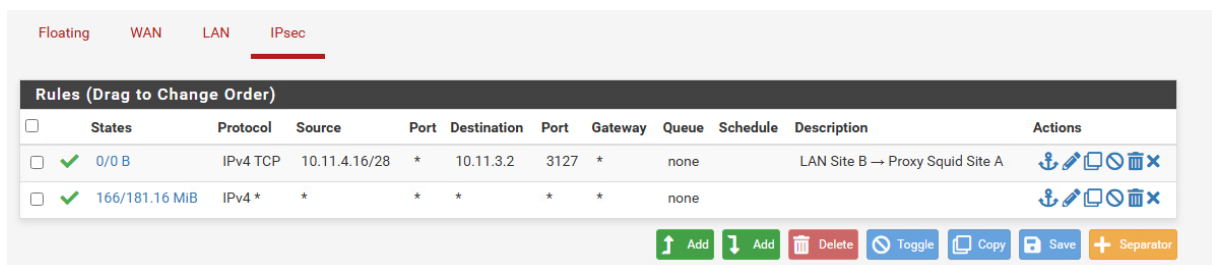
Rules (Drag to Change Order)											
☐	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓ 0/0 B	IPv4 TCP/UDP	10.11.3.2	*	10.11.3.18	53 (DNS)	*	none		Squid DMZ → DNS AD1	↕ ✎ 📄 🔄 🗑️ ✖
☐	✓ 0/0 B	IPv4 TCP	10.11.4.16/28	*	10.11.3.2	3127	*	none		Site B → Proxy Squid DMZ	↕ ✎ 📄 🔄 🗑️ ✖
☐	✓ 0/5.50 GiB	IPv4 *	*	*	*	*	*	none		IPsec Bât A vers Bât B	↕ ✎ 📄 🔄 🗑️ ✖

↑ Add	↓ Add	🗑️ Delete	🔄 Toggle	📄 Copy	💾 Save	+ Separator
-------	-------	-----------	----------	--------	--------	-------------

2.2 Sur pfSense-02 (Site B) — Firewall > Rules > IPsec

- Cliquer sur « Add » (insertion en tête de liste)
- Configurer la règle :

Champ	Valeur
Action	Pass
Interface	IPsec
Protocole	TCP
Source	10.11.4.16/28 (LAN Site B)
Destination	10.11.3.2 (SRV-WEB-01)
Port destination	3127
Description	LAN Site B → Proxy Squid Site A



ÉTAPE 3 — CONFIGURATION SQUID SUR SRV-WEB-01 (DEBIAN 12.5)

Par défaut, Squid n'autorise que les sous-réseaux déclarés dans ses ACL. Il faut ajouter explicitement le réseau du Site B pour l'autoriser à utiliser le proxy.

3.1 Édition du fichier squid.conf

- Se connecter en SSH sur SRV-WEB-01 :

```
ssh root@10.11.3.2
```

- Ouvrir le fichier de configuration :

```
nano /etc/squid/squid.conf
```

- Localiser la section ACL — repérer la ligne « http_access deny all »
- Ajouter les lignes AVANT http_access deny all :

```
# ACL — Sous-réseau Site B distant (via tunnel
IPsec)
acl site_b src 10.11.4.16/28
```

```
# Autorisation explicite du Site B
http_access allow site_b
```

- Vérifier que le port d'écoute couvre l'interface DMZ :

```
http_port 10.11.3.2:3127
```

- Si SSL Bumping est actif, vérifier la présence de cette configuration :

```
acl step1 at_step SslBump1
ssl_bump peek step1
ssl_bump bump site_b
ssl_bump splice all
```

3.2 Vérification et rechargement

- Tester la syntaxe du fichier avant rechargement :

```
squid -k parse
```

- Recharger Squid sans interruption de service :

```
squid -k reconfigure
```

- Vérifier que Squid est actif :

```
systemctl status squid
```

```
GNU nano 7.2 /etc/squid/squid.conf *
# =====
# CONFIGURATION SQUID - MODE MANUEL (GPO) + SSL BUMP
# Auteur : CHADHOULI EL-Anrif - BTS SIO SISR 2026
# Serveur : SRV-WEB-01 - 10.11.3.2 - Debian 12.5
# =====

# -----
# RESEAUX AUTORISES
# -----
acl networklan      src 10.11.3.16/28
acl site_b_lan      src 10.11.4.16/28
acl localhost        src 127.0.0.1/32
```

```

● squid.service - Squid Web Proxy Server
   Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enabled)
   Drop-In: /etc/systemd/system/squid.service.d
            └─override.conf
   Active: active (running) since Sun 2026-03-29 15:49:44 CEST; 30s ago
     Docs: man:squid(8)
  Process: 40558 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, status=0/SUCCESS)
    Main PID: 40566 (squid)
      Tasks: 9 (limit: 2305)
     Memory: 349.4M
        CPU: 1min 46.333s
    CGroup: /system.slice/squid.service
            └─40566 /usr/sbin/squid --foreground -sYC
              └─40572 "(squid-1)" --kid squid-1 --foreground -sYC
                ├─40573 "(security_file_certgen)" -s /var/lib/squid/ssl_db -M 4MB
                ├─40574 "(security_file_certgen)" -s /var/lib/squid/ssl_db -M 4MB
                ├─40575 "(security_file_certgen)" -s /var/lib/squid/ssl_db -M 4MB
                ├─40576 "(security_file_certgen)" -s /var/lib/squid/ssl_db -M 4MB
                ├─40577 "(security_file_certgen)" -s /var/lib/squid/ssl_db -M 4MB
                └─40578 "(logfile-daemon)" /var/log/squid/access.log
                  └─40579 "(pinger)"

mars 29 15:49:44 SRV-WEB-01 squid[40572]: Set Current Directory to /var/spool/squid
mars 29 15:49:44 SRV-WEB-01 squid[40572]: Finished loading MIME types and icons.
mars 29 15:49:44 SRV-WEB-01 squid[40572]: ALERT: initgroups: unable to set groups for User proxy and Group 13
mars 29 15:49:44 SRV-WEB-01 squid[40572]: HTCP Disabled.
mars 29 15:49:44 SRV-WEB-01 squid[40572]: Pinger socket opened on FD 25
mars 29 15:49:44 SRV-WEB-01 squid[40572]: Squid plugin modules loaded: 0
mars 29 15:49:44 SRV-WEB-01 squid[40572]: Adaptation support is off.
lines 1-29

```

ÉTAPE 4 — CONFIGURATION DU POSTE CLIENT CL-WIN11-02 (WINDOWS 11)

4.1 Import du certificat « Squid Proxy CA »

Ce certificat doit être importé dans le magasin de l'ORDINATEUR LOCAL (pas Utilisateur), sinon les applications système ne lui font pas confiance et des alertes SSL apparaîtront sur tous les sites HTTPS.

Méthode PowerShell (administrateur) :

- Copier le fichier squid-proxy-ca.cer sur le poste (clé USB, partage réseau...)
- Ouvrir PowerShell en tant qu'Administrateur
- Exécuter :

```

Import-Certificate `
    -FilePath "C:\squid-proxy-ca.cer" `
    -CertStoreLocation "Cert:\LocalMachine\Root"

```

- Vérifier que le certificat est bien importé :

```

Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like "*Squid*"}

```

```

PS C:\Users\Administrateur> Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like "*Squid*"}

PSParentPath : Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint                                     Subject
-----
01938C59EB250DBD199143BC47449B84F353F258    C=FR, O=Lab, CN=Squid Proxy CA

PS C:\Users\Administrateur>

```

Méthode manuelle (certlm.msc) :

- Appuyer sur Win + R → taper certlm.msc → Entrée
- Aller dans : Autorités de certification racines de confiance > Certificats
- Clic droit → Toutes les tâches → Importer...
- Suivre l'assistant — sélectionner le fichier .cer
- Choisir le magasin : Ordinateur local → Autorités de certification racines de confiance
- Finaliser l'import

4.2 Configuration du proxy système

Méthode graphique :

- Ouvrir Paramètres Windows → Réseau et Internet → Proxy
- Désactiver « Détecter automatiquement les paramètres »
- Activer « Utiliser un serveur proxy »
- Adresse : 10.11.3.2 — Port : 3127
- Exceptions (ne pas proxifier) : localhost;127.*;10.11.4.*
- Cliquer sur Enregistrer

Modifier le serveur proxy

Utiliser un serveur proxy

☒ Activé

Adresse IP du proxy

10.11.3.2

Port

3127

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

☐ Ne pas utiliser le serveur proxy pour les adresses (intranet) locales

Enregistrer

Annuler

Méthode PowerShell :

```
$proxy = "10.11.3.2:3127"
$bypass = "localhost;127.*;10.11.4.*"
$path =
"HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings"

Set-ItemProperty -Path $path -Name ProxyEnable -
Value 1
Set-ItemProperty -Path $path -Name ProxyServer
Value $proxy
Set-ItemProperty -Path $path -Name ProxyOverride -
Value $bypass
```

ÉTAPE 5 — TESTS DE VALIDATION

5.1 Test de connectivité vers le proxy

- Ouvrir PowerShell sur CL-WIN11-02
- Exécuter :

```
Test-NetConnection -ComputerName 10.11.3.2 -Port 3127
```

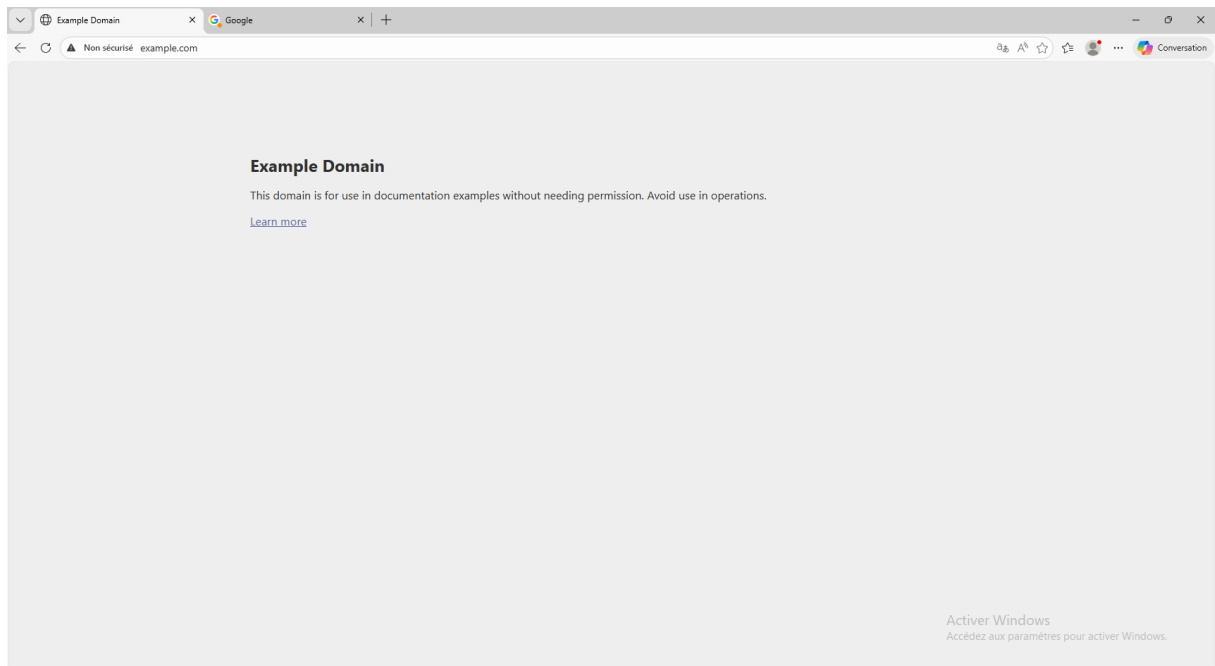
- Résultat attendu : TcpTestSucceeded = True

```
PS C:\Users\Administrateur> Test-NetConnection -ComputerName 10.11.3.2 -Port 3127

ComputerName      : 10.11.3.2
RemoteAddress     : 10.11.3.2
RemotePort        : 3127
InterfaceAlias    : Ethernet0
SourceAddress     : 10.11.4.22
TcpTestSucceeded  : True
```

5.2 Test de navigation HTTP

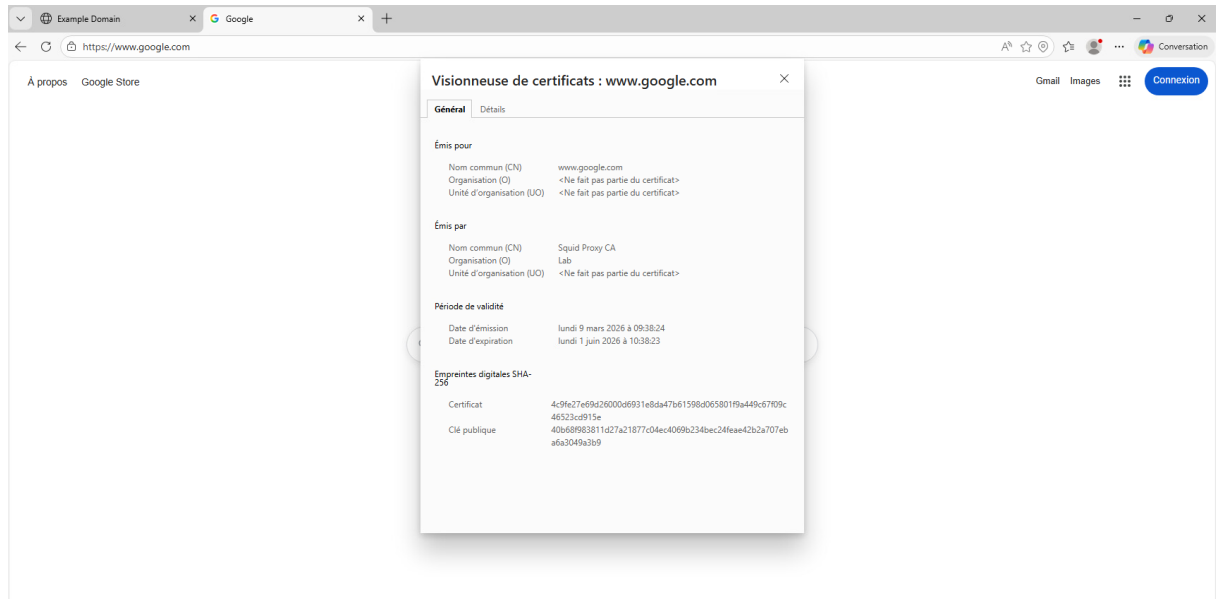
- Ouvrir un navigateur web sur CL-WIN11-02 (proxy configuré)
- Accéder à <http://example.com>
- La page doit s'afficher normalement



5.3 Test de navigation HTTPS (validation du certificat Squid Proxy CA)

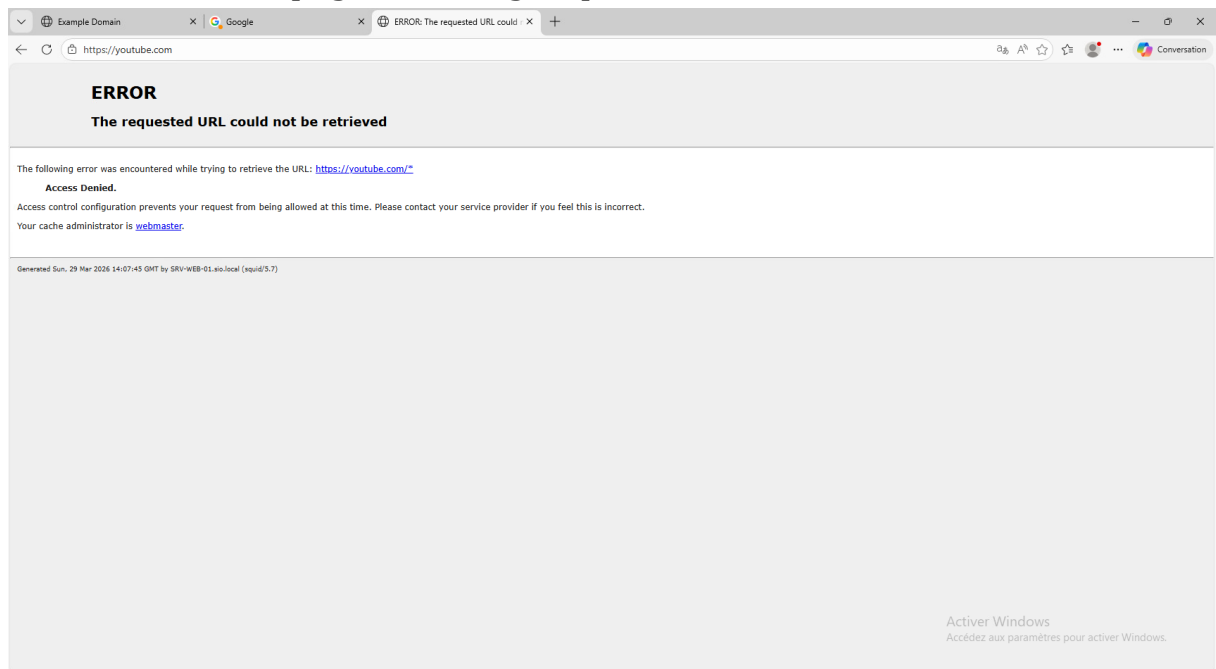
- Accéder à <https://www.google.com>

- Aucune alerte de sécurité SSL ne doit apparaître
- Dans la barre d'adresse : cliquer sur le cadenas → certificat émis par « Squid Proxy CA »



5.4 Test de blocage d'un site filtré

- Accéder à <https://www.youtube.com>
- Résultat attendu: page de blocage Squid « Access Denied »



5.5 Vérification des journaux Squid (SRV-WEB-01)

- Sur SRV-WEB-01, vérifier les logs d'accès en temps réel :

```
tail -f /var/log/squid/access.log
```

- Les requêtes provenant de 10.11.4.16/28 doivent apparaître dans les logs

```
root@SRV-WEB-01:~# tail -f /var/log/squid/access.log
1774793370.635 0 - TCP_DENIED/403 3168 GET http://www.microsoft.com/pki/certs/MicRooCerAut2011.2011.03.22.crt - HIER_NONE/- text/html
1774793370.653 99 10.11.4.22 NONE_NONE/200 0 CONNECT settings-win.data.microsoft.com:443 - HIER_NONE/- -
1774793370.183 0 - TCP_DENIED/403 3168 GET http://www.microsoft.com/pki/certs/MicRooCerAut2011.2011.03.22.crt - HIER_NONE/- text/html
1774793370.196 184 10.11.4.22 NONE_NONE/200 0 CONNECT settings-win.data.microsoft.com:443 - HIER_NONE/- -
1774793370.482 240 10.11.4.22 NONE_NONE/200 0 CONNECT fern.xboxservices.com:443 - HIER_DIRECT/20.71.22.186 -
1774793370.565 70 10.11.4.22 TCP_MISS/200 680 GET https://fern.xboxservices.com/GameBarFD/Experimentation/Anon? - HIER_DIRECT/20.71.22.186 application/json
1774793370.768 0 - TCP_DENIED/403 3168 GET http://www.microsoft.com/pki/certs/MicRooCerAut2011.2011.03.22.crt - HIER_NONE/- text/html
1774793370.778 530 10.11.4.22 NONE_NONE/200 0 CONNECT settings-win.data.microsoft.com:443 - HIER_NONE/- -
1774793371.442 327 10.11.4.22 NONE_NONE/200 0 CONNECT dlassets-ssl.xboxlive.com:443 - HIER_DIRECT/23.58.192.8 -
1774793371.540 97 10.11.4.22 TCP_MISS/200 638271 GET https://dlassets-ssl.xboxlive.com/public/content/kg1/Version/2662/kg1.2662.compressed - HIER_DIRECT/23.58.192.8 application/octet-stream
1774793410.483 6 10.11.4.22 TCP_DENIED/200 0 CONNECT youtube.com:443 - HIER_NONE/- -
```

VALIDATION FINALE : INFRASTRUCTURE OPERATIONELLE

La procédure d'extension du proxy Squid au Site B est désormais complète et validée. Les clients du Site B accèdent à Internet exclusivement via le proxy Squid hébergé en DMZ du Site A, au travers du tunnel IPsec chiffré AES-256. Le filtrage HTTPS est actif grâce au SSL Bumping et au certificat « Squid Proxy CA » déployé sur les postes clients. L'ensemble des flux est journalisé dans les logs d'accès Squid, garantissant la traçabilité complète de la navigation.

CHADHOULI EL-Anrif — BTS SIO SISR 2026 — MEWO Metz

Document confidentiel — Usage interne