PROCÉDURE TECHNIQUE · BTS SIO SISR

Déploiement d'un proxy Artica avec filtrage HTTPS et configuration par GPO

Installer Artica, déchiffrer et filtrer le trafic HTTPS, puis imposer le proxy et son certificat aux postes du domaine ngrange.local.

Auteur	Plot 1
Contexte	TP réalisé en équipe — Plot 1, domaine ngrange.local
Version	2.0 — novembre 2026
Environnement	Artica 4.50 SP10 (Debian 13, proxy Squid) · Windows Server (AD, GPO) · poste client Windows 11 · hyperviseur Proxmox
Durée estimée	2 h

Identifiants d'accès — Plot 1

Machine / service	Adresse	Identifiant	Mot de passe
SRV-ARTICA (console)	https://192.168.21.5:9000	`sio2`	`Azerty13.`
SRV-AD1EX / SRV-AD2	192.168.21.1 / .2	`NGRANGE\administrateur`	`Azerty13.`
PC-CLIENT	192.168.21.10	`sio2`	`Azerty13.`

À savoir

Les captures proviennent du TP réalisé en équipe : les adresses et noms visibles peuvent différer ; les valeurs à utiliser sont celles du texte (Plot 1).

Sommaire

1. Objectif
2. Architecture et prérequis
3. Installer et initialiser Artica
4. Mettre à jour et ajouter les services
5. Créer l'autorité ca-root
6. Activer le déchiffrement SSL
7. Redémarrer et contrôler le proxy
8. Distribuer ca-root par GPO
9. Installer le filtrage Web et bloquer un domaine
10. Imposer et verrouiller le proxy par GPO
11. Vérification
12. Dépannage
13. Sécurité et bonnes pratiques
14. Aide-mémoire : Artica Proxy au quotidien

1. Objectif

Mettre en place un proxy Artica qui contrôle la navigation Web du domaine `ngrange.local`. Le résultat attendu :

- le trafic HTTP et HTTPS des postes transite par le proxy `192.168.21.5:3128` ;
- le proxy déchiffre le HTTPS (inspection SSL) avec sa propre autorité `ca-root`, de confiance sur tous les postes grâce à une GPO ;
- un domaine de test est bloqué et affiche la page de refus d'Artica ;
- l'utilisateur ne peut pas contourner ni modifier le réglage du proxy.

L'inspection HTTPS est une interception volontaire : chaque poste doit donc **faire confiance à l'autorité** qui signe les certificats générés par le proxy, sinon le navigateur affichera une erreur de certificat sur chaque site.

2. Architecture et prérequis

Équipement	Adresse IP	Rôle
Contrôleurs de domaine (`SRV-AD1EX` VMID 201, `SRV-AD2` VMID 202)	192.168.21.1 · 192.168.21.2	Active Directory et DNS
Artica (`SRV-ARTICA.ngrange.local` , VMID 205)	192.168.21.5	Proxy et filtrage
Client de test (`PC-CLIENT` , VMID 210)	192.168.21.10	Poste Windows membre du domaine
pfSense	192.168.21.254	Passerelle

Paramètre	Valeur
Réseau	192.168.21.0/24
Domaine	`ngrange.local`
Console d'administration	`https://192.168.21.5:9000`
Proxy (port d'écoute de production)	`192.168.21.5:3128`
Ressources de la VM Artica	2 vCPU · 5 Go de RAM · 30 Go de disque · 1 carte réseau sur le LAN 192.168.21.0/24

Prérequis : ISO Artica disponible dans Proxmox ; accès administrateur au contrôleur de domaine (console `gpmc.msc`) ; un poste client joint au domaine ; accès Internet via pfSense pour les mises à jour ; une OU contenant les comptes utilisateurs et une OU contenant les comptes ordinateurs (exemple : OU `USER-PLOT1` , nom d'exemple à adapter à l'OU réelle de Plot 1).

À savoir

Le déroulé ci-dessous suit un ordre logique : le déchiffrement SSL est activé **avant** le téléchargement de ca-root (l'original renvoyait vers des sections ultérieures). Le port interne `62097` (127.0.0.1) est réservé à Artica : ne pas le modifier.

3. Installation et configuration

Partie A — Artica

1 Créer la VM et installer Artica

Dans Proxmox, créer une VM aux ressources du tableau précédent, carte réseau sur le LAN `192.168.21.0/24`. Monter l'ISO Artica, démarrer et terminer l'installation. Après le premier redémarrage, **éjecter l'ISO** pour éviter de relancer l'installeur.

2 Lancer l'assistant de configuration

Depuis un poste du réseau, ouvrir `https://192.168.21.5:9000` (accepter l'avertissement du certificat auto-signé), choisir le français puis renseigner :

Champ	Valeur
Nom d'hôte	`SRV-ARTICA`
Domaine	`ngrange.local`
Adresse IP fixe	`192.168.21.5/24`
DNS	`192.168.21.1` puis `192.168.21.2` (les contrôleurs de domaine)
Passerelle	`192.168.21.254`

À l'étape « activité principale », sélectionner **Service Proxy**, valider et attendre la fin de la préparation automatique. Un serveur proxy doit garder une adresse fixe : les postes la référencent par GPO.

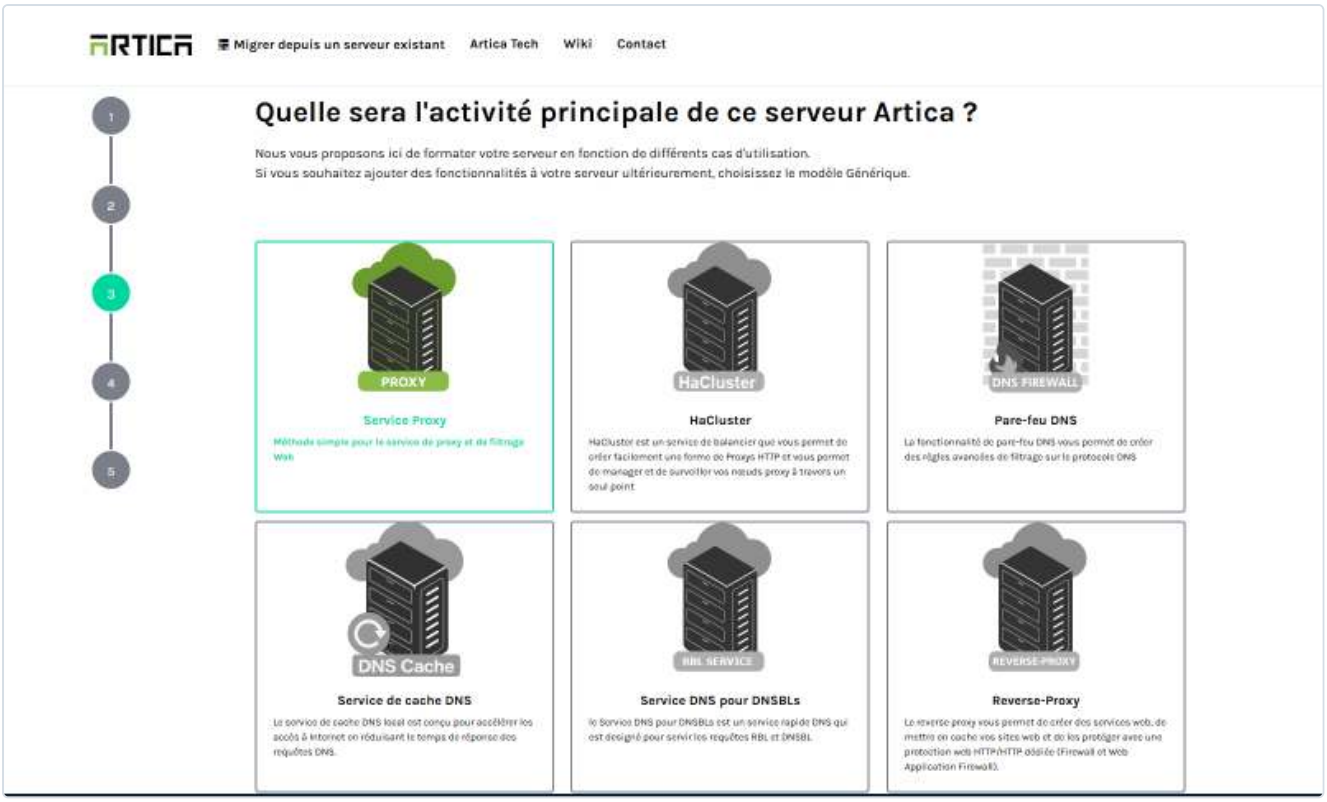

Figure 1 – Choix de l'activité « Service Proxy » dans l'assistant Artica

3 Contrôler le tableau de bord

Attendre que la préparation automatique soit terminée avant toute modification : intervenir pendant cette phase peut corrompre la configuration. Le tableau de bord doit s'afficher sans erreur réseau.

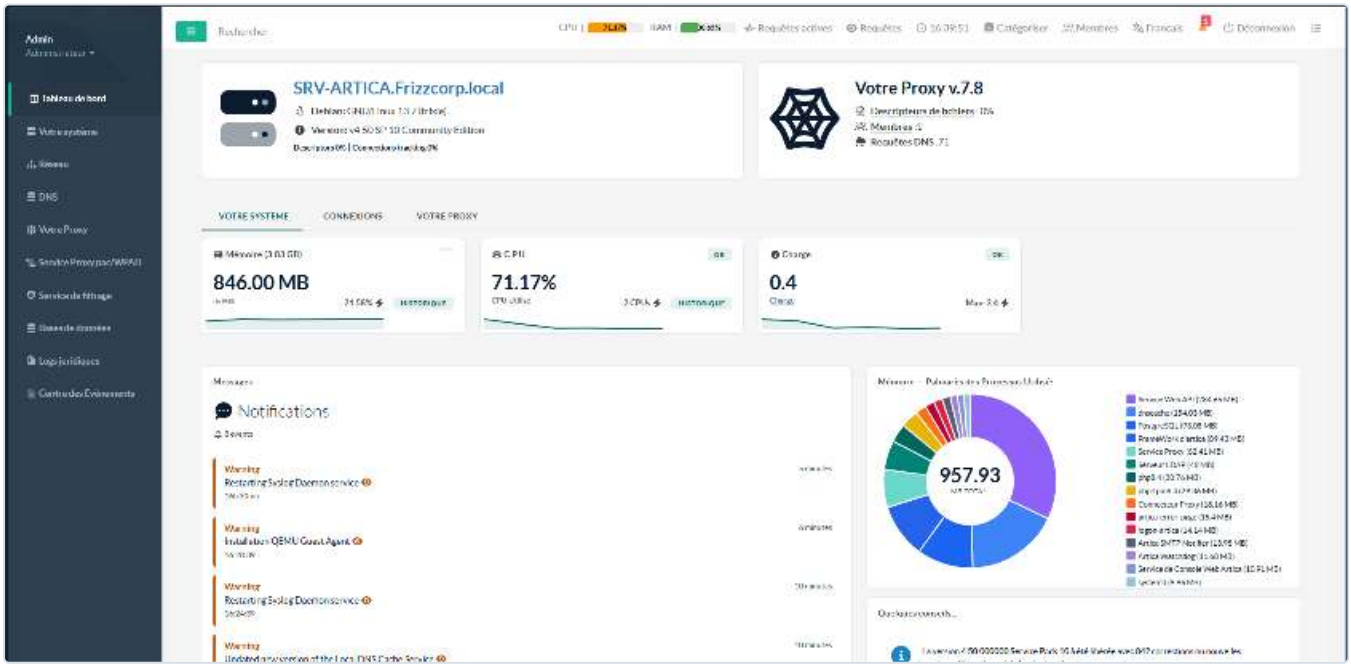

Figure 2 – Tableau de bord d'Artica après installation (Debian 13, Artica 4.50 SP10)

4 Mettre à jour et installer les deux services

Le proxy reçoit les connexions des navigateurs ; le service de filtrage applique les règles d'accès. Ce sont deux composants distincts, à installer l'un après l'autre.

1. *Votre système* > *Mise à jour* : rechercher les mises à jour, lancer l'installation et attendre 100 %.
2. *Votre système* > *Fonctionnalités* : rechercher puis installer **Proxy service**, puis **Service de filtrage**.

Les menus *Votre Proxy* et *Service de filtrage* apparaissent alors dans la colonne de gauche.

Partie B — Autorité ca-root et déchiffrement SSL

5 Créer le certificat racine ca-root

L'inspection HTTPS exige une autorité de certification qui signe les certificats présentés aux clients. Dans *Votre système* > *Centre des certificats*, conserver le certificat `SRV-ARTICA` créé automatiquement, puis cliquer sur **Nouveau certificat racine auto-signé** :

Champ	Valeur
Nom du certificat	`ca-root` (nom repris dans Artica et dans la GPO)
Nom commun (CN)	`SRV-ARTICA.ngrange.local`
Noms alternatifs	`SRV-ARTICA.ngrange.local` · `192.168.21.5` · `artica`
Pays / région / localité	FRANCE / PACA / Marseille
Organisation / unité	SIO / Plot 1
Niveau de chiffrement	RSA 4096 (SHA-256)
Durée de validité	3650 jours (10 ans)

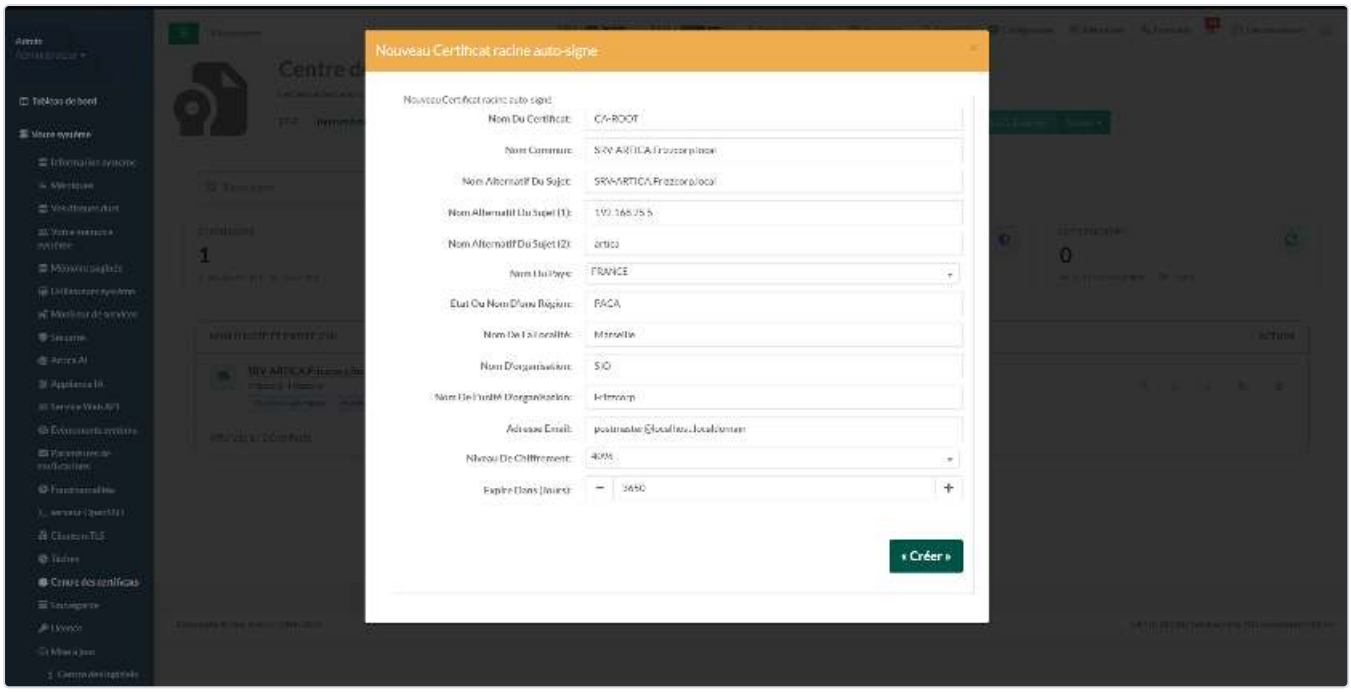

Figure 3 – Formulaire de création du certificat racine ca-root

Attention

Deux certificats portent désormais le même nom commun. Seul `ca-root` sert à l'inspection SSL ; le certificat automatique reste en place mais ne doit pas être déployé par GPO.

6 Associer ca-root au port 3128

Cette association indique au proxy quelle autorité utiliser pour signer les certificats déchiffrés. Dans *Votre Proxy* > *Ports d'écoute*, vérifier que le port de production `3128` existe avec l'état OK, puis :

1. Cliquer sur **Activer le déchiffrement SSL** et choisir un certificat déjà présent.
2. Dans la liste, cliquer sur **Sélectionner** en face de `ca-root` (et non du certificat automatique).
3. Cliquer sur **Appliquer**.

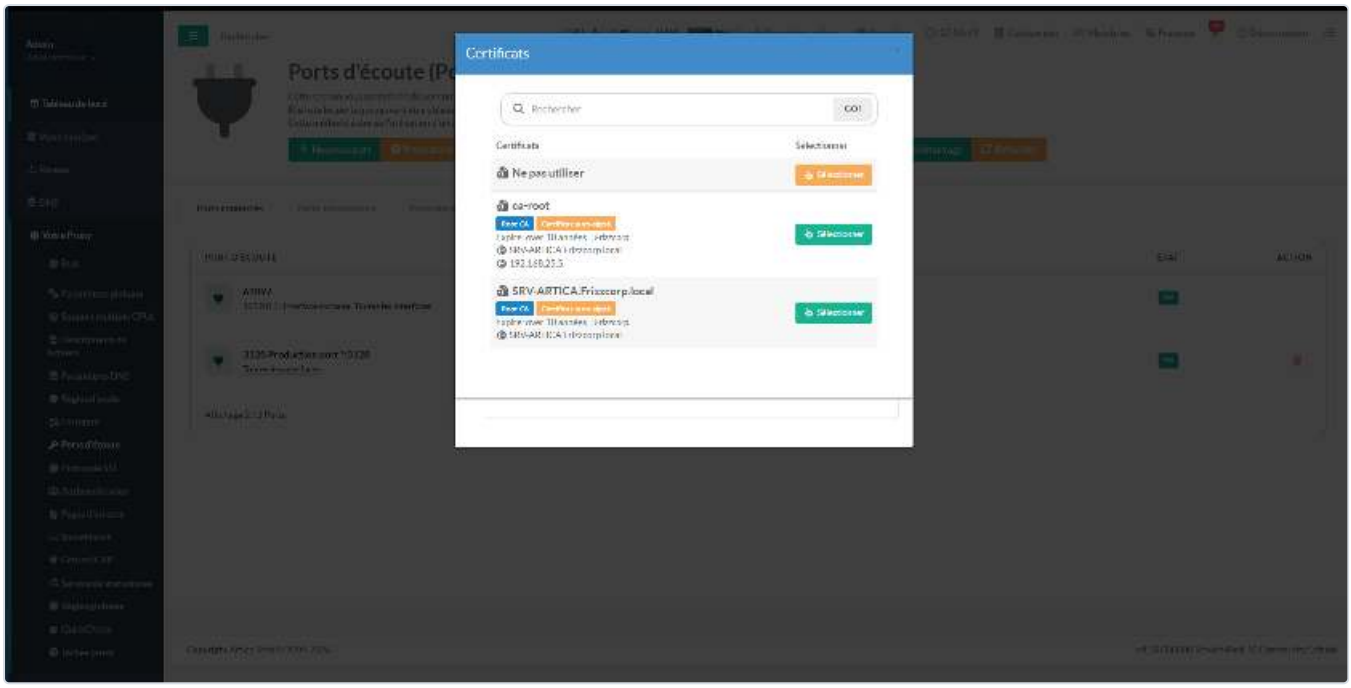

Figure 4 – Liste des certificats : sélectionner ca-root, pas le certificat automatique

7 Appliquer la configuration et contrôler les ports

Le redémarrage recharge les paramètres enregistrés. Cliquer sur **Configurer les ports & redémarrage**, attendre la fin de la barre de progression sans fermer la page, puis cliquer sur **Rafraîchir**. Un état « ÉCHEC » transitoire est normal pendant la reconstruction ; seul l'état final compte. Contrôler que le port interne `62097` et le port `3128` affichent **OK**, le second avec l'étiquette « Déchiffrement SSL » et le certificat `ca-root`.

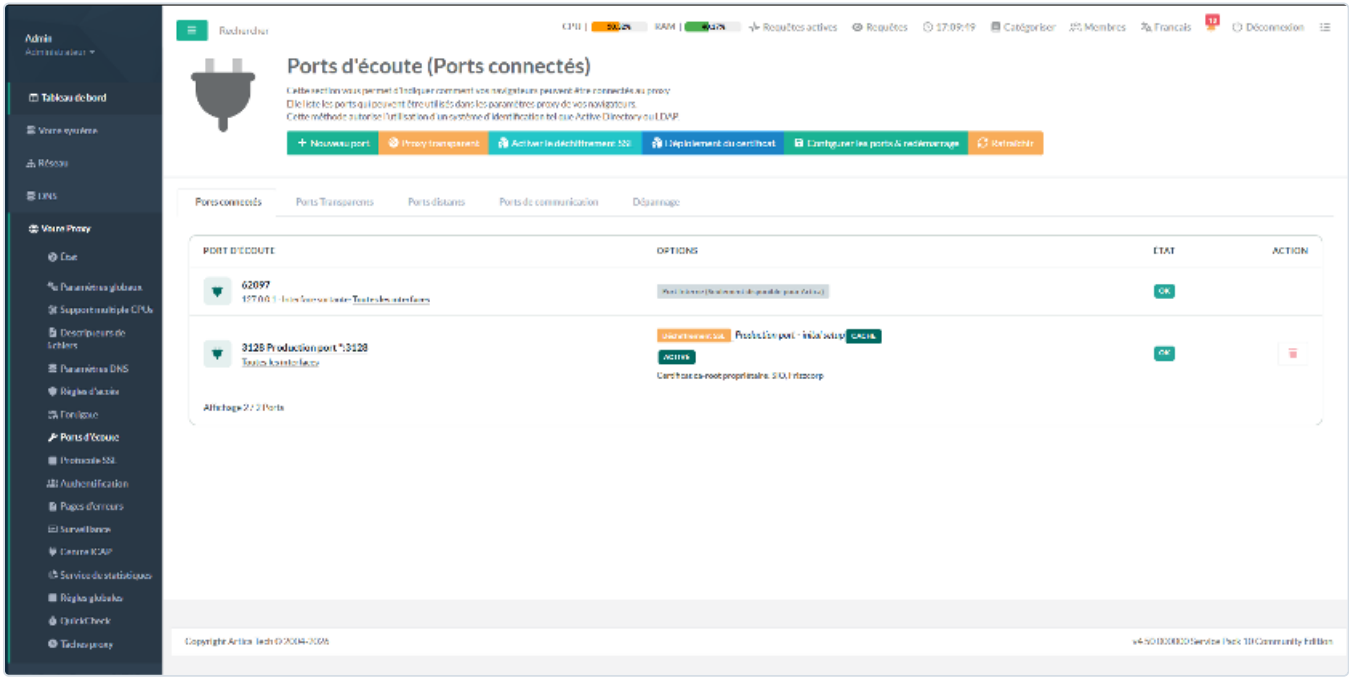

Figure 5 – Port 3128 opérationnel avec déchiffrement SSL et certificat ca-root

8 Télécharger le certificat public ca-root.crt

Ouvrir *Votre Proxy* > *Protocole SSL*, puis **Liste des certificats** dans la zone de déploiement. Sur la ligne `ca-root` associée au port 3128, cliquer sur l'icône de téléchargement de la colonne **CRT** et enregistrer `ca-root.crt`. La colonne PS1 fournit un script d'installation : elle n'est pas utilisée ici, l'import se fait par GPO. Ne pas télécharger la ligne `SRV-ARTICA.ngrange.local` marquée « Pas utilisé ». Copier ensuite le fichier sur le contrôleur de domaine.

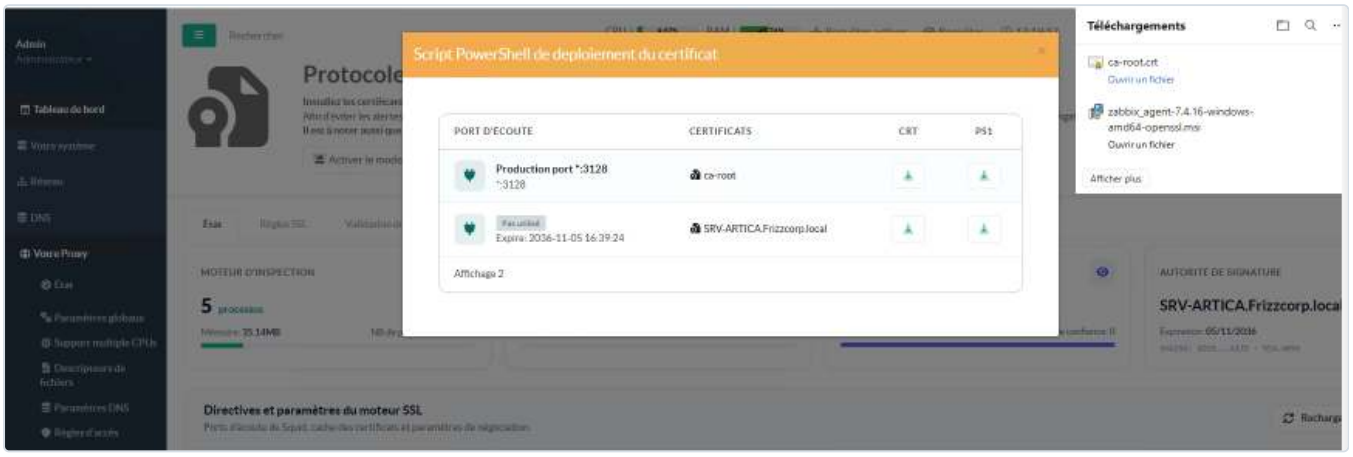

Figure 6 – Téléchargement du fichier CRT de ca-root, utilisé par le port 3128

Relever dès maintenant l'empreinte du fichier, pour la comparer plus tard avec celle du certificat déployé (les deux certificats portant le même nom, l'empreinte est le seul critère fiable) :

```
certutil -hashfile ca-root.crt SHA1
```

Partie C — Distribution du certificat par GPO

9 Créer et lier la GPO « Déploiement Certificat Artica »

Une GPO distribue un réglage aux objets de son périmètre. Le certificat est un réglage de **configuration ordinateur** : la GPO doit donc être liée à une OU qui contient les **comptes ordinateurs** (vérifier dans *Utilisateurs et ordinateurs Active Directory* que le PC client y figure).

1. Sur le contrôleur de domaine, ouvrir `gpmc.msc` et sélectionner l'OU des ordinateurs.
2. Clic droit > *Créer un objet GPO dans ce domaine, et le lier ici* ; nommer la GPO `Déploiement Certificat Artica`.
3. Vérifier que *Lien activé* est coché, puis clic droit > *Modifier*.

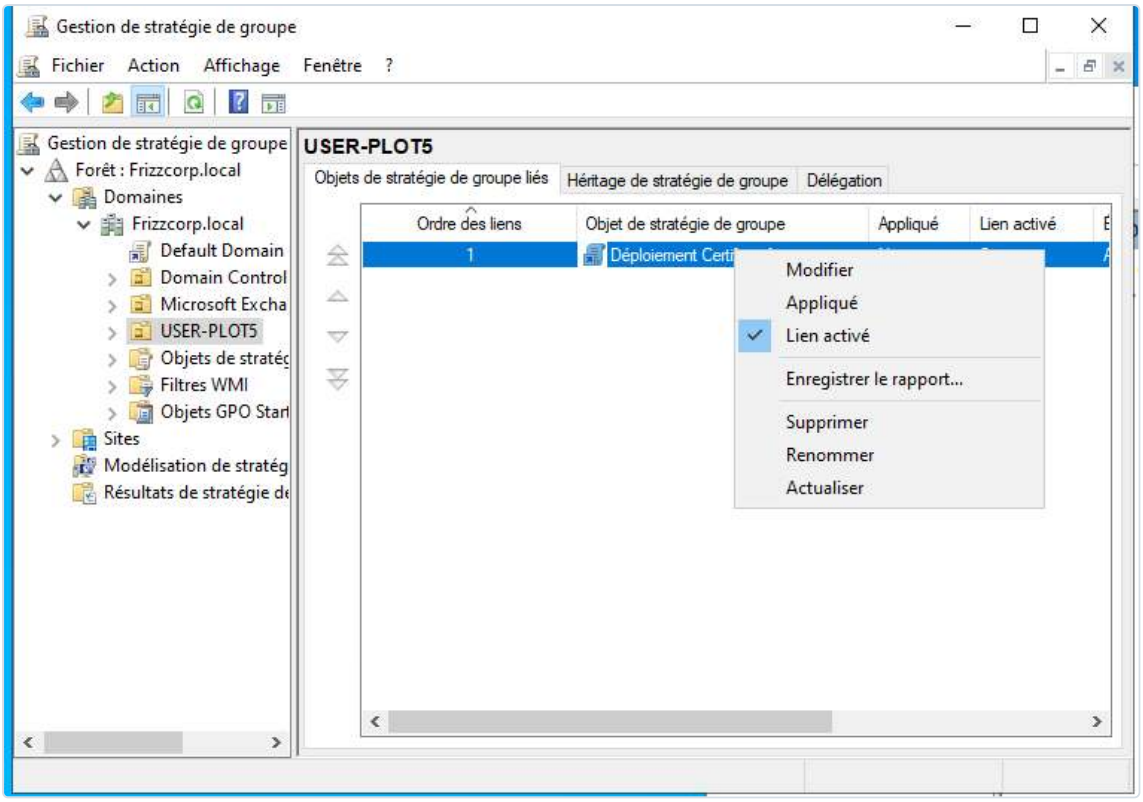

Figure 7 – GPO liée à l'OU, option « Lien activé » cochée

10 Importer ca-root dans les autorités racines de confiance

Le magasin des autorités racines indique à Windows quelles autorités reconnaître : c'est ce qui supprime les erreurs de certificat lors de l'inspection.

1. Éditeur de GPO : *Configuration ordinateur* > *Stratégies* > *Paramètres Windows* > *Paramètres de sécurité* > *Stratégies de clé publique*.
2. Clic droit sur *Autorités de certification racines de confiance* > *Importer*.
3. Choisir `ca-root.crt`, conserver le magasin *Autorités de certification racines de confiance*, terminer l'assistant.
4. Ouvrir le certificat importé et comparer son empreinte avec celle du fichier. Windows l'affiche sous son nom commun `SRV-ARTICA.ngrange.local`, non sous le libellé « ca-root ».

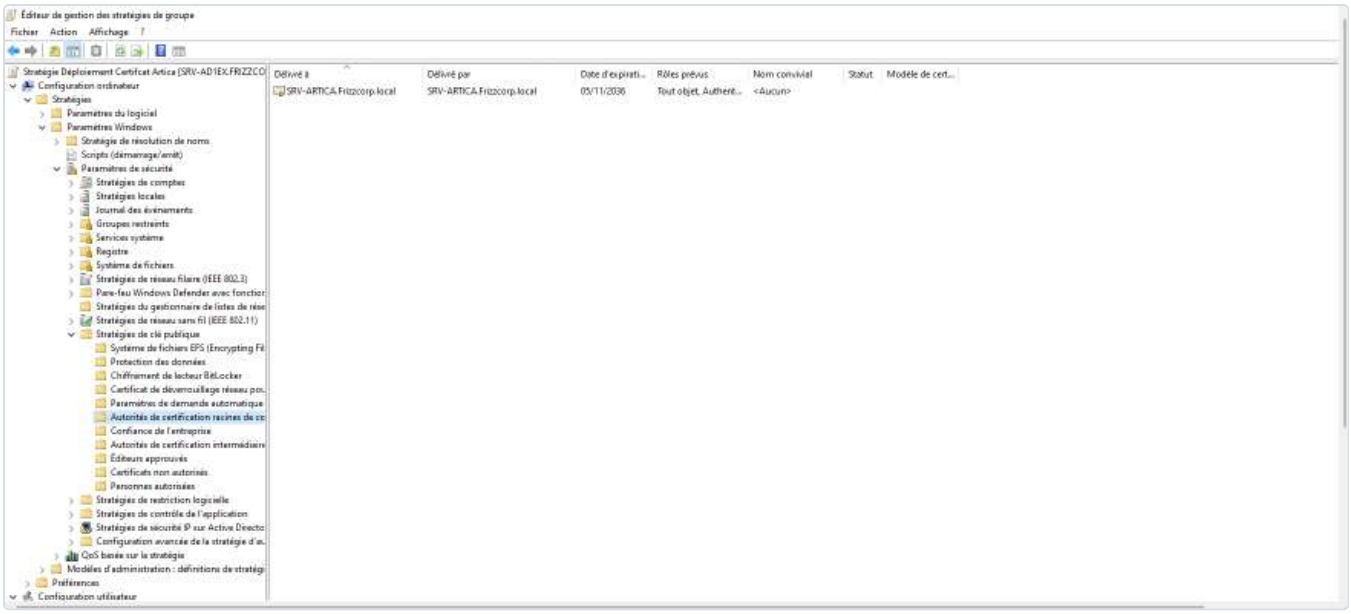

Figure 8 – Certificat importé dans le magasin des autorités racines de la GPO

Partie D — Filtrage Web

11 Installer le service de filtrage Web

La tuile **Service de filtrage Web** est distincte du service de filtrage général déjà actif. Dans *Service de filtrage > Fonctionnalités*, repérer la tuile affichée « Désactivé », cliquer sur **Installation** et attendre la fin de la progression (le service peut redémarrer seul). Rafraîchir et vérifier qu'elle n'est plus désactivée.

À l'issue de l'installation, le service indique 0 catégorie : aucune base de catégories n'est chargée. Cela n'empêche pas de bloquer un domaine par règle explicite, utilisée à l'étape suivante.

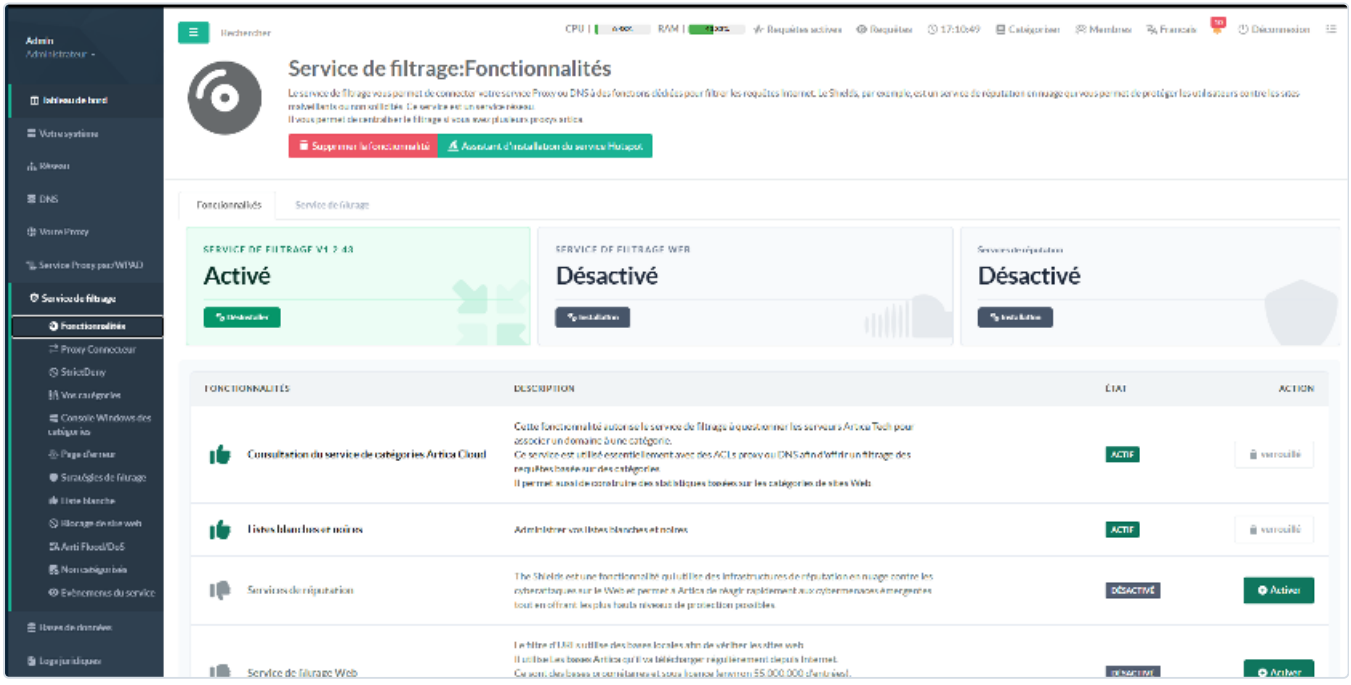

Figure 9 – Service de filtrage Web encore désactivé, avant installation

12 Bloquer un domaine de test

Choisir un domaine de test et le conserver pour la validation (le TP utilise `rassemblementnational.fr`). Dans *Service de filtrage* > *Blocage de site web* :

1. Cliquer sur **Domaines** et saisir le domaine **sans** `https://` ni chemin, puis valider.
2. Vérifier qu'il apparaît dans la liste.
3. Cliquer sur **Appliquer les paramètres** : la règle n'est transmise au service qu'à ce moment. Attendre la fin de la barre « Construction des paramètres ».

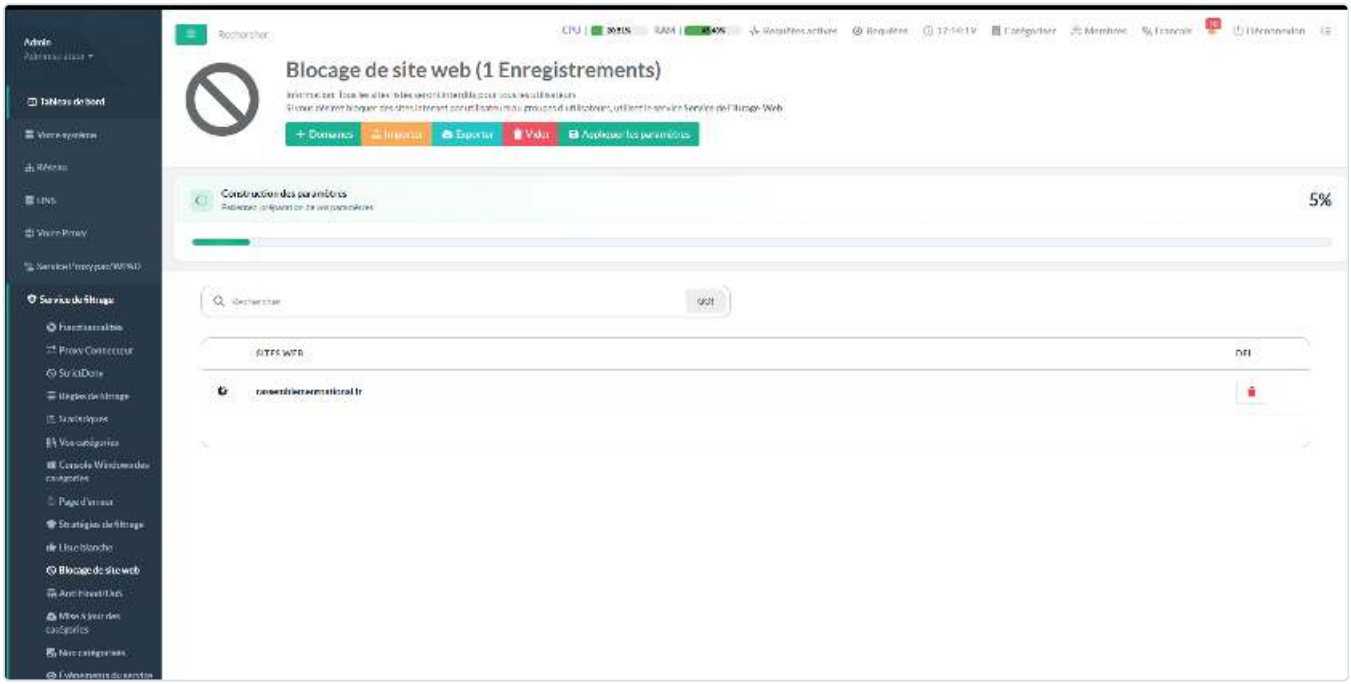

Figure 10 – Domaine ajouté à la liste de blocage et application des paramètres en cours

Partie E — Configuration et verrouillage du proxy par GPO

13 Créer la GPO « Configuration Proxy Artica »

Cette GPO configure la **session de l'utilisateur** : la lier à l'OU contenant les comptes utilisateurs concernés. Le poste doit être joint au domaine et la session ouverte avec un compte de ce périmètre.

1. Dans `gpmc.msc`, sur l'OU des utilisateurs : créer et lier la GPO `Configuration Proxy Artica`, vérifier *Lien activé*, puis *Modifier*.
2. Aller dans *Configuration utilisateur* > *Préférences* > *Paramètres du Panneau de configuration* > *Paramètres Internet*.
3. Clic droit dans la zone vide > *Nouveau* > *Internet Explorer 10* : cette préférence règle le proxy système Windows, repris par Edge et Chrome.

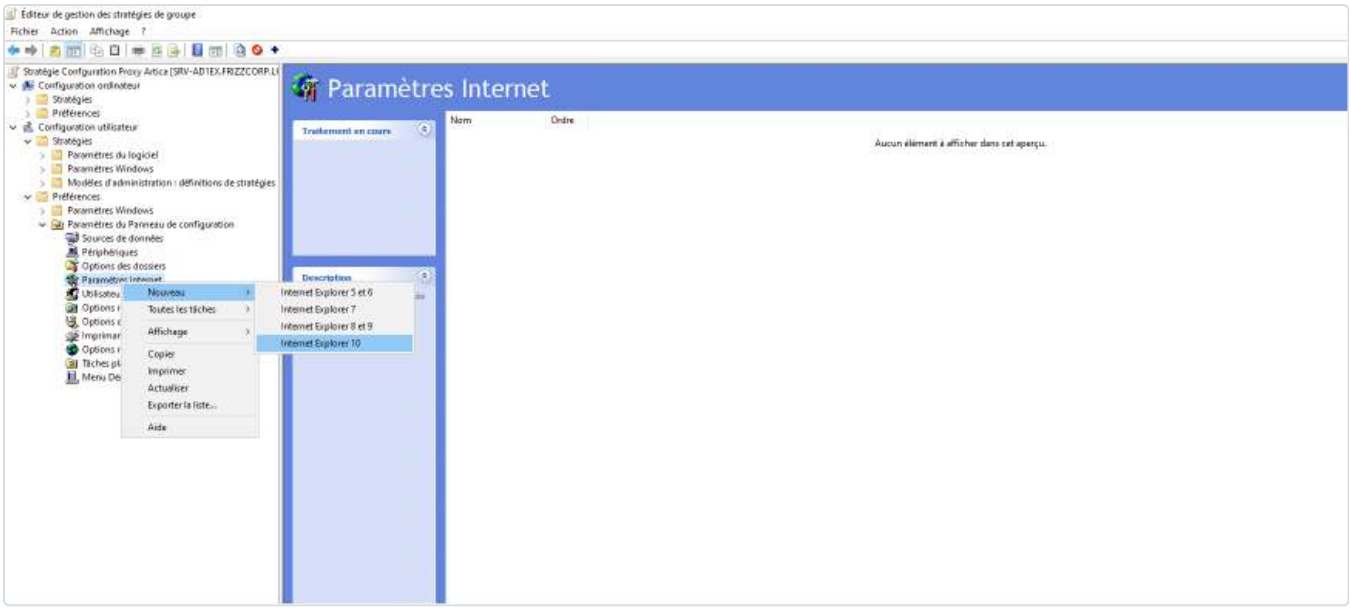

Figure 11 – Création de la préférence « Internet Explorer 10 » dans les paramètres Internet

14 Renseigner l'adresse du proxy

1. Onglet *Connexions* > *Paramètres réseau*.
2. Cocher *Utiliser un serveur proxy* ; saisir `192.168.21.5` dans *Adresse* et `3128` dans *Port* (sans `https://`).
3. Cocher *Ignorer le serveur proxy pour les adresses locales* (noms courts uniquement). Dans *Avancé*, ajouter dans le champ d'exceptions les noms internes complets, par exemple `*.ngrange.local;192.168.21.*` *(exemple à adapter)*.
4. Appuyer sur **F5** : les champs actifs passent en soulignement **vert**, ce qui signifie qu'ils seront transmis par la GPO. Valider avec OK, puis OK dans la fenêtre principale.

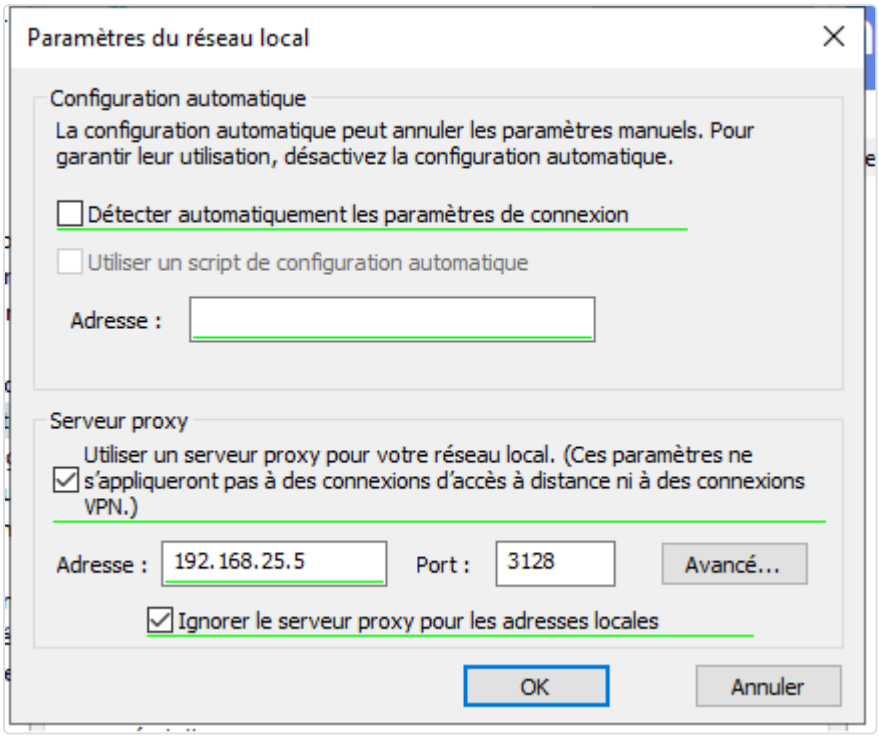

Figure 12 – Adresse et port du proxy renseignés dans la préférence GPO

> **Attention**
> Contrôler l'adresse exacte `192.168.21.5` et le port `3128` : une faute de frappe coupe la navigation de tous les utilisateurs du périmètre.

15 Verrouiller le réglage

La préférence renseigne le proxy mais n'interdit pas à l'utilisateur de le modifier. Dans la **même OU**, créer et lier une seconde GPO (`GPO Proxy Verrouillage`), puis :

1. *Modifier* > *Configuration utilisateur* > *Stratégies* > *Modèles d'administration* > *Composants Windows* > *Internet Explorer*.
2. Ouvrir **Empêcher la modification des paramètres du proxy**, choisir *Activé*, valider.

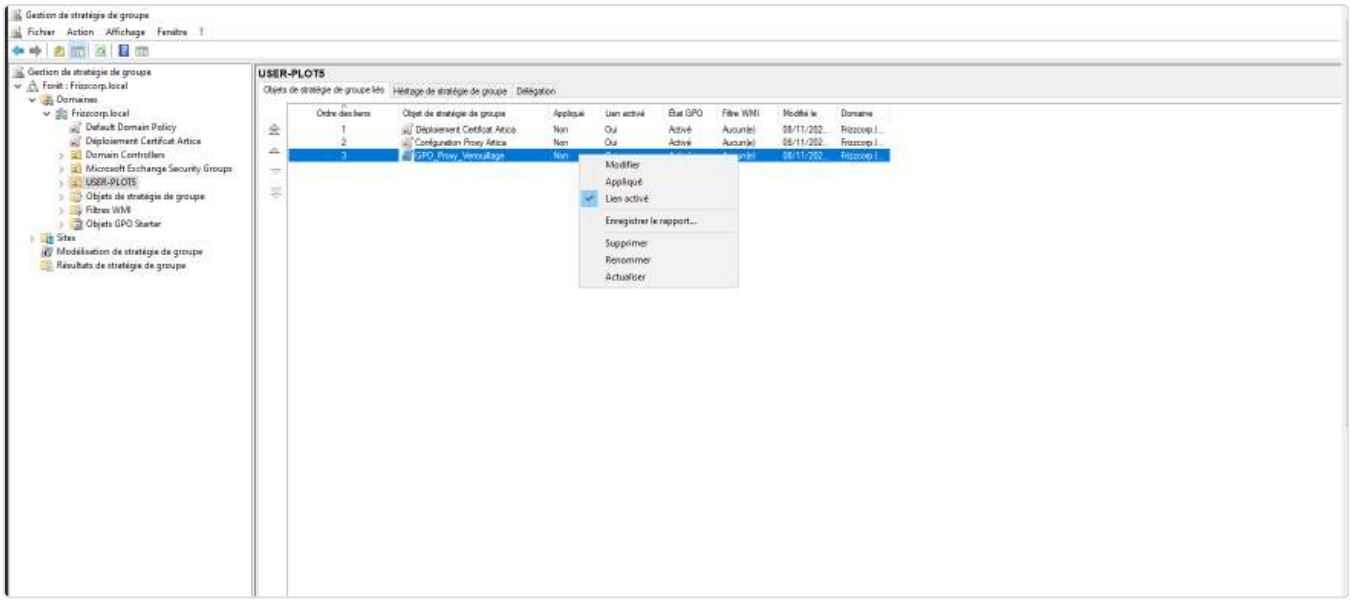

Figure 13 – Les trois GPO liées à l'OU des utilisateurs (certificat, configuration, verrouillage)

> **À savoir**
> Dans le TP, les trois GPO sont toutes liées à l'OU `USER-PLOT1` *(nom d'exemple)*. La GPO du certificat étant un réglage ordinateur, elle ne s'applique que si les comptes ordinateurs sont dans cette OU : sinon, la lier à l'OU des ordinateurs (ou activer le traitement en boucle, *loopback*).

4. Vérification

Effectuer les contrôles sur le client de test (`192.168.21.10`), dans une session d'utilisateur du domaine.

16 Appliquer les stratégies et contrôler le client

```
gpupdate /force
:: fermer la session ou redémarrer, puis rouvrir la session

gpresult /r /scope user                 :: GPO utilisateur appliquées
gpresult /r /scope computer             :: GPO ordinateur appliquées
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings" /v
ProxyServer
Test-NetConnection 192.168.21.5 -Port 3128      # PowerShell
certutil -hashfile ca-root.crt SHA1             :: empreinte du fichier d'origine
```

Contrôler aussi graphiquement : `certlm.msc` > *Autorités de certification racines de confiance* > *Certificats* (comparer l'empreinte avec celle de `ca-root.crt`) et *Paramètres Windows* > *Réseau et Internet* > *Proxy* (adresse `192.168.21.5` , port `3128`).

17 Tester la navigation et le blocage

Ouvrir un site autorisé, puis le domaine placé en liste de blocage. Conserver une capture de chaque résultat. Test en ligne de commande, qui montre aussi l'émetteur du certificat :

```
curl.exe -vI -x http://192.168.21.5:3128 https://www.google.com 2>&1 | findstr /i
"issuer HTTP/"
```

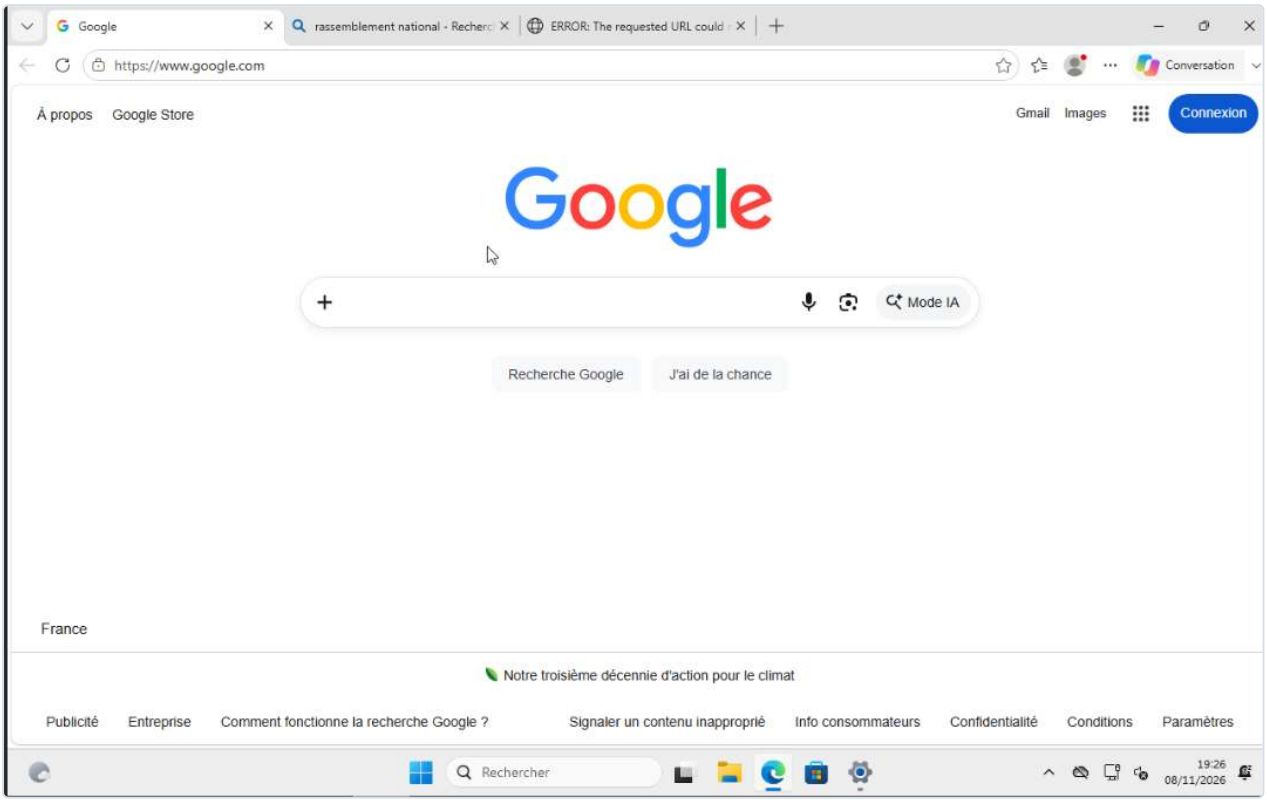

Figure 14 – Site autorisé : la navigation passe par le proxy

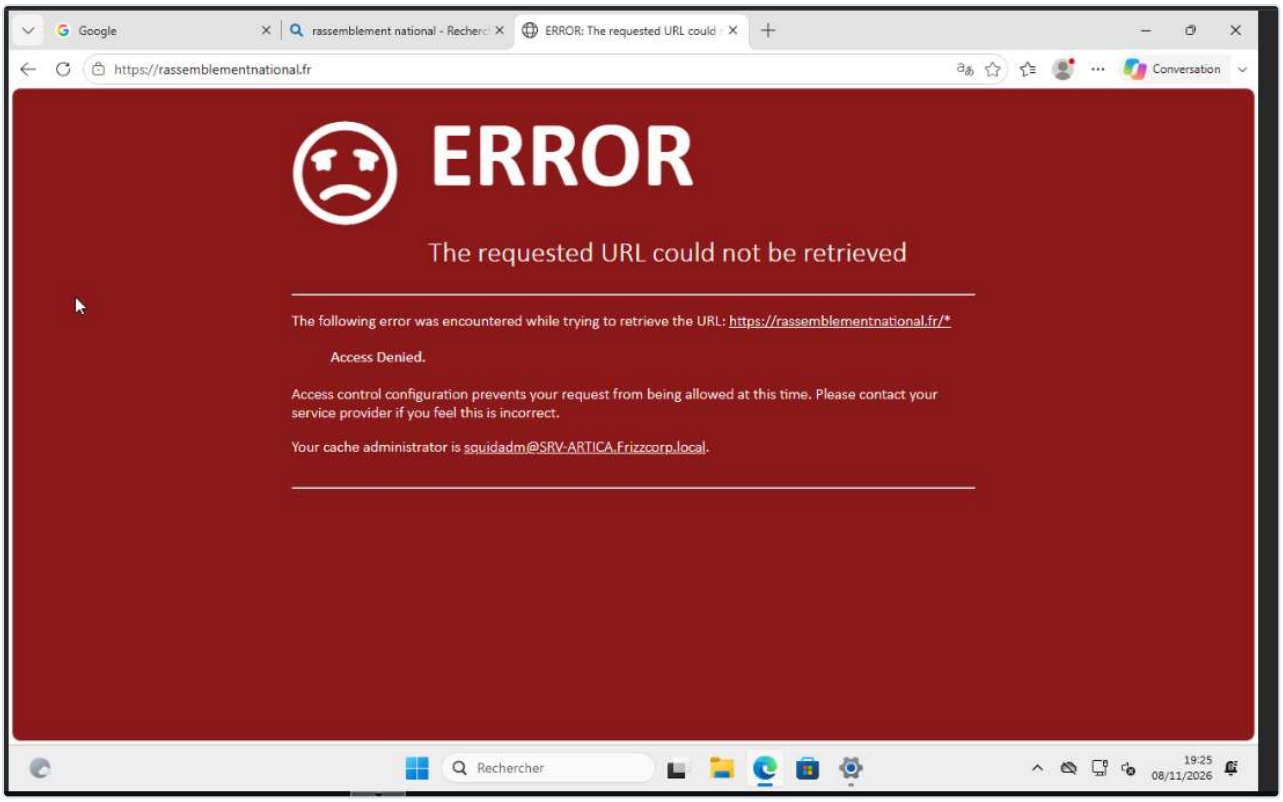

Figure 15 – Domaine bloqué : page « Access Denied » générée par Artica

Résultat attendu

Le proxy 192.168.21.5:3128 est appliqué et grisé (non modifiable) ; l'empreinte du certificat de la GPO correspond à `ca-root.crt` ; un site autorisé s'ouvre sans erreur de certificat, avec `ca-root` comme émetteur ; le domaine bloqué affiche la page de refus d'Artica (« Access Denied »).

5. Dépannage

Symptôme	Cause probable	Solution
Console inaccessible sur le port 9000	VM éteinte, IP différente, ISO encore montée	Contrôler la console Proxmox, l'IP `192.168.21.5` et éjecter l'ISO
Port 3128 en état ÉCHEC	Redémarrage encore en cours, ou configuration incomplète	Attendre la fin de la reconstruction puis *Rafraîchir* ; relancer *Configurer les ports & redémarrage*
Erreur de certificat (NET::ERR_CERT_AUTHORITY_INVALID) sur les sites HTTPS	ca-root non déployé, GPO non appliquée, ou mauvais certificat associé au port	Vérifier `gpresult /r /scope computer`, l'OU des ordinateurs et que le port 3128 utilise bien `ca-root`
Erreur de certificat seulement dans Firefox	Firefox utilise son propre magasin de certificats	Activer `security.enterprise_roots.enabled` (`about:config`) ou déployer la stratégie correspondante
Le poste n'utilise pas le proxy	GPO utilisateur non appliquée (mauvaise OU, session non rouverte)	`gpupdate /force`, nouvelle session, `gpresult /r /scope user`
Le domaine bloqué reste accessible	Paramètres non appliqués, cache du navigateur, ou trafic hors proxy	Cliquer sur *Appliquer les paramètres*, tester en navigation privée, vérifier le proxy actif
Les ressources internes passent par le proxy et échouent	Exceptions locales absentes	Compléter *Avancé* : `*.ngrange.local;192.168.21.*` *(exemple)*
Le service de filtrage Web affiche 0 catégorie	Base de catégories non téléchargée (normal après installation)	Utiliser le blocage par domaine, ou charger les catégories via le menu *Mise à jour des catégories*

6. Sécurité et bonnes pratiques

- Protéger la **clé privée de ca-root** : elle permet de signer n'importe quel certificat accepté par tous les postes. Limiter l'accès à la console Artica (port 9000) aux administrateurs et ne jamais exporter la clé.
- Ne distribuer que le certificat public (`.crt`), jamais la clé privée.

- Informer les utilisateurs de l'inspection HTTPS et exclure du déchiffrement les sites sensibles (banque, santé) selon la politique de l'organisation et le cadre légal (RGPD, charte informatique).
- Empêcher le contournement du proxy *(recommandation, non réalisée dans le TP)* : sur pfSense, n'autoriser les flux HTTP/HTTPS sortants du LAN que depuis `192.168.21.5`.
- Changer le mot de passe administrateur Artica par défaut, tenir l'appliance à jour et sauvegarder sa configuration.
- Planifier le renouvellement de ca-root avant l'expiration (3650 jours après la création) et redéployer le nouveau certificat par GPO.
- Tester toute modification de GPO sur un poste pilote avant la généralisation.

7. Aide-mémoire : utiliser Artica Proxy au quotidien

Référence rapide des gestes courants. Les entrées de menu citées sont celles visibles dans l'interface du TP (Artica 4.50 SP10) ; l'organisation exacte des écrans et des onglets peut varier selon la version, les passages marqués *« à vérifier »* sont à confirmer dans votre interface. Console : `https://192.168.21.5:9000`.

Ajouter des règles de filtrage Web

- **Bloquer un domaine pour tous** : *Service de filtrage* > *Blocage de site web* > *Domaines* (domaine sans `https://`), puis **Appliquer les paramètres** (voir étape 12).
- **Autoriser quoi qu'il arrive** : *Service de filtrage* > *Liste blanche* : y ajouter le domaine ; elle sert aux exceptions (site métier bloqué par erreur).
- **Filtrer par catégories ou par groupes d'utilisateurs** : *Service de filtrage* > *Règles de filtrage* (création d'une règle, choix des catégories à bloquer, puis association aux objets ou groupes concernés, éventuellement via *Stratégies de filtrage*) ; *à vérifier* selon la version. Les catégories nécessitent le **Service de filtrage Web** installé et ses bases chargées (*Mise à jour des catégories*).
- Personnaliser le message affiché au refus : *Service de filtrage* > *Page d'erreur*.

> **À savoir**
> Le blocage de site web s'applique à tous les utilisateurs. Pour cibler un groupe, passer par les règles de filtrage. Toujours terminer par **Appliquer** et vérifier depuis un poste client.

Authentification Active Directory / LDAP

Menu *Votre Proxy* > *Authentification* : choisir la méthode (Active Directory ou LDAP) et renseigner le domaine `ngrange.local`, le contrôleur `192.168.21.1` et un compte de liaison dédié (droits en lecture seule). Conditions : Artica utilise le DNS `192.168.21.1`, son heure est synchronisée avec le contrôleur (écart faible, requis par Kerberos), le compte de liaison a un mot de passe sans expiration. Après enregistrement, utiliser **Configurer les ports & redémarrage** (*Votre Proxy* > *Ports d'écoute*) pour recharger le proxy, puis tester avec un compte du domaine.

> **Attention**
> L'authentification oblige chaque navigateur à présenter des identifiants ; le proxy transparent et les applications sans gestion d'authentification (mises à jour, agents) échouent alors. À prévoir dans les exceptions.

Déployer le proxy sur les postes

Méthode	Mise en œuvre
GPO (retenue au TP)	Préférence Paramètres Internet + GPO de verrouillage : étapes 13 à 15
WPAD / PAC	Menu *Service Proxy.pac/WPAD* : publier un fichier PAC (*à vérifier*) ; faire résoudre `wpad.ngrange.local` vers `192.168.21.5` dans le DNS de l'AD ; sur le poste, activer « Détecter automatiquement les paramètres de connexion » ou indiquer l'adresse du script PAC
Manuel (test)	*Paramètres Windows* > *Réseau et Internet* > *Proxy* > *Configuration manuelle* : `192.168.21.5` , port `3128`
Applications système	Les services Windows (WinHTTP) ont leur propre réglage

```
netsh winhttp set proxy 192.168.21.5:3128
netsh winhttp show proxy
netsh winhttp reset proxy
```

Consulter les journaux et les statistiques

- Barre supérieure de la console : **Requêtes actives** et **Requêtes** (trafic en temps réel).
- *Votre Proxy* > *Service de statistiques* et *Surveillance* : volumétrie, sites et utilisateurs les plus actifs.
- *Service de filtrage* > *Statistiques* et *Évènements du service* : blocages et rechargements du filtrage.
- Menu *Centre des Évènements*, *Évènements système* et *Logs juridiques* (journaux de connexion conservés au titre de la conservation légale).

Si l'accès SSH à l'appliance est ouvert, journal d'accès Squid, emplacement habituel (*à vérifier*) :

```
tail -f /var/log/squid/access.log
grep rassemblementnational /var/log/squid/access.log | tail
```

Inspection SSL / HTTPS (prudence)

Activation, certificat `ca-root` et déploiement : étapes 5 à 10. Pour exclure des sites du déchiffrement (banque, santé, applications qui épinglent leur certificat), utiliser *Votre Proxy* > *Protocole SSL*, onglet **Règles SSL** (*à vérifier*), puis **Configurer les ports & redémarrage**. Désactiver le déchiffrement du port 3128 ramène à un simple filtrage par nom de domaine (sans erreur de certificat).

> **Attention**
> Le déchiffrement donne accès au contenu des échanges chiffrés : informer les utilisateurs, limiter l'accès aux journaux et respecter le RGPD et la charte informatique.

Mises à jour

- **Artica** : *Votre système* > *Mise à jour* : rechercher, installer, attendre 100 % ; prévoir une sauvegarde ou un snapshot Proxmox avant.
- **Catégories de filtrage** : *Service de filtrage* > *Mise à jour des catégories*.
- **Fonctionnalités** : *Votre système* > *Fonctionnalités* (installation et suppression des services).

Sauvegarde de la configuration

Menu *Votre système* > *Sauvegarde* : créer une sauvegarde de la configuration, la télécharger ou l'envoyer vers un emplacement externe à la VM (*à vérifier* : options exactes selon la version). Compléter par une sauvegarde de la VM entière depuis Proxmox (`vzdump <vmid> --storage <stockage> --mode snapshot --compress zstd`) avant toute mise à jour importante. Conserver aussi le **certificat ca-root** (sans sa clé en clair hors coffre) : sa perte obligerait à redéployer un nouveau certificat sur tous les postes.

Raccourcis et emplacements utiles

Élément	Valeur ou emplacement
Console d'administration	`https://192.168.21.5:9000`
Proxy de production · port interne	`192.168.21.5:3128` · `127.0.0.1:62097` (réservé à Artica)
Ports, SSL, authentification	*Votre Proxy* > *Ports d'écoute* / *Protocole SSL* / *Authentification*
Blocage, liste blanche, règles	*Service de filtrage* > *Blocage de site web* / *Liste blanche* / *Règles de filtrage*
Certificats	*Votre système* > *Centre des certificats*
Mises à jour · sauvegarde	*Votre système* > *Mise à jour* · *Votre système* > *Sauvegarde*
GPO du TP	`Déploiement Certificat Artica` · `Configuration Proxy Artica` · `GPO Proxy Verrouillage`
Commandes client	`gpupdate /force` · `gpresult /r` · `netsh winhttp show proxy`

Sources : documentation officielle Artica (wiki.articatech.com) · documentation Microsoft Learn (stratégies de groupe, préférences Paramètres Internet, `gpresult` , `certutil`) · documentation Squid (SSL-Bump) · Procédure rédigée à partir d'un TP réalisé en équipe.