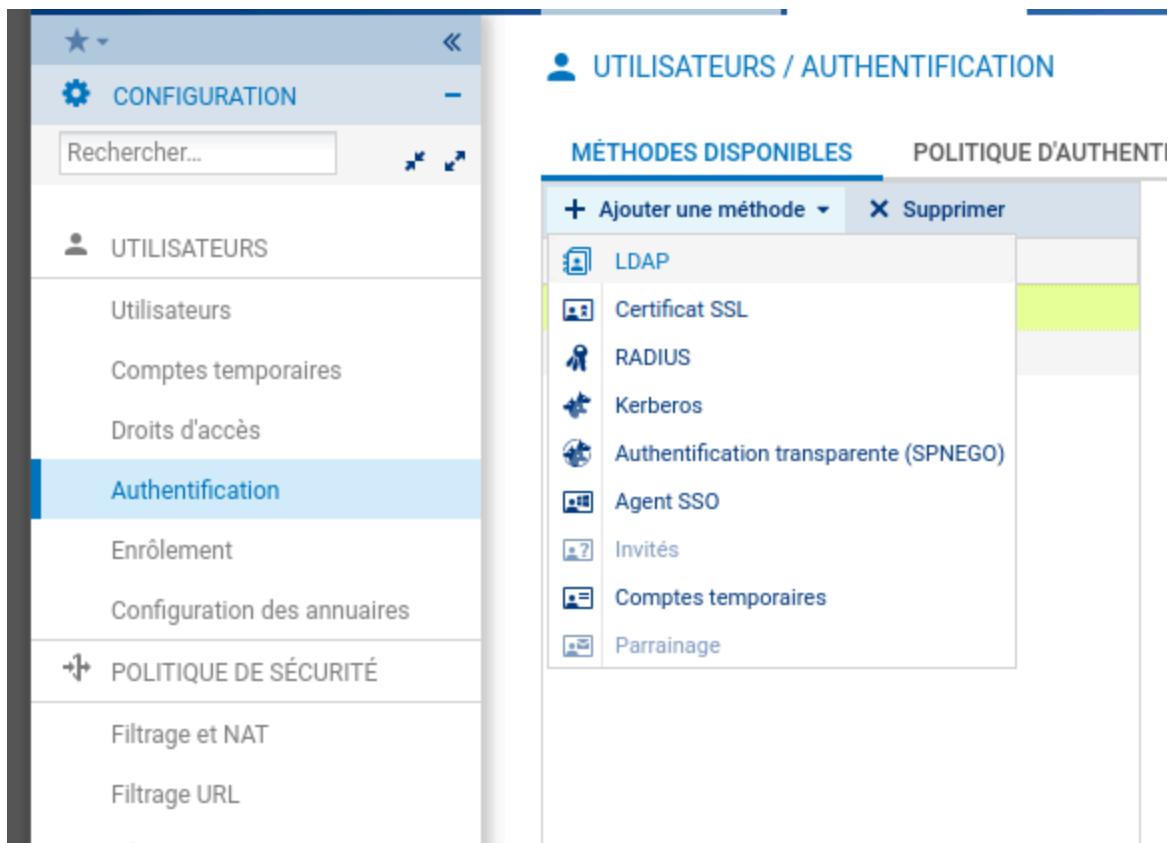


# SP4 - Portail - Mission 3

ⓘ Liam Boigegrain 901

## Mise en place du portail captif

Ajout de la connexion LDAP



The screenshot shows a configuration interface with a sidebar and a main panel. The sidebar on the left has sections for UTILISATEURS, AUTHENTICATION, and POLITIQUE DE SÉCURITÉ. The AUTHENTICATION section is currently selected. The main panel is titled 'UTILISATEURS / AUTHENTIFICATION' and shows a list of 'MÉTHODES DISPONIBLES' (Available Methods). The 'LDAP' method is selected and highlighted with a yellow background. Other methods listed include Certificat SSL, RADIUS, Kerberos, Authentification transparente (SPNEGO), Agent SSO, Invités, Comptes temporaires, and Parrainage. A 'Supprimer' (Delete) button is visible next to the LDAP entry.

MÉTHODES DISPONIBLES
LDAP
Certificat SSL
RADIUS
Kerberos
Authentification transparente (SPNEGO)
Agent SSO
Invités
Comptes temporaires
Parrainage

Connexion à l'annuaire Microsoft Active Directory :

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

CHOIX DU TYPE D'ANNUAIRE - (ÉTAPE 1 SUR 3)



- Connexion à un annuaire Microsoft Active Directory
- Connexion à un annuaire LDAP externe
- Connexion à un annuaire LDAP externe de type PosixAccount
- Création d'un annuaire LDAP interne

 ANNULER

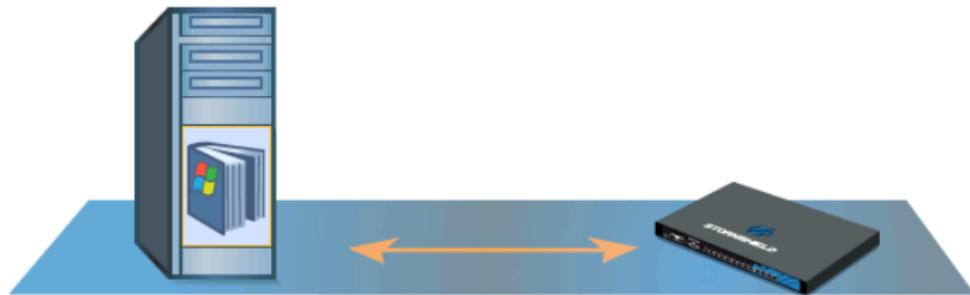
« PRÉCÉDENT

SUIVANT »

Renseignements LDAP :

## ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

### ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Nom de domaine:	local.epoka3.lan
Serveur:	ADEPOKA
Port:	ldap
Domaine racine (Base DN):	dc=local,dc=epoka3,dc=lan
Identifiant (user DN):	cn=Administrateur, cn=users
Mot de passe:	*****
Hachage des mots de passe:	SHA256

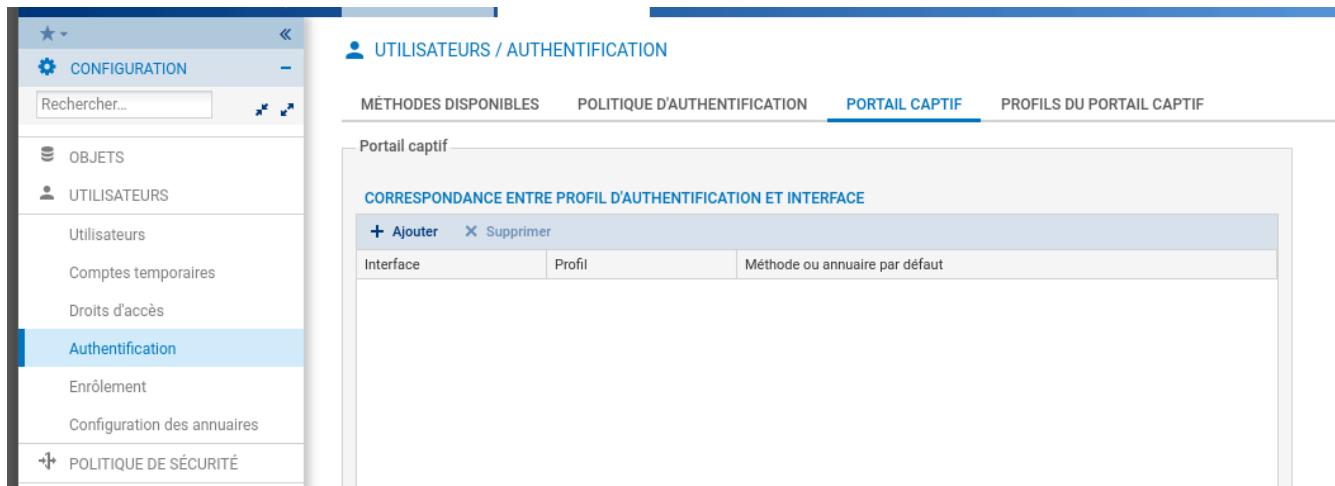
X ANNULER    « PRÉCÉDENT    SUIVANT »

### Vérification de la connexion :

<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <span style="color: #4F81BD; font-weight: bold;">+ Ajouter un annuaire</span>    <span style="color: #4F81BD; font-weight: bold;">≡ Action ▾</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">         Domain name  <span style="color: #4F81BD;">local.epoka3.lan</span> </div>	<div style="border-bottom: 1px solid #4F81BD; padding-bottom: 5px;"> <span style="color: #4F81BD; font-weight: bold;">CONFIGURATION</span>    <span style="color: #4F81BD; font-weight: bold;">STRUCTURE</span> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <b>Annuaire distant</b> <p><input checked="" type="checkbox"/> Activer l'utilisation de l'annuaire utilisateur</p> <table border="0"> <tr> <td>Serveur:</td> <td>ADEPOKA</td> </tr> <tr> <td>Port:</td> <td>ldap</td> </tr> <tr> <td>Domaine racine (Base Dn):</td> <td>dc=local,dc=epoka3,dc=lan</td> </tr> <tr> <td>Identifiant:</td> <td>cn=Administrateur, cn=users</td> </tr> <tr> <td>Mot de passe:</td> <td>*****</td> </tr> </table> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> <b>Connexion sécurisée (SSL)</b> </div>	Serveur:	ADEPOKA	Port:	ldap	Domaine racine (Base Dn):	dc=local,dc=epoka3,dc=lan	Identifiant:	cn=Administrateur, cn=users	Mot de passe:	*****
Serveur:	ADEPOKA										
Port:	ldap										
Domaine racine (Base Dn):	dc=local,dc=epoka3,dc=lan										
Identifiant:	cn=Administrateur, cn=users										
Mot de passe:	*****										

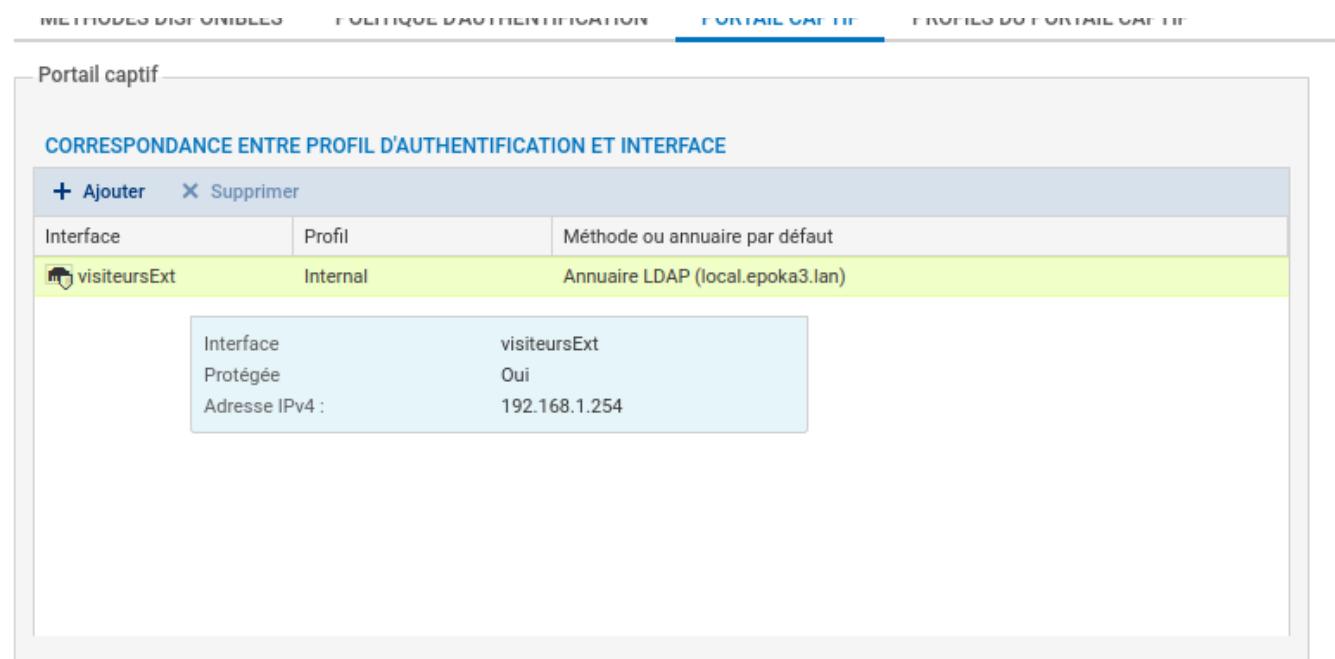
### Configuration du portail captif

## Accès : Utilisateur / Authentification / Portail captif



The screenshot shows the 'Utilisateurs / Authentification' interface. The left sidebar has 'Authentification' selected. The top navigation bar has 'PORTAIL CAPTIF' selected. The main content area shows a table for 'CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE' with a single row: 'visiteursExt' (Interface) -> 'Internal' (Profil) -> 'Annuaire LDAP (local.epoka3.lan)' (Méthode ou annuaire par défaut).

Associer le portail captif à l'interface Wi-Fi + LDAP :



The screenshot shows the 'Portail captif' configuration interface. The table 'CORRESPONDANCE ENTRE PROFIL D'AUTHENTIFICATION ET INTERFACE' shows a row for 'visiteursExt' (Interface) -> 'Internal' (Profil) -> 'Annuaire LDAP (local.epoka3.lan)' (Méthode ou annuaire par défaut). A detailed view of the 'visiteursExt' profile shows the following settings:

Interface	visiteursExt
Protégée	Oui
Adresse IPv4 :	192.168.1.254

Réglages du profil du portail

## 👤 UTILISATEURS / AUTHENTIFICATION

MÉTHODES DISPONIBLES

POLITIQUE D'AUTHENTIFICATION

PORTAIL CAPTIF

PROFILS DU PORTAIL CAPTIF

Internal | Renommer |

Authentification

Méthode ou annuaire par défaut: Annuaire LDAP (local.epoka3.lan) |

Activer le parrainage

Conditions d'utilisation de l'accès à Internet

Activer l'affichage des conditions d'utilisation d'accès à Internet

Fréquence d'affichage des Conditions: 4 heure(s) 0 minute(s)

Champs personnalisés du portail captif (méthode Invités uniquement)

Champ n°1: Vide

Champ n°2: Vide

Champ n°3: Vide

Durées d'authentification autorisées

Durée minimale: 0 heure(s) 15 minute(s)

Durée maximale: 4 heure(s) 0 minute(s)

Pour l'authentification transparente: 4 heure(s) 0 minute(s)

▲ Configuration avancée

Activer le portail captif

Activer la page de déconnexion

Autoriser l'accès au fichier de configuration du proxy (.pac) pour ce profil

Interdire l'authentification simultanée d'un utilisateur sur plusieurs machines

Expiration du 'cookie' HTTP: A la fin de la période d'authentification

## Règle NAT – Authentification

Création d'une règle permettant la redirection captive :

Network Security MONITORING CONFIGURATION EVAT VMSNSX02H5207A9

LOCAL.EPOKA3.LAN + X

CONFIGURATION

Rechercher... X

UTILISATEURS

- Utilisateurs
- Comptes temporaires
- Droits d'accès
- Authentification
- Enrôlement
- Configuration des annuaires

POLITIQUE DE SÉCURITÉ

Filtrage et NAT

Filtrage URL

**Filtrage** NAT

Rechercher... + Nouvelle règle X Supprimer ↑ ↓ X Couper

	État	Action	Source
1	on	passer	Any

Sélection du réseau Visiteur :

ASSISTANT D'AUTHENTIFICATION

Objectif : Rediriger vers le portail captif les utilisateurs qui ne sont pas authentifiés  
Par exemple, lors d'une première authentification ou après expiration de la session.

SOURCE		DESTINATION	
Qui:	les utilisateurs non authentifiés	Vers:	Internet
Depuis:	LAN_VisiteursExt	Hormis pour les URL:	+ Ajouter X Supprimer authentication_bypass

**TERMINER**

Restriction du trafic uniquement à internet :

MONITORING CONFIGURATION EVA1 VMSNSX02H5207A9

Politique de Sécurité / Filtrage et NAT

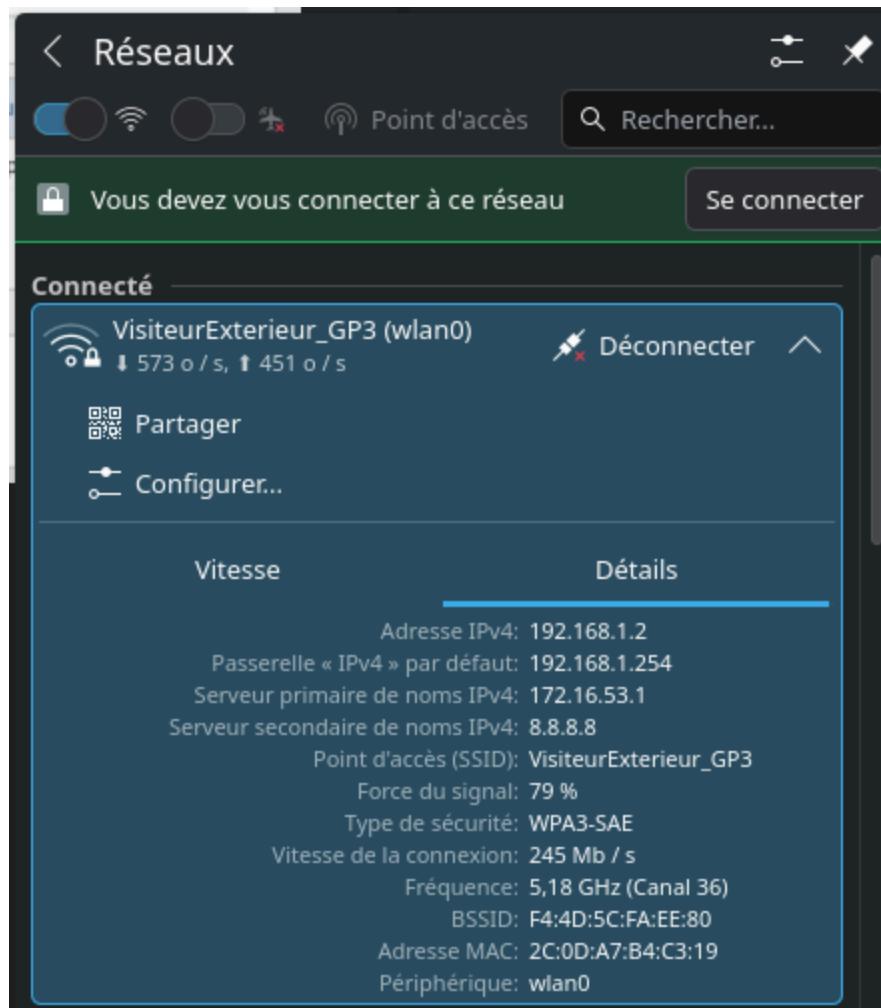
(10) Pass all | [Editor](#) | [Exporter](#) | [?](#)

**Filtrage NAT**

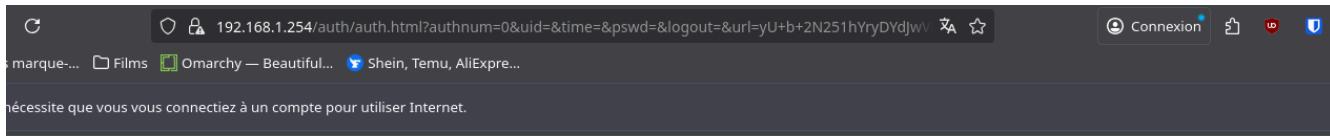
	Etat	Action	Source	Destination	Port dest.
1	on	Portail d'authentification	Hormis : authentification	Internet	http https dns
2	on	passer	any @ Network_visiteursExt interface: visiteursExt	ADEPOKA	dns
3	on	passer	any @ Network_visiteursExt interface: visiteursExt	Internet	http https dns
4	on	bloquer	Network_visiteursExt interface: visiteursExt	* Any	* Any
5	on	passer	* Any	* Any	* Any

## Identification depuis un poste

Après s'être connecté au wifi, notre poste nous signale qu'il faut s'authentifier :



Sur le portail captif, il faut s'authentifier avec un utilisateur sur l'AD :



STORMSHIELD Network Security

FR

Veuillez indiquer votre mot de passe d'authentification

Nom d'utilisateur: Administrateur

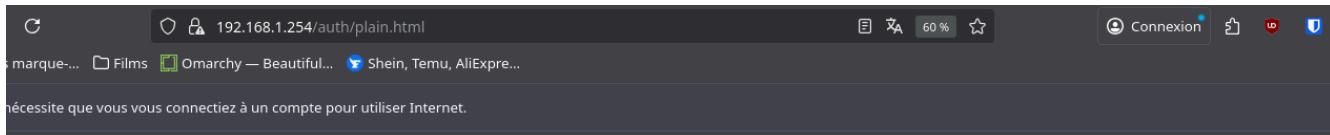
Mot de passe: ..... (password field)

Durée d'authentification: 4 heures

OK

Annuler

### Accepter les conditions d'utilisation :



STORMSHIELD Network Security

FR

Conditions d'utilisation de l'accès Internet

**Téléchargement de logiciels, ou d'œuvres protégées**

Le téléchargement par l'utilisateur de logiciels ou d'œuvres protégées, sans autorisation des ayants-droits, est de nature à engager la responsabilité de «MON ENTREPRISE» et comme tels sont strictement interdits. L'Administrateur se réserve la possibilité d'effacer du Système d'information toute trace de ces logiciels et œuvres introduites dans le Système, en violation des droits de propriété intellectuelle d'autrui.

**Consultation de sites illicites**

La consultation et le téléchargement du contenu de sites à caractère pornographique, pédophile, raciste, ou xénophobe sont contraires aux bonnes mœurs et peuvent revêtir le caractère d'une infraction pénale. Cette activité est strictement interdite.

**Consultation d'internet à des fins privées**

La consultation de sites web à titre privé est autorisée dans la mesure où cette navigation est exceptionnelle, limitée, n'entrave pas l'accès professionnel et qu'elle ne gêne pas de façon significative la productivité et la bonne marche du travail de l'utilisateur.

Il est précisé que le téléchargement de fichiers multimédia ou tout autre format de compression ne rentrant pas dans l'accès professionnel et gênant la bonne marche du Système d'information en raison de l'encombrement qu'il génère est strictement interdit.

Il est également interdit d'utiliser les réseaux de « Peer-to-Peer » pour un usage ne rentrant pas dans l'accès professionnel pour des raisons de sécurité et d'encombrement du réseau.

**Participation à des forums**

La participation à des forums peut engager la responsabilité de «MON ENTREPRISE». L'utilisateur doit disposer des autorisations internes afin de s'exprimer au nom de «MON ENTREPRISE» et devra préalablement prendre contact avec la Direction de «MON ENTREPRISE».

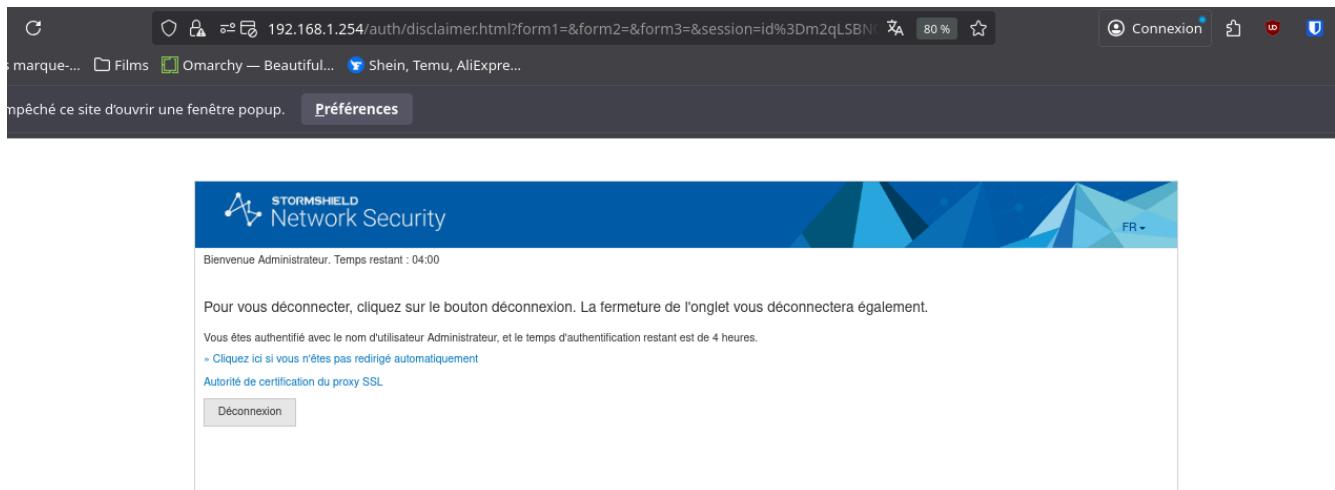
L'utilisateur est en outre responsable du respect des règles de confidentialité applicables à l'activité de «MON ENTREPRISE» et s'engage notamment, dans le cadre de sa participation à des forums, à ne pas :

- Utiliser des termes ou expressions jugés obscénités, pour toute forme, à un tiers non habilité à en avoir connaissance,
- Utiliser des Services d'échanges et de synchronisation de fichiers pour publier ou échanger des informations jugées confidentielles,
- Laisser sans surveillance et en tout lieu accessible à des tiers des informations jugées confidentielles,
- Ne pas diffuser ou publier sous toute forme que ce soit, sur les espaces en ligne accessibles au public et les réseaux sociaux externes, toute information ayant trait à «MON ENTREPRISE» et aux autres Utilisateurs, ainsi que les signes distinctifs de «MON ENTREPRISE» (marques, logos, ...).

J'ai pris connaissance de la charte

J'accepte

La connexion est réussite :



Bienvenue Administrateur. Temps restant : 04:00

Pour vous déconnecter, cliquez sur le bouton déconnexion. La fermeture de l'onglet vous déconnectera également.

Vous êtes authentifié avec le nom d'utilisateur Administrateur, et le temps d'authentification restant est de 4 heures.

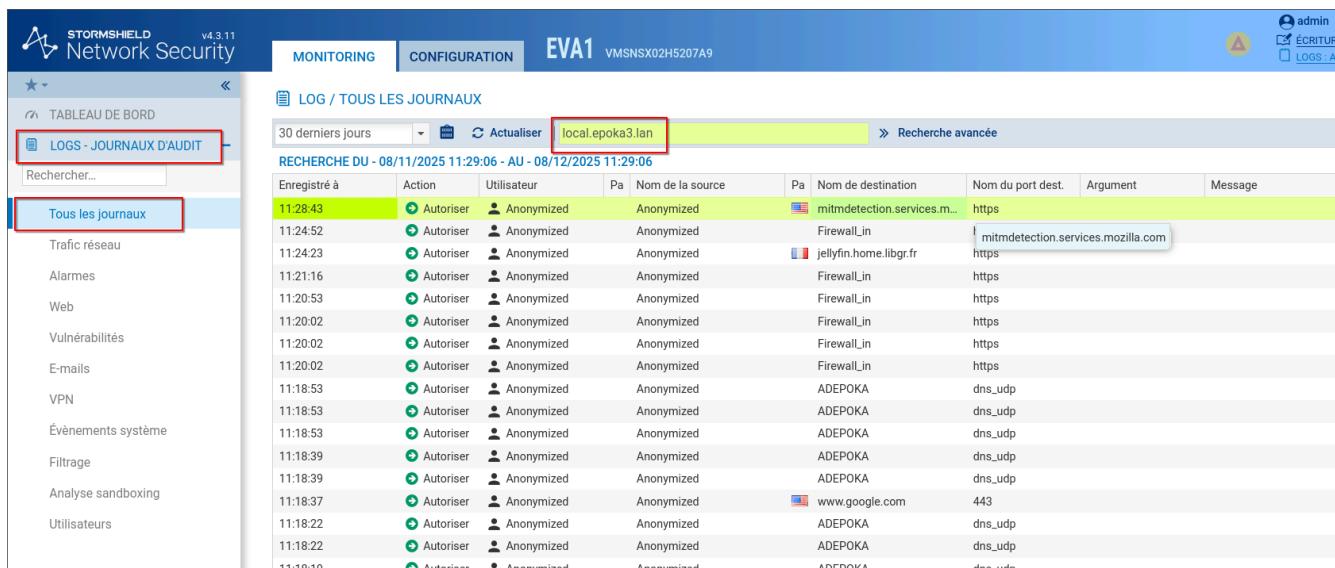
« Cliquez ici si vous n'êtes pas redirigé automatiquement

Autorité de certification du proxy SSL

Déconnexion

## Journalisation

Pour voir l'intégralité des journaux référant aux Visiteurs Exterieur, aller dans “Monitoring/LOGS/Tous les journaux” et rechercher le nom de l'AD:



Enregistré à	Action	Utilisateur	Pa	Nom de la source	Pa	Nom de destination	Nom du port dest.	Argument	Message
11:28:43	Autoriser	Anonymized	Anonymized	mitmdetection.services.m...	USA	mitmdetection.services.mozilla.com	https		
11:24:52	Autoriser	Anonymized	Anonymized	Firewall_in					
11:24:23	Autoriser	Anonymized	Anonymized	jellyfin.home.libgr.fr					
11:21:16	Autoriser	Anonymized	Anonymized	Firewall_in					
11:20:53	Autoriser	Anonymized	Anonymized	Firewall_in					
11:20:02	Autoriser	Anonymized	Anonymized	Firewall_in					
11:20:02	Autoriser	Anonymized	Anonymized	Firewall_in					
11:20:02	Autoriser	Anonymized	Anonymized	Firewall_in					
11:18:53	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:53	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:53	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:39	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:39	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:37	Autoriser	Anonymized	Anonymized	www.google.com	USA	443			
11:18:22	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:18:22	Autoriser	Anonymized	Anonymized	ADEPOKA					
11:10:10	Autoriser	Anonymized	Anonymized	ADEPOKA					

Ceci permet de voir toutes les connexion, web et paquets.

Pour voir uniquement les sites et requêtes, aller dans “Trafic réseau”:

STORMSHIELD Network Security v4.3.11

MONITORING CONFIGURATION EVA1 VMSNSX02H5207A9

LOG / TRAFIC RÉSEAU

RECHERCHE DU - 08/11/2025 11:22:31 - AU - 08/12/2025 11:22:31

Enregistré à Action Utilisateur Pa Nom de la source Pa Nom de destination Nom du port dest. Argument Message Reçu

11:18:37 Autoriser Anonymized Anonymized www.google.com 443 24.34 Ko

11:18:22 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 105 o

11:18:22 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 67 o

11:18:22 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 71 o

11:18:22 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 59 o

11:18:22 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 70 o

11:18:13 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 108 o

11:17:56 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 66 o

11:17:56 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 104 o

11:17:54 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 84 o

11:17:54 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 72 o

11:17:43 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 164 o

11:17:43 Autoriser Anonymized Anonymized ADEPOKA dns\_udp 176 o

11:16:52 Autoriser Anonymized Anonymized jellyfin.home.libgr.fr https 206.22 Ko

11:16:52 Autoriser Anonymized Anonymized jellyfin.home.libgr.fr https 2.98 Ko

11:16:51 Autoriser Anonymized Anonymized trilium.home.libgr.fr https 31.49 Ko

11:16:51 Autoriser Anonymized Anonymized jellyfin.home.libgr.fr https 7.67 Ko

11:16:51 Autoriser Anonymized Anonymized jellyfin.home.libgr.fr https 3.53 Ko

11:16:51 Autoriser Anonymized Anonymized jellyfin.home.libgr.fr https 9.91 Ko

11:16:43 Autoriser Anonymized ADEPOKA dns\_udp 120 o

DÉTAILS DE LA LIGNE DE LOG

Pour voir les authentifications, allez dans "Utilisateurs":

STORMSHIELD Network Security v4.3.11

MONITORING CONFIGURATION EVA1 VMSNSX02H5207A9

LOG / UTILISATEURS

RECHERCHE DU - 08/11/2025 11:26:24 - AU - 08/12/2025 11:26:24

Enregistré à Utilisateur Source Méthode Message

11:17:16 Anonymized Anonymized PLAIN user is logged out

11:07:39 Anonymized Anonymized PLAIN user is logged in for 4 hours

01/12/2025 16:07:41 Anonymized Anonymized PLAIN user is logged in for 4 hours

01/12/2025 15:27:24 Anonymized Anonymized PLAIN user is logged in for 4 hours

01/12/2025 15:26:42 Anonymized Anonymized PLAIN authentication failed, bad password

01/12/2025 14:41:01 Anonymized Anonymized PLAIN user is logged out

01/12/2025 14:39:12 Anonymized Anonymized PLAIN user is logged in for 4 hours

DÉTAILS DE LA LIGNE DE LOG