

Artica Proxy : Une Solution Complète de Gestion et Sécurisation du Réseau



Réalisé par : Karim maâli

🏠 Introduction :

Artica Proxy est une solution de proxy open-source permettant la gestion et la sécurisation des connexions Internet dans un réseau d'entreprise. Il repose sur **Squid** et intègre une interface graphique avancée facilitant son administration. Cette solution est particulièrement appréciée pour ses fonctionnalités avancées en matière de filtrage, de reporting et de contrôle d'accès.

🏠 Fonctionnalités principales :

Artica Proxy offre un large éventail de fonctionnalités, notamment :

Filtrage Web avancé : blocage des sites web indésirables via des listes noires et des catégories prédéfinies.

Contrôle d'accès : restriction de l'accès à Internet selon des règles spécifiques basées sur les utilisateurs, groupes ou horaires.

Gestion de la bande passante : limitation de la consommation pour éviter la saturation du réseau.

Cache Web : amélioration des performances en stockant localement les contenus fréquemment consultés.

Authentification centralisée : support des protocoles LDAP, Active Directory et RADIUS pour la gestion des utilisateurs.

Reporting et statistiques : génération de rapports détaillés sur l'utilisation d'Internet.

🏠 Avantages et cas d'utilisation :

Entreprises : Sécurisation et optimisation de l'accès à Internet pour les employés.

Écoles et universités : Filtrage des contenus inappropriés et gestion des accès étudiants.

Centres de données : Amélioration des performances réseau grâce au cache Web.

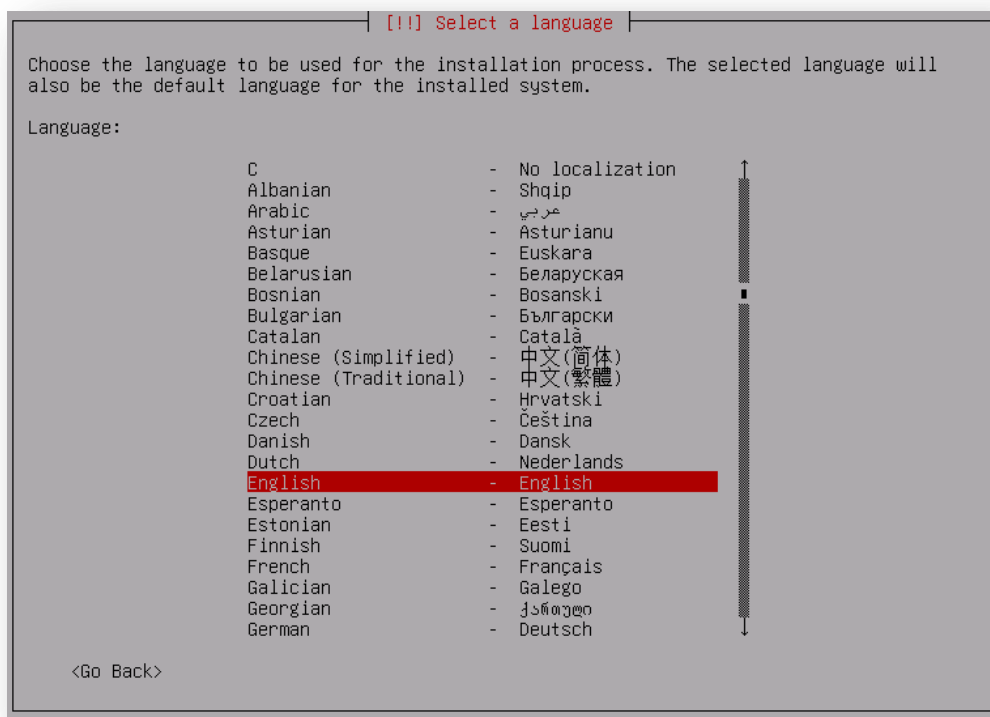
Administrations publiques : Respect des politiques de cybersécurité et surveillance des connexions.

Guide d'installation et de configuration d'Artica :

Étape 1 : Sélectionner : “Artica v4.50 hotfix 20250204-20”



Choisissez une langue à utiliser pendant le processus d'installation. La langue sélectionnée sera également la langue par défaut du système en cours d'installation.



Sélectionnez votre emplacement

Le pays sélectionné est utilisé pour définir le fuseau horaire et déterminer les paramètres régionaux du système. Il s'agit le plus souvent du pays dans lequel vous vivez.

La liste restreinte affichée dépend de la langue que vous avez sélectionnée précédemment. Sélectionnez <<Autre>> si votre pays n'est pas affiché.

Dans notre cas, nous choisirons un **autre** pays pour rechercher **l'Afrique - le Maroc**

[!!] Choix de votre situation géographique	
Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.	
La courte liste affichée dépend de la langue précédemment choisie. Choisissez « Autre » si votre pays n'est pas affiché.	
Pays (territoire ou région) :	
	Belgique
	Canada
	France
	Luxembourg
	Suisse
	Autre
<Revenir en arrière>	

Veuillez choisir le continent ou la région où est situé votre emplacement géographique :

Afrique

[!!] Choix de votre situation géographique	
Le pays choisi permet de définir le fuseau horaire et de déterminer les paramètres régionaux du système (« locale »). C'est le plus souvent le pays où vous vivez.	
Veuillez choisir le continent ou la région où est situé votre emplacement géographique.	
Continent ou zone géographique :	
	Afrique
	Amérique Centrale
	Amérique du Nord
	Amérique du Sud
	Antarctique
	Asie
	Caraïbes
	Europe
	Océan Atlantique
	Océan Indien
	Océanie
<Revenir en arrière>	

Maroc



Vous êtes invité à saisir une adresse IP pour déterminer comment l'appareil se connecte au réseau.

Il est préférable d'utiliser une adresse IP statique afin qu'elle ne change pas après un redémarrage de l'appareil, ce qui peut entraîner des problèmes de connexion.

[[!]] Configurer le réseau

L'adresse IP est propre à une machine et peut être constituée de :

- * quatre nombres séparés par des points (IPv4) ;
- * des blocs de caractères hexadécimaux séparés par le caractère « deux-points » (IPv6).

Il est également possible d'ajouter un masque de sous-réseau au format CIDR (par exemple « /24 »).

Si vous ne savez pas quoi indiquer, veuillez consulter l'administrateur de votre réseau.

Adresse IP :

192.168.1.150/24

<Revenir en arrière><Continuer>

passerelle :

[[!]] Configurer le réseau

La passerelle est une adresse IP (quatre nombres séparés par des points) qui indique la machine qui joue le rôle de routeur ; cette machine est aussi appelée le routeur par défaut. Tout le trafic qui sort du réseau (p. ex. vers Internet) passe par ce routeur. Dans quelques rares circonstances, vous n'avez pas besoin de routeur. Si c'est le cas, vous pouvez laisser ce champ vide. Consultez votre administrateur si vous ne connaissez pas la réponse correcte à cette question.

Passerelle :

192.168.1.1

<Revenir en arrière><Continuer>

À cette étape, il vous est demandé de saisir les adresses des serveurs DNS, chargés de résoudre les noms de domaine.

[[!]] Configurer le réseau

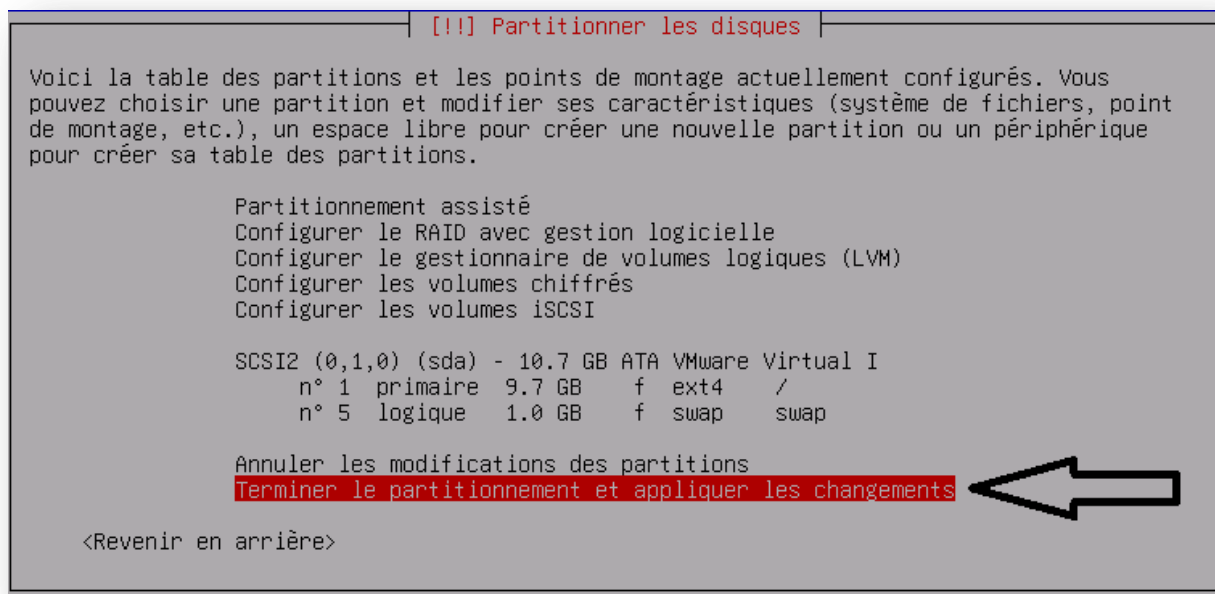
Les serveurs de noms servent à la recherche des noms d'hôtes sur le réseau. Veuillez donner leurs adresses IP (pas les noms des machines) ; vous pouvez inscrire au plus trois adresses, séparées par des espaces. N'utilisez pas de virgule. Le premier serveur indiqué sera interrogé en premier. Si vous ne voulez pas utiliser de serveur de noms, laissez ce champ vide.

Adresses des serveurs de noms :

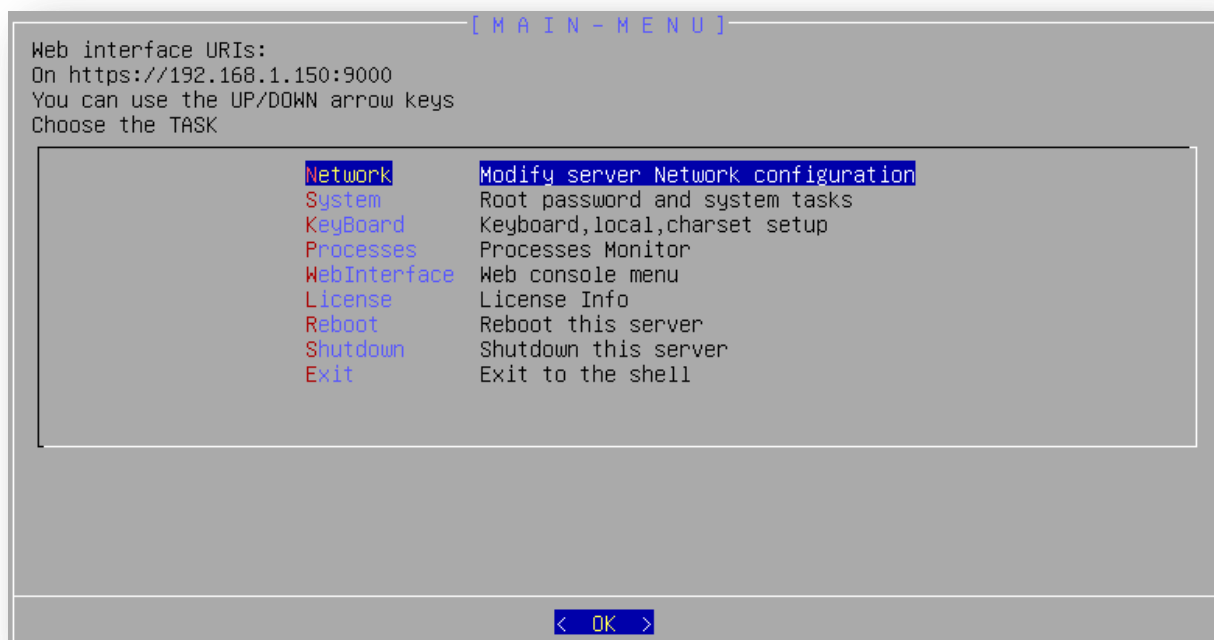
192.168.1.1

<Revenir en arrière><Continuer>

Choisir → Terminer le partitionnement et appliquer les changements



Une fois Artica Proxy installé, vous devez ouvrir votre navigateur Web pour accéder à son interface graphique et effectuer les paramètres initiaux.



Ouvrez un navigateur Web (Google Chrome, Firefox, Edge...).

<https://192.168.1.150:9000>



Vous verrez un avertissement de sécurité dans votre navigateur (en raison du certificat non fiable), vous pouvez contourner l'avertissement en cliquant sur « Continuer vers le site » ou « Avancé > Continuer ».

Configuration de base :

Après avoir installé Artica Proxy et ouvert son interface via un navigateur, l'interface de configuration initiale vous sera présentée, où vous serez dirigé pour ajuster les paramètres de base du serveur.

Cette étape consiste à définir le fuseau horaire et la langue de l'interface pour garantir que le serveur fonctionne correctement en fonction de votre emplacement et de vos préférences.



Bienvenue dans le projet Artica

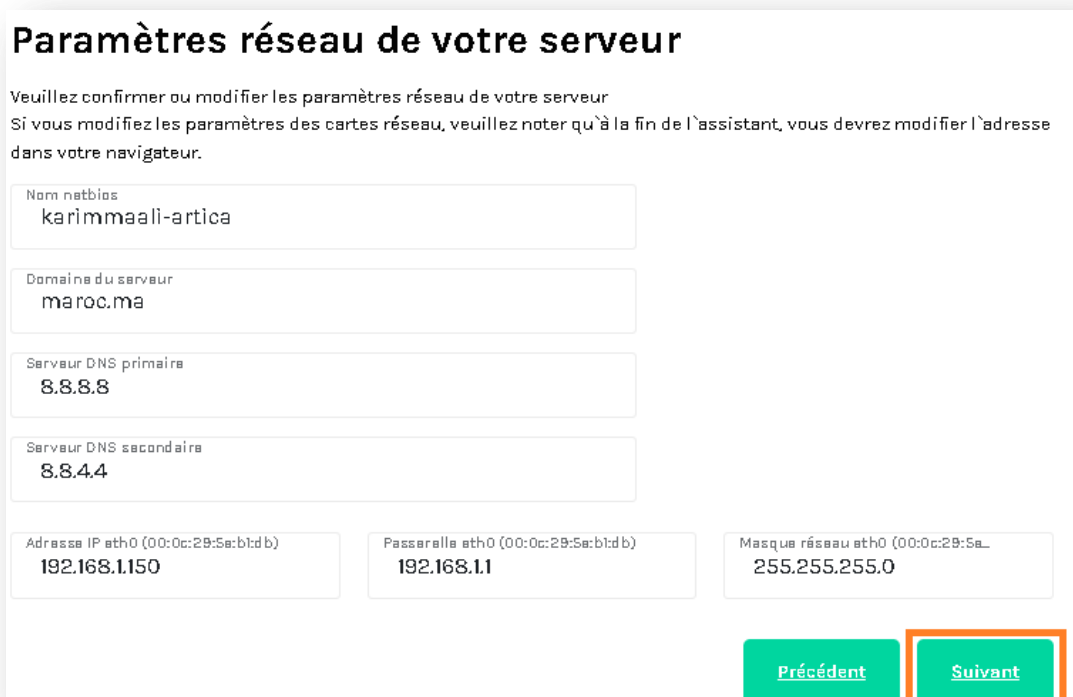
Cet assistant va vous guider afin de paramétrer les options principales de votre serveur.
Cliquez sur suivant afin de continuer

Zone de temps
Africa/Casablanca

Ma langue
Francais

 [Suivant](#)

Cette étape vous permet de confirmer ou de modifier les paramètres réseau du serveur, garantissant ainsi une connexion correcte au réseau local et à Internet.



Paramètres réseau de votre serveur

Veuillez confirmer ou modifier les paramètres réseau de votre serveur
Si vous modifiez les paramètres des cartes réseau, veuillez noter qu'à la fin de l'assistant, vous devrez modifier l'adresse dans votre navigateur.

Nom netbios
karimmaali-artica

Domaine du serveur
maroc.ma

Serveur DNS primaire
8.8.8.8

Serveur DNS secondaire
8.8.4.4

Adresse IP eth0 (00:0c:29:5e:b1:d b)
192.168.1.150

Passerelle eth0 (00:0c:29:5e:b1:d b)
192.168.1.1

Masque réseau eth0 (00:0c:29:5e: b1:d b)
255.255.255.0

[Précédent](#) [Suivant](#)

Dans cette étape, vous déterminez le rôle principal que le serveur Artica exécutera en fonction de votre utilisation réelle. Cette sélection affectera les services qui seront activés lors de la configuration.

Quelle sera l'activité principale de ce serveur Artica ?

Nous vous proposons ici de formater votre serveur en fonction de différents cas d'utilisation.
Si vous souhaitez ajouter des fonctionnalités à votre serveur ultérieurement, choisissez le modèle Générique.

 Service Proxy Web proxy simple pour le service de proxy et de filtrage Web.	 Pare-feu DNS La fonctionnalité de pare-feu DNS vous permet de créer des règles avancées pour protéger le protocole DNS.	 Reverse-Proxy Le serveur proxy vous permet de créer des règles avancées pour protéger vos services Web, de manière cachée, et de vous protéger contre les attaques par déni de service (DDoS) et les attaques par force brute (Brute Force).
 Puits de logs La fonctionnalité de puits de logs vous permet de contrôler les données de logs et de les analyser en temps réel.	 Passerelle minimale Vous pouvez utiliser ce serveur minimaliste pour protéger vos services.	 Restaurer un instantané Si vous avez des données de logs ou des données de configuration, vous pouvez les restaurer à l'aide de ce serveur.

[Précédent](#) [Suivant](#)

⇒ Service proxy

Artica vous permet de fonctionner comme un proxy Web pour contrôler votre navigation sur Internet, avec la possibilité de filtrer le contenu et de bloquer les sites Web.

Convient aux entreprises et organisations qui souhaitent contrôler l'utilisation d'Internet par leurs employés.

⇒ Pare-feu DNS

Vous permet de créer des règles avancées pour protéger le trafic DNS, telles que le blocage de sites malveillants ou la direction de requêtes vers des serveurs DNS personnalisés.

Il est utilisé pour protéger le réseau des sites malveillants et empêcher l'espionnage DNS.

⇒ **Reverse Proxy**

Il vous permet d'exécuter un serveur Web protégé, d'améliorer la vitesse du site via la mise en cache et de sécuriser les applications avec un pare-feu d'application Web (WAF).

Convient si vous hébergez des sites Web ou des applications internes et souhaitez améliorer leurs performances et leur sécurité.

⇒ **Logs (stockage et analyse des logs)**

Il fait du serveur un référentiel central pour les journaux réseau, ce qui aide à l'analyse de sécurité et au respect des réglementations légales.

Utile pour les administrateurs réseau et de sécurité qui ont besoin de conserver des journaux détaillés.

⇒ **Passerelle minimaliste**

Installe le strict minimum de services pour exécuter Artica, sans ajouter de fonctionnalités avancées.

Une option appropriée pour les tests ou une utilisation légère.

⇒ **Restaurer un instant (restaurer une sauvegarde)**

Si vous disposez d'une sauvegarde d'un serveur Artica précédent, vous pouvez le restaurer directement.

Utile dans les cas de reconfiguration sans perdre les anciens paramètres.

Choisissez le travail qui correspond à vos besoins et appuyez sur « Suivant » pour continuer.

Si vous n'êtes pas sûr, vous pouvez choisir Passerelle minimale puis ajouter les fonctionnalités plus tard.

Dans notre cas, nous choisirons le **service proxy**.

Dans cette étape, vous allez configurer le compte administrateur principal chargé de gérer le serveur via l'interface Web, ainsi que de saisir les informations de l'organisation et de lier l'e-mail pour recevoir des notifications.

Compte Administrateur/Société virtuelle

Le compte administrateur disposera de tous les privilèges sur l'interface web d'administration.

Après l'assistant, vous serez en mesure de créer d'autres utilisateurs avec des droits restreints via une base locale, Active Directory ou LDAP.

Ce formulaire vous permet également d'indiquer une adresse mail et le nom d'une entité (le nom de votre entreprise par exemple).

Ces données seront utilisées afin de personnaliser l'interface web et les pages web affichées à l'intention vos utilisateurs.

Compte Administrateur

karim

Mot de passe

Votre adresse email

karimmaali99@gmail.com

organization

My Company

Fichier de licence

Choisir un fichier

Aucun fichier choisi

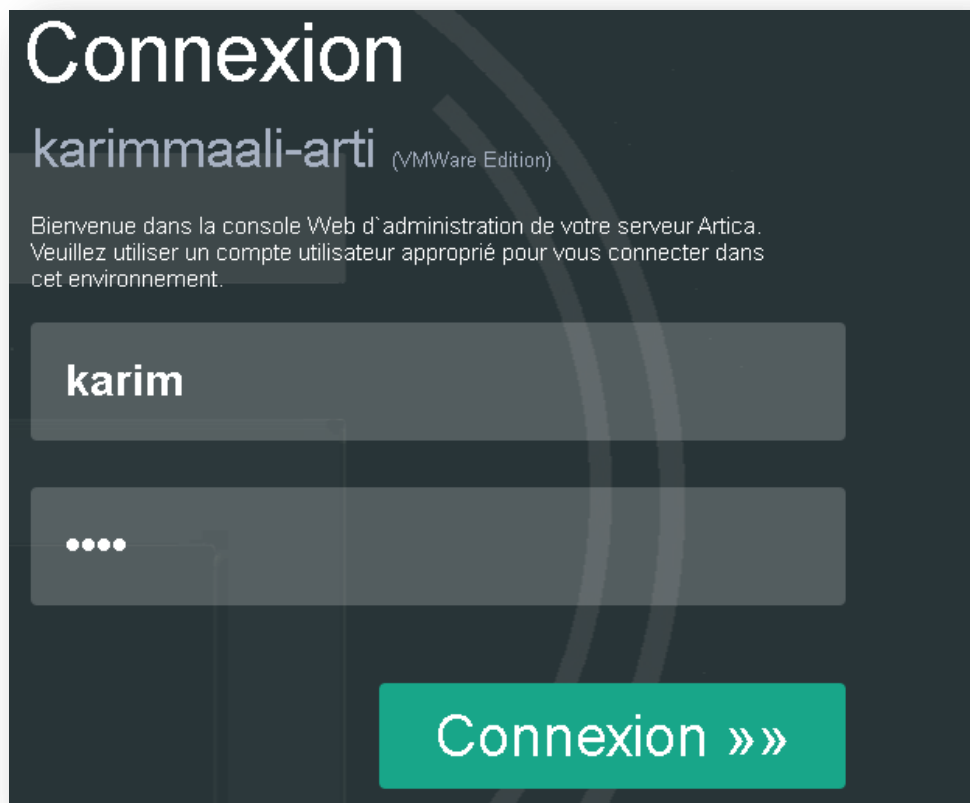
[Précédent](#)

[Suivant](#)

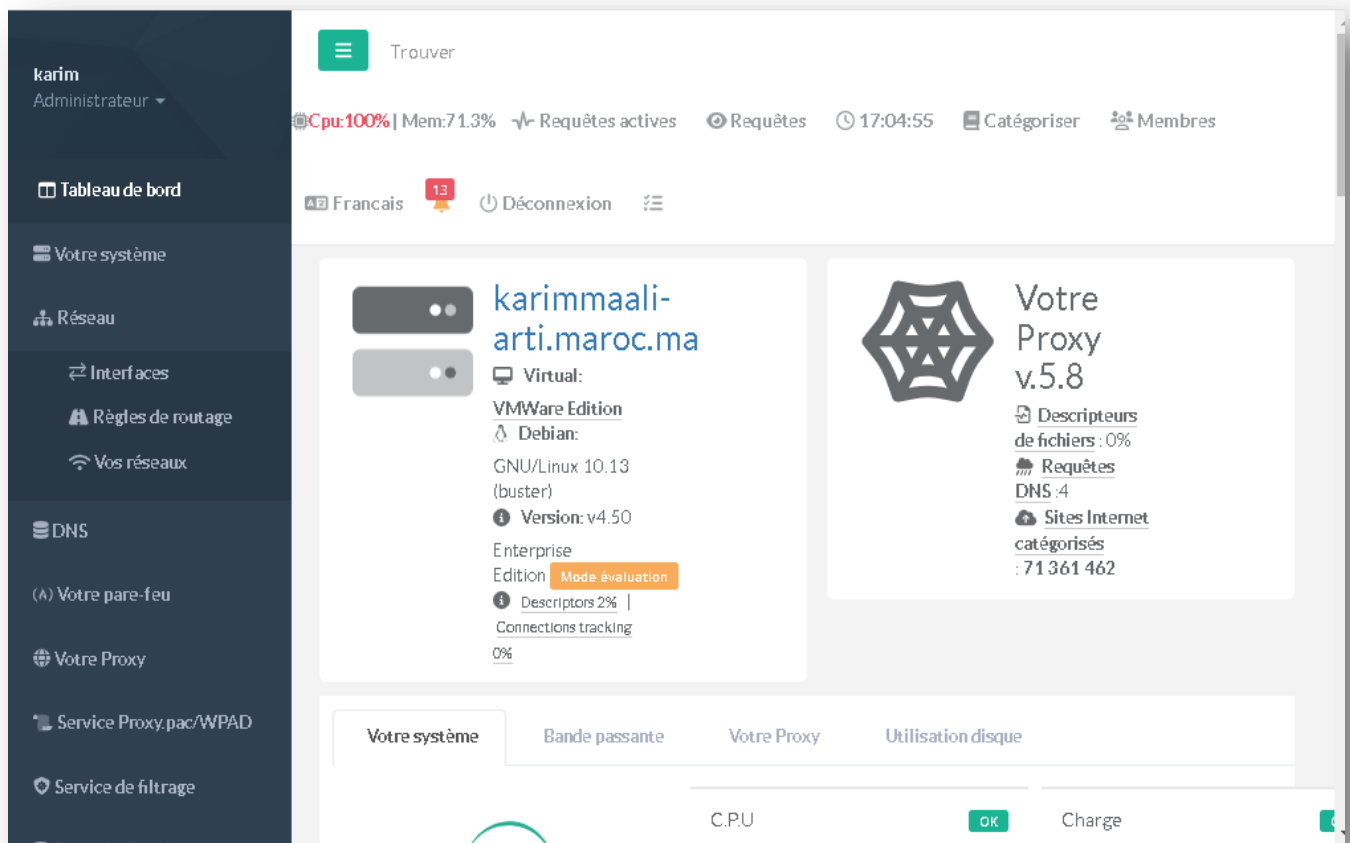


Après avoir saisi les informations, cliquez sur « **Suivant** » pour passer aux étapes finales de la configuration.

Saisissez le nom d'utilisateur et le mot de passe que vous avez définis pour accéder à l'interface Artica.



L'interface Artica fonctionne correctement



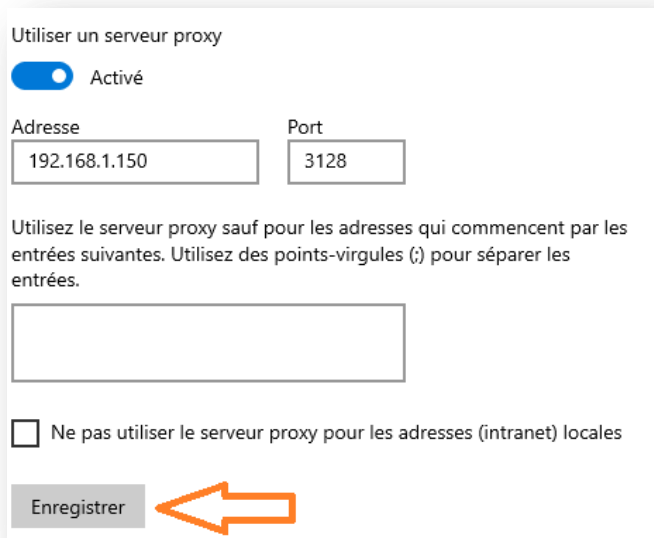
Gestion de Proxy et Sécurité Web avec Artica :

Comment bloquer un site à l'aide des listes de contrôle d'accès (ACL) ?

Tout d'abord, le client doit se connecter à notre serveur proxy :

Ip proxy : 192.168.1.150

Port par défaut : 3128



Utiliser un serveur proxy

☒ Activé

Adresse: 192.168.1.150 Port: 3128

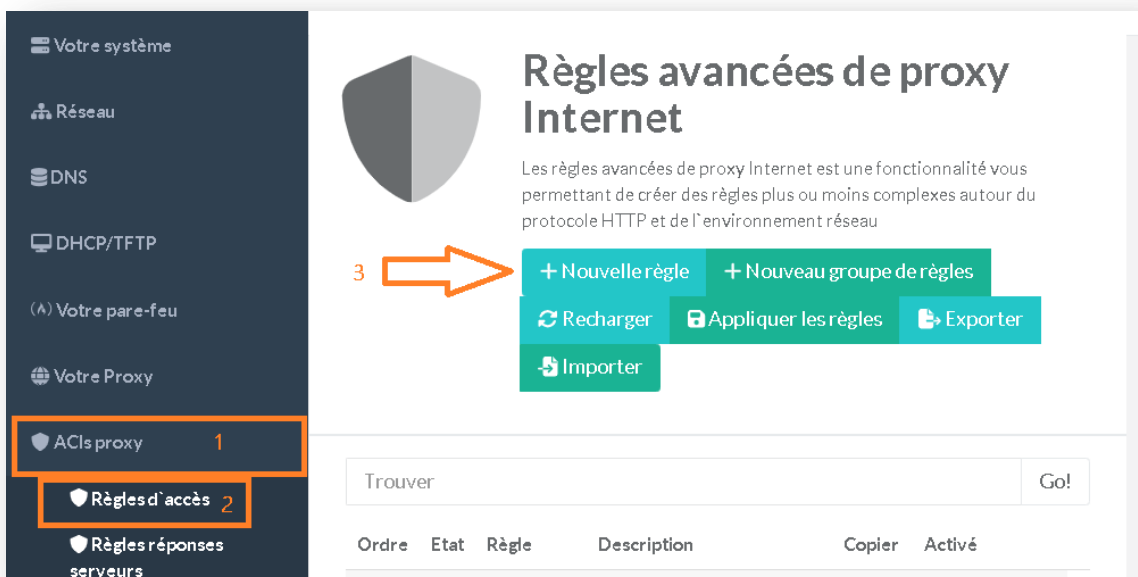
Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

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

Enregistrer

Pour bloquer un site Web à l'aide de listes de contrôle d'accès (ACL) sur la plateforme Artica, vous pouvez suivre ces étapes :

- ⇒ Dans le menu de gauche, choisissez « **ACLs proxy** » / « **régles d'accès** »
- ⇒ Cliquez sur nouvelle règle



Votre système

Réseau

DNS

DHCP/TFTP

(A) Votre pare-feu

Votre Proxy

ACLs proxy 1

Règles d'accès 2

Règles réponses serveurs

Règles avancées de proxy Internet

Les règles avancées de proxy Internet est une fonctionnalité vous permettant de créer des règles plus ou moins complexes autour du protocole HTTP et de l'environnement réseau

3

+ Nouvelle règle + Nouveau groupe de règles

Recharger Appliquer les règles Exporter

Importer

Trouver Go!

Ordre	Etat	Règle	Description	Copier	Activé
-------	------	-------	-------------	--------	--------

Donnez un nom à la règle. Dans ce cas, nous l'avons nommé **interdire_netflix** car nous souhaitons bloquer le site **netflix**

- ⇒ Et le **type**, choisissez **interdire l'accès** car nous voulons bloquer l'accès au site , et Cliquez sur ajouter

A screenshot of a web application form for creating a rule. The form has three input fields: 'Nom De La Règle:' with the value 'interdire_netflix', 'Type:' with a dropdown menu showing 'Interdire l'accès', and 'Methode:' with a dropdown menu showing 'Toutes méthodes'. At the bottom right, there is a green button with the text '« Ajouter »' highlighted by an orange rectangle.

Après avoir créé cette règle, cliquez dessus pour terminer ses paramètres.

A screenshot of a web application showing the configuration summary for the rule 'interdire_netflix'. The rule name is highlighted with an orange rectangle. Below the rule name, there is a description: 'Lors de la connexion avec la méthode «Toutes méthodes», Interdire l'accès'. To the right of the description, there are several icons: a refresh icon, a copy icon, a checkmark icon, an up arrow icon, a down arrow icon, and a trash icon. At the bottom, there is a section labeled 'Finalement' with a dropdown menu showing 'Finalement, tout autoriser' and a green checkmark icon.

Cliquez sur Objets proxy et créez object

A screenshot of a web application showing the 'Objets proxy' section. The 'Objets proxy' tab is highlighted with an orange rectangle. Below the tabs, there are three buttons: '+ Nouvel objet' (highlighted with an orange rectangle), 'Lier l'objet', and 'Nouveau groupe d'objets'. Below the buttons, there is a search bar with the text 'Trouver' and a 'Go!' button. At the bottom, there is a table with columns: 'Ordre', 'Est/N Est Pas', 'Objets', 'Type', and 'Éléments'.

Nommez-le selon votre choix et appuyez sur Sélectionner. (**choisir**)

Choisissez ensuite "**le serveur Web ou le domaine**"

, Et Cliquez sur ajouter

Nouvel objet

Nom De L'Objet:

Type: Choisir

« Annuler » « Ajouter »

Cliquez ensuite ici pour ajouter le site

Ordre	Est/N Est Pas	Objets	Type	Éléments
1	Est	<u>block_site</u>	☁ Serveur Web ou domaine	0 + ✕ ↑ ↓ ↺

Ajoutez le site que vous souhaitez bloquer, dans notre cas nous voulons bloquer netflix , puis cliquez sur **Ajouter**.

Modèle:

1 netflix.com

« Ajouter »

Vous devez **ensuite ajouter un autre objet** Nouvel pour appliquer cette règle à tout le monde.

Dans Type, sélectionnez Tout (all) pour l'appliquer à tous.

puis cliquez sur **Ajouter**.

+ Nouvel objet Lier l'objet Nouveau groupe d'objets

Nouvel objet

Nom De L'Objet: tous

Type: all Choisir

« Annuler » « Ajouter »

Enfin, cliquez sur Appliquer les règles pour enregistrer les modifications.

➡ Appliquer les règles Exporter Importer

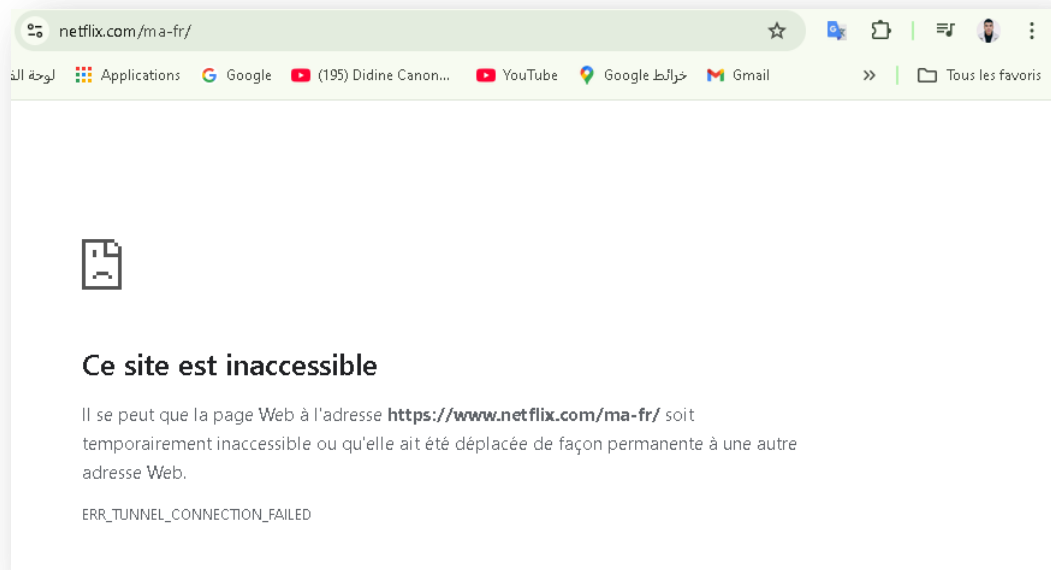
Centres des acces: 100% Fait Reloading proxy service [«détails»](#)

Centres des acces - 100% Fait Reloading proxy service

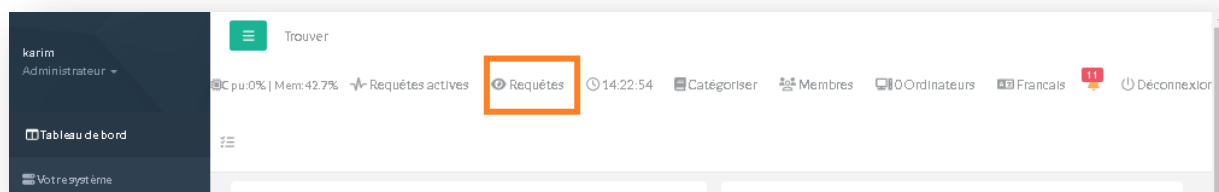
Trouver Go!

Ordre	Etat	Règle	Description	Copier	Activé
0	Inconnu	<u>interdire_netflix</u>	Lors de la connexion avec la méthode «Toutes méthodes», Pour les objets « block site » (1 Éléments) alors Interdire l'accès		

Résultat :



Pour surveiller tous les sites Web visités par le client



Tous les emplacements en temps réel

14:24:36	192.168.1.9 mac: a8:6b:ad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	www.google.com
14:24:21	192.168.1.9 mac: a8:6b:ad:47:53:47	Bannis - ERR_ACCESS_DENIED - Forbidden - port distant	SSL	Google	mtalk.google.com
14:24:20	192.168.1.9 mac: a8:6b:ad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	mtalk.google.com
14:23:36	192.168.1.9 mac: a8:6b:ad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	www.google.com

Vous pouvez cliquer sur un site à partir d'ici et le bloquer facilement.

14:24:36	192.168.1.9 mac: a8:6bad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	www.google.com
14:24:21	192.168.1.9 mac: a8:6bad:47:53:47	Bannis - ERR_ACCESS_DENIED - Forbidden - port distant	SSL	Google	mtalk.google.com
14:24:20	192.168.1.9 mac: a8:6bad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	mtalk.google.com
14:23:36	192.168.1.9 mac: a8:6bad:47:53:47	SSL Connect - Pass - finalement autoriser	SSL	Google	www.google.com

cliquez sur

 Appliquer

Pour le bloquer

*.google.com

Google

Vous désirez rapporter une mauvaise catégorisation ou bien une non-catégorisation de ce site, veuillez cliquer sur le bouton.

? Rapport De La Catégorie

ACIs proxy

Ajouter à un objet ACL

Sélectionner


Mettre ce site en liste blanche

Sauvegarde ce site Internet dans la liste des sites Internet autorisés.
Ce site web sera alors disponible pour l'ensemble des utilisateurs.

Appliquer

Interdire ce site

Sauvegarder ce site Internet dans la liste des sites interdits par le Filtrage Web.
Tous les utilisateurs seront impactés par le blocage de ce site Internet.

 Appliquer